MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA

RECURSO EXTRAORDINÁRIO 1.301.250/RJ
RELATORA: MINISTRA ROSA WEBER
RECORRENTES: GOOGLE BRASIL INTERNET LTDA. E OUTROS
ADVOGADOS: EDUARDO BASTOS FURTADO DE MENDONÇA E OUTROS
RECORRIDOS: ESTADO DO RIO DE JANEIRO E OUTROS
PARECER ARESV/PGR Nº 378743/2021

RECURSO EXTRAORDINÁRIO. PROCESSO PENAL. CONSTITUCIONAL REPERCUSSÃO GERAL. TEMA 1148. SIGILO DE DADOS TELEMÁTICOS. AFASTAMENTO. PARÂMETROS. PESSOAS INDETERMINADAS. POSSIBILIDADE. REGISTROS DE CONEXÃO E ACESSO À INTERNET REQUISITOS. MCI. DADOS AUXILIARES DE IDENTIFICAÇÃO. SUBSIDIARIEDADE. OBRIGAÇÕES ACESSÓRIAS. RECURSO EXTRAORDINÁRIO. PARCIAL PROVIMENTO.

1. Recurso extraordinário *leading case* do Tema 1148 da sistemática da Repercussão Geral: "*limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas*".

2. A análise da proteção à privacidade no Direito Comparado sinaliza crescente preocupação com a possibilidade de coleta e armazenamento indiscriminado de dados, seja pelo Estado, seja por terceiros, na linha do reconhecimento da

autodeterminação informativa. Todavia, contemplam-se explicitamente exceções, na linha das restrições legítimas aos direitos fundamentais, notadamente aquelas ligadas à preservação de direitos fundamentais de terceiros, com níveis de acesso matizados consoante a sensibilidade dos dados obtidos e o interesse premente na sua obtenção.

3. A jurisprudência do Supremo Tribunal Federal aponta para a existência de um direito à proteção de dados, assegurado por mecanismos de salvaguarda revelados por normas de proteção e normas de organização e procedimento, cuja definição decorre de análise conjunta e integrada das previsões em relação ao tema do microssistema jurídico protetivo dos dados e comunicações, no qual se destacam as Leis nº 9.296/96, nº 12.965/2014 e nº 13.709/2018.

4. O descarte *a priori* de um meio de investigação legítimo, de modo arbitrário, quando possível seu emprego dentro de balizas que respeitem e se ajustem aos demais direitos fundamentais seria, em si, medida inconstitucional e incompatível com o direito à memória e à verdade das vítimas e os deveres de investigação efetiva e punição decorrentes dos tratados de Direitos Humanos assinados pelo Brasil, notadamente no contexto de graves violações a bens jurídicos protegidos por estes tratados.

5. Os parâmetros para o uso harmonizado do afastamento do sigilo de dados de pessoas indeterminadas com o ordenamento jurídico brasileiro inclui a observância de normas protetivas, representadas pelos requisitos para o deferimento do acesso aos dados, calibrados consoante a sensibilidade da informação disponibilizada e o contexto

investigativo; e de normas de organização e procedimento, que estabelecem obrigações associadas ao acesso às informações, notadamente ligadas à transferência, guarda e inutilização dos dados de terceiros obtidos e a seu emprego no contexto do processo criminal.

6. Proposta de Tese de Repercussão Geral:

É permitido o afastamento de sigilo de dados telemáticos, no âmbito de procedimentos penais, ainda que em relação a pessoas indeterminadas, nos seguintes parâmetros:

I – Aplica-se, no tocante aos requerimentos de registros de conexão ou acesso a aplicações de internet, os requisitos previstos no art. 22 da Lei nº 12.965/2014 (Marco Civil da Internet): a apresentação dos fundados indícios da ocorrência do ilícito; a justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e a delimitação do período ao qual se referem os registros.

II – Quando os dados telemáticos solicitados forem associados a dados pessoais que possam contribuir para a identificação do usuário ou do terminal, cumpre à autoridade requerente também justificar fundamentadamente:

a) A necessidade da medida para a investigação em concreto, que há de ser subsidiária em relação a outros meios de prova menos gravosos a direitos de terceiros;

b) A pertinência das informações obtidas em relação ao fato investigado, que hão de ser especificadas no máximo possível com base em elementos identificativos e contextuais atinentes ao possível ilícito.

III – A transferência de dados às autoridades requerentes há de ocorrer unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.

IV – Cumpre à autoridade requerente providenciar ao final das investigações a inutilização dos dados obtidos de terceiros que sejam desnecessários para a continuidade do processo-crime, mediante requerimento ao juízo competente, na forma do art. 9º da Lei nº 9.296/96, com a oitiva prévia dos demais interessados.

V – Incumbe aos interessados no processo-crime, sob pena de preclusão, caso pretendam a produção de prova para a qual seja imprescindível ter acesso aos dados telemáticos de terceiros coligidos nas investigações, postular sua realização até a intimação para manifestar-se sobre a inutilização dos dados, de modo fundamentado, a fim de serem preservados os elementos imprescindíveis à diligência.

VI – É necessário para o oferecimento da denúncia que o dado telemático, possivelmente aleatório, seja corroborado por outros elementos colhidos na investigação.

— Parecer pelo provimento parcial do recurso extraordinário, com a fixação da tese e eventual modulação sugeridas.

Excelentíssima Senhora Ministra Rosa Weber,

SUMÁRIO

7. Mediação entre o direito à privacidade e o direito à memória e à verdade, como dever de investigar e punir, no afastamento do direito de dados de pessoas indeterminadas

7.1. A constitucionalidade, convencionalidade e legalidade do afastamento de sigilo de dados telemáticos de pessoas indeterminadas no âmbito de procedimentos penais

7.2. O princípio da proporcionalidade e a ponderação de direitos fundamentais na elucidação dos parâmetros para o afastamento de sigilo de dados telemáticos de pessoas indeterminadas no âmbito de procedimentos penais

7.3. Os requisitos necessários para o afastamento do sigilo de dados telemáticos de pessoas indeterminadas

7.3.1. Os registros de conexão ou acesso a aplicações de internet (art. 22 do Marco Civil da Internet)

7.3.2. A autodeterminação informativa, os princípios da finalidade, necessidade, adequação, segurança e prevenção e a obrigação de fundamentação agravada diante de dados pessoais e de conteúdo de comunicações privadas (o art. 10 do MCI)

7.4. As obrigações específicas associadas ao pedido de afastamento do sigilo nas dimensões de guarda e inutilização: os princípios da segurança, da prevenção, da responsabilização e prestação de contas.

7.4.1. As obrigações associadas atinentes à guarda das informações obtidas

7.4.2. As obrigações associadas atinentes à inutilização das informações de terceiros obtidas após o encerramento das investigações

1. RELATÓRIO

Trata-se de recurso extraordinário das sociedades empresariais Google Brasil Internet Ltda. e Google Inc., representativo do Tema 1148 da sistemática da Repercussão Geral, referente aos limites para decretação judicial do afastamento de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas.

Na origem, as recorrentes impetraram mandado de segurança visando a anular determinação judicial proferida pelo juízo originário de primeiro grau referente ao afastamento de sigilo de dados telemáticos das pessoas que, em determinado lapso temporal, pesquisaram informações no buscador da Google a partir de determinadas palavras-chave.

Argumentaram que inexistiria base constitucional e legal que subsidiasse a determinação judicial para afastamento de sigilo de dados telemáticos de forma ampla, sem a necessária individualização dos alvos. Entendem que a manutenção da determinação judicial violaria os princípios e direitos constitucionais assegurados no art. 5º, II, X e XII, da Constituição Federal e as disposições contidas nas Leis nº 9.296/96 e 12.965/2014, no Decreto nº 8.771/2016 e na Resolução CNJ nº 59/2008.

Defenderam que a fundamentação da determinação judicial em referência seria insuficiente, por não preencher os requisitos exigidos pela legislação e pela jurisprudência para o afastamento do sigilo de dados telemáticos. Entendem que haveria necessidade de fundamentação específica e adequada diante de uma determinação judicial restritiva de direito fundamental, conforme o art. 93, IX, da Constituição Federal.

Sustentaram que a determinação judicial passaria à condição de suspeitos um número indeterminado de pessoas que teriam pesquisado informações com base em determinadas palavras-chave, violando o devido processo legal e o princípio da presunção de inocência previstos no art. 5º, LIV e LVII, da Constituição Federal.

Afirmaram que a forma como foi determinado o acesso aos dados telemáticos violaria os direitos: *(i)* à privacidade, na medida em que a navegação na *web* poderia revelar informações sobre a vida privada do cidadão; e *(ii)* de acesso à informação e à liberdade de comunicação, pois geraria efeito silenciador diante da possibilidade de qualquer usuário ser envolvido em atos de investigação criminal ao buscar informações com base em determinadas palavras-chave.

Concluíram que o afastamento do sigilo de dados telemáticos das pessoas que, em determinado lapso temporal, pesquisaram informações no

buscador da Google a partir de determinadas palavras-chave seria inadequada, desnecessária e desproporcional em sentido estrito.

O Tribunal de Justiça do Estado do Rio de Janeiro denegou a segurança em acórdão assim ementado (e-STJ, fl. 83):

> *Mandado de Segurança. Decisão que decretou no curso de investigação criminal, entre outras medidas, a quebra de sigilo telemático de um conjunto não identificado de pessoas. Alegação de que o ato combatido, nesse item específico, seria genérico e aleatório, além de carente de base constitucional e legal, violando direitos constitucionais e legais, mais especificamente os previstos no artigo 5º, incisos X, XII, LVII e LIV, da Constituição da República. Direitos à privacidade e ao sigilo de dados que, por não serem absolutos, podem ser relativizados em hipóteses excepcionais, dentre as quais a de investigação criminal. Trata-se de inquérito policial instaurado a fim de apurar a prática, a autoria e a materialidade de dois homicídios qualificados e um homicídio tentado. Crimes graves e de grande repercussão. Não há ilegalidade na decisão motivada, eis que a Constituição da República prevê expressamente, sem seu artigo 5º, inciso XII, a possibilidade da quebra de sigilo de dados, por ordem judicial, desde que fundamentada. A Lei nº 9.296/96, artigo 2º, parágrafo único, permite a não indicação e qualificação dos investigados. Ausência de direito líquido e certo das Impetrantes. Denegação da segurança.*

Interposto recurso ordinário em mandado de segurança, o Superior Tribunal de Justiça negou-lhe provimento em acórdão assim ementado (e-STJ, fl. 407-411):

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.

1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. No Brasil, a Constituição Federal, no art. 5º, X, estabelece que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital.

2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, 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, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.

3. Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de aparelhos utilizados por

usuários que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio.

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

5. Os dispositivos que se referem às interceptações das comunicações indicados pelos recorrentes não se ajustam ao caso sub examine. Deveras, 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, os quais regulamentam o art. 5º, XII, da CF, não se aplica a procedimento que visa a obter dados pessoais estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet. A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados.

6. Não há como pretender dar uma interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é devidamente prevista no Marco Civil da Internet, o qual não impõe, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios.

7. Os arts. 22 e 23 do Marco Civil da Internet, em complemento ao art. 10, parágrafo único, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie - se houvesse tal obrigatoriedade legal - plenamente dedutível da complexidade e da dificuldade de identificação da autoria mediata dos crimes investigados.

8. Logo, a quebra do sigilo de dados armazenados, assim entendida a requisição mediante ordem judicial de registros de conexão e acesso à internet, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado.

9. Conforme dispõe o art. 93, IX, da CF, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação". Na espécie, tanto os indícios da prática do crime, como a justificativa quanto à utilização da medida e o período ao qual se referem os registros foram minimamente explicitados pelo Magistrado de primeiro grau.

10. Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que

pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por mais de dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam - tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional - não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados.
11. Logo, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes cometidos por agentes públicos contra as vidas de três pessoas - mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura estatal fluminense - não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada.
12. Recurso em mandado de segurança não provido.

Seguiu-se a interposição de recurso extraordinário pelas sociedades empresariais.

Nas razões, as recorrentes sustentam que o acórdão impugnado vai de encontro aos arts. 5º, X e XII; e 93, IX, da Constituição Federal.

Defendem que haveria incompatibilidade entre o núcleo essencial de proteção à privacidade e a forma como foi determinado o acesso aos dados

telemáticos (supostamente exploratória e sobre pessoas indeterminadas), pois os dados atinentes à navegação do usuário na *web* seriam resguardados pela cláusula geral de proteção da intimidade (art. 5º, X) e pela norma específica de sigilo de dados (art. 5º, XII).

Argumentam ser a medida inconstitucional, pois a determinação judicial não contemplaria de forma específica e contextual a justa causa (materialidade e indícios de envolvimento) que permitiria a relativização dos direitos e garantias fundamentais em discussão.

Sustentam que a Suprema Corte, em decisões anteriores, teria impedido ordens de afastamento de sigilo que assumissem perfil de *fishing expedition* por serem genéricas e lhes faltar causa provável (indícios de envolvimento), como seria o caso concreto.

Concluem que o acesso aos dados telemáticos das pessoas que, em determinado lapso temporal, pesquisaram informações a partir de determinadas palavras-chave seria inadequado, desnecessário e desproporcional em sentido estrito.

Nas contrarrazões, o Ministério Público do Rio de Janeiro, preliminarmente, pleiteia o não conhecimento do recurso extraordinário

diante do óbice previsto no verbete 284 da Súmula de jurisprudência do STF, da inexistência de repercussão geral e da ilegitimidade ativa das recorrentes.

No mérito, argumenta que os direitos fundamentais não seriam absolutos, pois são suscetíveis a restrições quando ponderados com outros direitos e interesses de igual importância.

Entende que as informações solicitadas envolveriam os *IPs* ou *Device IDs* daqueles que realizaram a pesquisa com os parâmetros indicados, sem a identificação do usuário ou de seus dados pessoais.

Argumenta que os dados seriam inutilizados no caso deles não guardarem relação com a investigação, preservando a privacidade do usuário.

Sustenta que a determinação judicial de afastamento do sigilo de dados telemáticos, no caso concreto, atenderia os requisitos autorizadores previstos no art. 22 da Lei nº 12.965/2014, pois foi indicada a materialidade delitiva, a necessidade da medida e o período dos registros. A inexistência de indicação da autoria seria o motivo da medida.

Conclui que a medida seria adequada, necessária e proporcional em sentido estrito.

Também nas contrarrazões, o Ministério Público Federal argumenta sobre a diferenciação do campo de incidência dos incisos X e XII do art. 5º da Constituição Federal, sendo aquele voltado à proteção dos dados em si (elementos estáticos) e este à inviolabilidade das comunicações (elementos em fluxo).

Defende que os requisitos previstos nas Leis nº 9.296/96 e 12.965/2014, que regulamentam, respectivamente, os incisos XII e X do art. 5º da Constituição Federal, teriam sido preenchidos.

Conclui que o afastamento do sigilo de dados telemáticos, no caso concreto, seria necessário, adequado e estritamente proporcional diante do interesse público na atividade de persecução penal em busca da autoria de crimes dolosos contra a vida.

O apelo extraordinário foi admitido na origem e teve reconhecida repercussão geral em acórdão assim ementado (fl. 647):

> *DIREITO CONSTITUCIONAL. DIREITO PROCESSUAL PENAL. QUEBRA DE SIGILO DE DADOS PESSOAIS. REGISTROS DE ACESSO À INTERNET E FORNECIMENTO DE IP. DECISÃO GENÉRICA. NÃO INDICAÇÃO DE PARÂMETROS MÍNIMOS PARA IDENTIFICAÇÃO DOS USUÁRIOS. NÃO DELIMITAÇÃO, ADEMAIS, DO ESPAÇO TERRITORIAL EM QUE VEICULADA A ORDEM. PROTEÇÃO À INTIMIDADE E AO SIGILO DE DADOS (ART.*

> *5º, X e XII, CF). QUESTÃO CONSTITUCIONAL. POTENCIAL MULTIPLICADOR DA CONTROVÉRSIA. REPERCUSSÃO GERAL RECONHECIDA. 1. Possui índole constitucional e repercussão geral a controvérsia relativa aos limites e ao alcance de decisões judiciais de quebra de sigilo de dados pessoais, nas quais determinado o fornecimento de registros de acesso à internet e de IPs (internet protocol address), circunscritos a um lapso temporal demarcado, sem, contudo, a indicação de qualquer elemento concreto apto a identificar os usuários. 2. Repercussão geral reconhecida.*

Vieram os autos à Procuradoria-Geral da República para parecer.

2. DELIMITAÇÃO DA CONTROVÉRSIA A SER EXAMINADA NESTE PARADIGMA.

Foi delimitado como tema para exame sob a sistemática da repercussão geral, nestes autos, os limites para decretação judicial do afastamento de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas.

O Tribunal de Justiça local e o Superior Tribunal de Justiça entenderam que a determinação judicial de afastamento do sigilo de dados telemáticos, no caso concreto, harmoniza-se com a Constituição Federal e cumpre os requisitos legais.

Para o Tribunal de Justiça, a ausência de violação à Constituição Federal fundamenta-se: *(i)* no caráter não absoluto dos direitos fundamentais,

que podem sofrer restrições diante do interesse público na atividade de persecução penal; *(ii)* na previsão contida no próprio texto constitucional, que possibilita o acesso aos dados em investigações criminais mediante ordem judicial; e *(iii)* na inexistência de violação ao direito à privacidade, pois os dados são inutilizados quando verificada sua desnecessidade para a investigação.

O Superior Tribunal de Justiça, por sua vez, aponta que a determinação judicial tem por objeto dados estáticos, que, embora sejam protegidos pelo inciso X do art. 5º da Constituição Federal, não o são pelo seu inciso XII. Tem-se, então, a desnecessidade de indicar os elementos de individualização, pois tal medida está restrita aos dados previstos no inciso XII do art. 5º da Constituição Federal.

As recorrentes sustentam *(i)* a ausência de autorização constitucional e legal que possibilite o afastamento do sigilo de dados telemáticos de indivíduos indeterminados; *(ii)* ser premissa para que se permita a medida a demonstração de indícios de envolvimento do indivíduo na prática da infração penal investigada; e *(iii)* que a manutenção da determinação judicial de acesso aos dados telemáticos de indivíduos indeterminados configura nova modalidade inconstitucional de *fishing expedition*, violando o disposto nos arts. 5º, X e XII, e 93, IX, da Constituição Federal.

O Supremo Tribunal Federal, ao reconhecer a repercussão geral, apontou a existência de decisões proferidas pela Suprema Corte em que foram delimitados os requisitos mínimos, à luz da Constituição Federal, para efetivação da quebra de sigilos de registros bancários, fiscais e telefônicos.

Concluiu que *"a proteção de dados pessoais (art. 5º, XII, CF) na Era da Informação constitui desafio à privacidade"*, havendo necessidade de *"compatibilização de quebras de sigilo de dados com os requisitos constitucionais mínimos"*.

A temática guarda complexidade e é superlativa a relevância da questão, pois, nas palavras de Vossa Excelência, Ministra Relatora:

> *Está, pois, na agenda desta Corte o enfrentamento dos maiores desafios contemporâneos à proteção da privacidade em conflito com os imperativos de segurança nacional e da eficiência do Estado, com a proliferação de sistemas de vigilância e mídias sociais, junto com a manipulação maciça de dados pessoais em redes computacionais por inúmeros agentes públicos e privados.*

3. O CONFLITO ENTRE O DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS E O DIREITO À MEMÓRIA E À VERDADE NA PERSPECTIVA DO DEVER ESTATAL DE INVESTIGAR E PUNIR.

A discussão no presente caso guarda desafios, pois em jogo os direitos à privacidade e à proteção de dados e o dever estatal de investigar e

punir, corolário do direito das vítimas e seus familiares à memória e à verdade.

Merece atenção a análise acerca da evolução da noção de privacidade ao longo do tempo, tanto no direito comparado como no ordenamento jurídico brasileiro.

Primordialmente, a privacidade vinculava-se à ideia de propriedade – *every man's house is his castle*[1]. Com as mudanças sociais e tecnológicas passou a significar o direito de ser deixado só, pressupondo uma função negativa de não intervenção estatal e uma dicotomia entre as esferas privada e pública. Diante do incremento do poder de processamento da informática em que os dados passam a representar aspectos da personalidade, chega-se à noção de autodeterminação informativa.

No ordenamento jurídico brasileiro, a Constituição Federal ocupou-se da privacidade fazendo menção específica a determinados aspectos de sua proteção, prevendo a inviolabilidade do sigilo das comunicações telefônicas, telegráficas e de dados (art. 5, X e XII). A técnica legislativa adotada e os pressupostos da privacidade em sua acepção do direito de ser deixado só, conjuntamente, influenciaram uma interpretação em que os dados pessoais seriam protegidos em relação à sua comunicação e não ao seu conteúdo em si.

[1] Decisão proferida por Sir Cook no Semayne's Case, julgado em 1603.

Diante da nova conjuntura social, a jurisprudência do Supremo Tribunal Federal, notadamente no julgamento para referendar a liminar concedida na ADI 6387, reconheceu a inexistência de dados insignificantes e, por isso, apontou para a existência de um direito à proteção de dados, assegurado por mecanismos de salvaguarda revelados por normas de proteção e normas de organização e procedimento.

Daí a importância de análise conjunta e integrada das previsões em relação ao tema do microssistema jurídico protetivo dos dados e comunicações, no qual se destacam três leis – a Lei nº 9.296/96, a Lei nº 12.965/2014 e a Lei nº 13.709/2018.

Esses diplomas legislativos hão de ser articulados com o direito à memória e à verdade das vítimas de crimes e seus familiares e com as exigências decorrentes dos deveres de investigar e punir do Estado, dentro de uma acepção que consagra o Direito Penal também como instrumento para a proteção a direitos fundamentais.

Dessa composição surgem os critérios que mediam o aparente conflito, no contexto do afastamento do sigilo de dados de pessoas indeterminadas, entre direito à privacidade e direito à memória e à verdade na perspectiva do dever de investigar e punir.

Essa harmonização aponta para a constitucionalidade, convencionalidade e legalidade da medida, desde que previstos mecanismos de salvaguarda.

Estes incluem normas protetivas, representadas pelos requisitos para o deferimento do acesso aos dados, calibrados consoante a sensibilidade da informação disponibilizada e o contexto investigativo; e normas de organização e procedimento, que estabelecem obrigações associadas ao acesso às informações, notadamente ligadas à transferência, guarda e inutilização dos dados de terceiros obtidos e a seu emprego no contexto do processo criminal.

A seguir, cada um dos pontos acima descritos será aprofundado.

4. O DIREITO À PRIVACIDADE NO DIREITO COMPARADO.

4.1. A experiência estadunidense com o direito à privacidade.

É especialmente relevante, na definição dos limites do direito à privacidade na óptica digital, a experiência dos Estados Unidos da América, notadamente pela ligação profunda entre as normas do país e a prática das grandes empresas de tecnologia.

No contexto do Direito Estadunidense, como referido por Louis Brandeis e Samuel Warren no artigo *The Right to Privacy*[2], a noção de privacidade afastou-se da ideia de propriedade, que havia de ser protegida contra invasões, e passou a significar o direito de ser deixado só (*right to be let alone)* e a ter como paradigma a ausência de interação entre os indivíduos (*zero-relationship*).[3]

O direito à privacidade passou a pressupor uma função negativa de não intervenção estatal e uma dicotomia entre as esferas privada e pública, em que o titular do direito poderia retrair aspectos de sua vida do domínio público.[4]

Desde 1890, a Suprema Corte estadunidense proferiu importantes decisões sobre o direito à privacidade, consolidando-o e adaptando-o diante dos avanços tecnológicos e das mudanças ocorridas na sociedade. Historicamente, e na perspectiva do direito à privacidade mais relevante ao

---

2 WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Civilistica.com**. Rio de Janeiro, a. 2, n. 3, jul.-set./2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/127/97. Acesso em 7 de julho de 2021.

3 Edward Shils aponta que "*privacy is a 'zero-relationship' between two persons or two groups or between a group and a person. It is a 'zero-relationship' in the sense that it is constituted by the absence of interaction or communication or perception within contexts in which such interaction, communication, or percption is practicable*". (SHILS, Edward. Privacy: its constitution and vicissitudes. Disponível em: https://scholarship.law.duke.edu/lcp/vol31/iss2/4. Acesso em 7 de julho de 2021.

4 BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** São Paulo: Editora Gen, 2019, p. 95. (livro eletrônico).

presente caso, cumpre em especial examinar a evolução jurisprudencial em torno da Quarta Emenda à Constituição dos EUA[5].

4.1.1. A evolução jurisprudencial em torno da Quarta Emenda à Constituição dos EUA.

A Quarta Emenda foi formulada com dois objetivos distintos, porém correlacionados. A primeira parte coíbe a realização de buscas e apreensões irrazoáveis, independentemente da existência de mandado judicial; e a segunda parte requer a prévia obtenção de mandado judicial, fundado em causa provável, para assegurar a constitucionalidade das buscas e apreensões.

A evolução da jurisprudência da Suprema Corte dos Estados Unidos, ao interpretar os termos da Quarta Emenda, contempla entendimentos absolutamente antagônicos. Passa da fase da *property-based approach*, pela Era *Boyd* e a inadmissibilidade da *mere evidence rule*, avançando

[5] Eis o texto original do dispositivo: "*Amendment IV - The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*" Sobre o tema exposto a seguir, vide LEGAL INFORMATION INSTITUTE. *Amendment IV. Search and Seizure*. Disponível em: https://www.law.cornell.edu/constitution-conan/amendment-4. Acesso em 13 de outubro de 2021.

pela regulação de *business information* e pela disciplina de *required records* até o total declínio de *Boyd*, chegando à *reasonable expectation of privacy*.

Nesse ínterim, a SCOTUS vem avançando na consolidação da exigência de mandado, com demonstração de causa provável (*probable cause)*, para fim de controle da intervenção estatal na privacidade dos cidadãos.

O que se chama de enquadramento da expectativa razoável de privacidade (*reasonable expectation of privacy framework)* opera-se, conjuntamente, por expectativas objetiva e subjetiva.

A expectativa objetiva se refere à ideia de que o espaço que contém a informação ou se realiza a atividade é costumeiramente reconhecido como privado ou deveria sê-lo reconhecido como tal por sua natureza; ou, ainda que não seja entendido como privado em qualquer contexto, seja percebido como protegido contra determinados tipos de inspeções não usuais (por exemplo, como uso de tecnologia).

A expectativa subjetiva se refere à ideia de que o que se inspeciona não está previsivelmente exposto a público, ou que haja esforços para ocultação, indicando que a pessoa teve a intenção de manter a privacidade.

A exigência de mandado (*warrant requirement)* é, portanto, uma regra de garantia de constitucionalidade das buscas e apreensões, calcada na

obtenção de mandado judicial prévio à realização da diligência intrusiva no direito à privacidade, com estabelecimento de causa provável, e baseado em juramento ou afirmação (*oath* ou *affirmation)* de que os fatos descritos no requerimento formulado à Corte são verdadeiros.

O caso *Katz v. United States* (1967), em relação ao caso *Olmstead v. United States* (1928), é emblemático ao demonstrar a evolução na percepção do que é privacidade diante das ameaças tecnológicas.[6]

A Suprema Corte estadunidense, por exemplo, considerou que a Quarta Emenda protege tanto pessoas e propriedades como dados em relação aos quais se tem uma expectativa razoável de privacidade, sendo exigível mandado judicial para grampear telefones.[7]

No recente caso *Carpenter v. United States* (2018), foi analisado o impacto da era da informação sobre as proteções e garantias constitucionais, também demonstrando evolução na noção de privacidade e necessidade de

---

[6] No caso *Olmstead v. United States*, a Suprema Corte norte-americana considerou inaplicável a Quarta Emenda e desnecessário o mandado judicial para grampear telefones. Na ocasião, Louis Brandeis, agora membro da Suprema Corte, proferiu seu voto de divergência e foi vencido. No caso *Katz v. United States*, a Suprema Corte norte-americana alterou seu entendimento (*overruling*); passou a considerar aplicável a Quarta Emenda e, assim, exigível mandado judicial para grampear telefones.

[7] Chief Justice Harlan criou o teste da "Expectativa Razoável de Privacidade" consistente em duas partes: (i) *"an individual has exhibited an actual (subjective) expectation of privacy"*; e (ii) *"the expectation is one that society is prepared to recognize as reasonable"*.

proteção de dados em relação aos casos *United States v. Miller* (1976) e *Smith v. Maryland* (1979).

No julgamento, a Suprema Corte estadunidense sustentou limitações à denominada *Third-party Doctrine*[8], diante da abrangente coleta automática de dados, que podem detalhar a vida privada e a personalidade do indivíduo.[9]

Concluiu que seria necessário mandado judicial para acesso aos dados de localização de aparelho celular por meio do chamado *cell-site location information* (CSLI)[10], pois haveria expectativa razoável de privacidade pelo indivíduo em relação aos seus dados de geolocalização.

Nesse percurso evolutivo, a privacidade passou a assumir novo perfil ao mudar sua matriz de "pessoa-informação-sigilo" para "pessoa-informação-circulação-controle".[11]

[8] A *Third-party Doctrine* sustenta que a comunicação voluntária de informações a terceiros obsta uma expectativa razoável de privacidade em relação a elas, afastando a proteção garantida pela Quarta Emenda.

[9] Para Chief Justice Roberts: *"Smith and Miller after all, did not rely solely on the act of sharing. Instead, they considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate expectation of privacy concerning their contents".* (trecho do voto disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. Acesso em 6 de agosto de 2021.

[10] A localização do aparelho celular pode ser feita por meio do CSLI ou GPS. O CSLI caracteriza-se pela informação coletada por torres de transmissão, que podem identificar a localização aproximada do aparelho celular utilizando a triangulação.

[11] RODOTÀ, Stefano. **A vida na sociedade da vigilância**. Rio de Janeiro: Renovar, 2008, p. 93.

4.1.2. A normativa estadunidense em torno da obtenção de dados telemáticos junto aos servidores de internet.

A obtenção de material investigativo-probatório junto aos provedores de internet (*network service providers*) nos Estados Unidos submete-se ao regramento do *The Stored Communication Act*, *U.S.C.* §§ 2701-2712, e se opera por três meios conforme a categoria de informações pretendida: *subpoena*, *court order* ou *search warrant*.

Simples *subpoena*, vale dizer, mera intimação judicial do provedor ou notificação administrativa autorizada por lei federal ou estadual, é suficiente para a obtenção de dados básicos de assinatura e sessão (“*basic subscriber and session information”)* consistentes em: (a) nome; (b) endereço; (c) registros de conexão telefônica local e de longa distância, ou registros de tempo e durações das sessões; (d) tempo de serviço (incluindo data de início) e tipos de serviço utilizados; (e) número de telefone ou instrumento ou outro número ou identidade de assinante, incluindo qualquer endereço de rede temporariamente atribuído; e (f) meio e fonte de pagamento para tal serviço (incluindo qualquer cartão de crédito ou número de conta bancária). Na categoria *temporarily assigned network address* está incluída a informação relativa ao *Internet Protocol* (IP).

A ordem judicial (*court order)* é necessária para a obtenção de registros de comunicações eletrônicas ("*records of eletronic communications"),* categoria genérica que contempla todas as informações para além das de *basic subscriber* e *session information*, exceto aquelas referentes ao conteúdo das comunicações.

Nessa categoria, inclui-se, por exemplo, a integralidade do *account log* e todos os *transactional records*. Para a obtenção dessa ordem judicial, o pedido dever conter fatos específicos e articuláveis que demonstrem motivos razoáveis (*reasonable grounds*) para se acreditar que a informação seja relevante e material para a investigação em curso.

Já para acesso ao conteúdo total das comunicações é obrigatório o atendimento a exigência de mandado judicial (*warrant)*, com atendimento dos requisitos de comprovação de causa provável e particularidade descritiva do mandado, decorrentes da Quarta Emenda da *Bill of Rights*.[12]

[12] Um capítulo especial da discussão acerca do direito à privacidade na perspectiva telemática, ainda em curso nos Estados Unidos, diz com os chamados "*geofence warrants*". Trata-se do requerimento, sem autoria precisa, para a coleta de dados de histórico de localização a partir de especificações de área geográfica e faixa de tempo.

A SCOTUS ainda não se posicionou quanto à constitucionalidade dessa prova, todavia, as Cortes de outros níveis não a têm considerado inconstitucional *per se*. Nesse tema, está em curso na *District Court for the Eastern District of Virginia, Richmond Division,* o caso *United States of America v. Okello T. Chatrie*, no qual se discute a constitucionalidade dos *geofence warrants* ante a Quarta Emenda. Nele, a empresa *Google LLC*, ao apresentar *brief of amicus curiae*, faz questão de registrar que não se manifesta nos autos em suporte à acusação ou à defesa, ou seja, não considera ela própria inconstitucionais *per se* os *geofence warrants.* Sustenta apenas que os dados de histórico de localização dos usuários só poderiam ser

4.1.3. O processo penal estadunidense e o conceito de *fishing expedition*.

A expressão *fishing expedition* em direito estadunidense deriva de interpretação da Suprema Corte acerca do uso adequado da *Rule 17*, estabelecida nas *Federal Rules of Criminal Procedure*.

As Regras Federais de Processo Penal (*Rule 17(c)(1))* estabelecem a possibilidade de obtenção de livros, papéis, documentos ou outros objetos, diretamente de pessoas ou empresas, mediante intimação da Corte (*subpoena*), para apresentação em juízo, com subsequente autorização de acesso às partes ao seu conteúdo, total ou parcial.

A fim de evitar que a regra se subverta em subterfúgio para excessos, a própria normativa federal – *Rule 17(c)(2)* – estabelece que a ordem

obtidos por meio de *warrant.* Significa dizer que, nos Estados Unidos, a posição processual da Google LLC, em situação análoga, não é de suporte à tese defensiva de inconstitucionalidade das investigações em contexto de *geofence*, ou seja, utilizando-se de dados de localização de pessoas indeterminadas.

Eis o trecho do *brief of amicus curiae* (p. 24)*:* "*Google takes no position on whether the warrant in this case satisfies the requirements of probable cause and particularity or, if it does not, whether suppression is appropriate. But in resolving those questions, the Court should take into account the complete factual and legal context, and it should hold that both the SCA and the Fourth Amendment require the government* to *obtain a warrant to compel Google to search LH information via a geofence search.*". *Brief of Amicus Curiae Google, LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence From a "Geofence" General Warrant* (ECF No. 29), Chatrie, 3:19-cr-00130, ECF No. 59-1 at *8 (Dec. 20, 2019). Disponível em "https://www.nacdl.org/getattachment/723adf0b-90b1-4254-ab82-e5693c48e951/191220-chatrie-google-amicus-brief.pdf". Acesso em 13 de outubro de 2021.

judicial pode ser revogada ou alterada em sua extensão desde que, mediante petição (*motion*) tempestiva, seja demonstrada irrazoabilidade ou abuso.

O *leading case* na temática é *Bowman Dairy Co. v. United States*, 341 U.S. 214 (1951)[13], que estabeleceu que a intimação para a produção de evidências (*"subpoena duces tecum")* não pode ser usada como meio de imposição de revelação integral do acervo de evidências entre as partes, tratando-se unicamente de meio de conferir celeridade ao processo, por possibilitar tempo de análise de determinado material probatório antes do julgamento.

Em caso de referência sobre o assunto, *United States v. Nixon*, 418 U.S. 683 (1974), a Suprema Corte validou *subpoena* concedida pela *District Court for the District of Columbia* que obrigava a apresentação em juízo de fitas, memorandos, papéis, transcrições e outros escritos relativos a encontros do então Presidente Richard Nixon com certos membros de sua equipe da Casa Branca e apoiadores políticos, todos acusados de crimes federais.

O caso *Nixon* confirmou o teste para adequação com a Rule 17 (c), contemplando quatro requisitos: (1) os documentos ou objetos serem material evidenciário relevante; (2) que não possam ser obtidos por outro meio com razoável antecedência ao julgamento pelo exercício de devida diligência pelo

[13] Disponível em "https://supreme.justia.com/cases/federal/us/341/214/". Acesso em 14 de outubro de 2021.

requerente; (3) que a parte não possa se preparar adequadamente para o julgamento sem o fornecimento e a análise prévia do material, e se a sua não obtenção tenda a postergar irrazoavelmente o julgamento; e (4) a pretensão seja de boa-fé e não intencionada como ampla "*fishing expedition*".

Nesse cenário, a Suprema Corte entendeu que competia ao *Special Prosecutor* o ônus de especificar a relevância do material pretendido para o caso; a sua admissibilidade no acervo probatório dos autos conforme os ditames das *Federal Rules of Evidence*; e a especificidade da pretensão (vale dizer, qual rol de conversas, em parâmetros limitados de tempo, pertinentes a fatos específicos em apuração).

Ao fim, a SCOTUS concluiu que a privacidade e a confidencialidade do Presidente dos Estados Unidos não prevalecem sobre as demandas de direito fundamental concernentes ao devido processo legal, eis que sem acesso pela promotoria a fatos específicos, a ação penal poderia ser totalmente frustrada.[14]

[14] "*In the communications of his office is general in nature, whereas the constitutional need for production of relevant evidence in a criminal proceeding is specific and central to the fair adjudication of a particular criminal case in the administration of justice. Without access to specific facts, a criminal prosecution may be totally frustrated. The President's broad interest in confidentiality of communications will not be vitiated by disclosure of a limited number of conversations preliminarily shown to have some bearing on the pending criminal cases.*
We conclude that, when the ground for asserting privilege as to subpoenaed materials sought for use in a criminal trial is based only on the generalized interest in confidentiality, it cannot prevail over the fundamental demands of due process of law in the fair administration of criminal justice. The generalized assertion of privilege must yield to the demonstrated, specific

Em síntese, a noção de *fishing expedition* no Direito Estadunidense liga-se ao abuso de prerrogativas de produção de prova, fora de parâmetros específicos que conectem as informações buscadas ao fato criminoso e da teleologia que informa a possibilidade de uso dos referidos poderes.

4.2. A experiência alemã com o direito à privacidade.

Um outro marco relevante, em termos de Direito Comparado, é o desenvolvimento do conceito de autodeterminação informativa pelo Tribunal Constitucional Alemão.

Reclamações constitucionais foram ajuizadas contra a Lei do Censo alemão de 1983 sob a alegação de que ela violaria o direito ao livre desenvolvimento da personalidade dos reclamantes diante do método de coleta de informações que seria utilizado e o destino a ser dado a elas, impedindo o indivíduo de conhecer o uso efetivo que seria feito de suas informações.[15]

A Corte alemã reconheceu *"ser incompatível com a dignidade humana e o direito ao livre desenvolvimento da personalidade que o indivíduo não seja protegido*

need for evidence in a pending criminal trial." United States v. Nixon, 418 U.S. 683 (1974). Disponível em "https://supreme.justia.com/cases/federal/us/418/683/#tab-opinion-1950928". Acesso em 14 de outubro de 2021.

[15] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, n.p. (livro eletrônico).

contra uma ilimitada coleta, armazenamento, aproveitamento, transferência e divulgação de seus dados pessoais".[16] [17]

Haveria de ser preservado o direito do indivíduo manter o controle sobre os próprios dados pessoais a fim de evitar violação ao direito da personalidade, pois eles *"estariam abrangidos no âmbito de proteção do direito à autodeterminação informativa e que somente o próprio interessado poderia decidir sobre sua coleta, processamento e transmissão".*[18]

> *Com isso, um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados 'insignificantes' no contexto do processamento eletrônico de dados. O fato de informações dizerem respeito a processos íntimos não decide por si só se elas são sensíveis ou não. É muito mais necessário o conhecimento do contexto de*

---

16 SARLET, Ingo Wolfgang; MITIDIERO, Daniel; MARINONI, Luiz Guilherme. **Curso de direito constitucional**. 9. ed. São Paulo: Saraiva, 2020, p. 637. (livro eletrônico)

17 *"Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso"*. (SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.** Konrad-Adenauer-Stiftung, 2005, p. 237. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf. Acesso em 8 de julho de 2021).

18 MENDES, Laura Schertel Ferreira. **Autodeterminação informativa: a história de um conceito.** Disponível em: https://periodicos.unifor.br/rpen/article/view/10828. Acesso em 8 de julho de 2021.

> *utilização, para que se constate a importância do dado em termos de direito da personalidade".*[19]

A decisão do Tribunal Constitucional Alemão é paradigmática ao delinear um direito implícito à autodeterminação informativa, ao conjugar o princípio da dignidade da pessoa humana e o direito ao livre desenvolvimento da personalidade. Assim, no tratamento do direito à privacidade o Tribunal afastou-se da dicotomia entre as esferas privada e pública.

Como o Tribunal pontuou, o direito à autodeterminação informativa não assegura ao indivíduo um controle absoluto sobre os seus dados. Há de se tolerar eventuais limitações ao seu direito em favor do interesse geral diante de sua inserção no meio social e da responsabilidade comunitária.[20]

Em síntese, a experiência do Direito Comparado sinaliza, portanto, crescente preocupação com a possibilidade de coleta e armazenamento indiscriminado de dados, seja pelo Estado, seja por terceiros, na linha do reconhecimento de um direito à autodeterminação informativa. Todavia,

---

[19] SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.** Konrad-Adenauer-Stiftung, 2005, p. 239.

[20] SARLET, Ingo Wolfgang. **Fundamentos constitucionais: o direito fundamental à proteção de dados**. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otávio Luiz (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 50. (livro eletrônico).

contemplam-se explicitamente exceções, na linha das restrições legítimas aos direitos fundamentais, notadamente aquelas ligadas à preservação de direitos fundamentais de terceiros. Os níveis de acesso são matizados consoante a sensibilidade dos dados obtidos e o interesse premente na sua obtenção.

5. O DIREITO À PRIVACIDADE NO ORDENAMENTO JURÍDICO BRASILEIRO.

5.1. O perfil constitucional do direito à privacidade e sua leitura pela jurisprudência do Supremo Tribunal Federal.

O afastamento de sigilo de dados se insere em um contexto em que, para obtenção de informações, o desenvolvimento da informática proporcionou a utilização de *big data*, consistente em um grande volume de dados, obtidos ou recebidos de diversas origens, compartilhados em alta velocidade[21].

Esse contexto foi bem explicitado pelo Ministro Ruy Rosado de Aguiar em voto proferido no REsp 22.337/RS:

> *A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações de Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida,*

[21] Conhecido como os três Vs do *Big Data*: volume, velocidade e variedade.

> *permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas, vezes sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica.*

Mais uma vez os avanços tecnológico e social desafiaram a noção de privacidade e impactaram o contexto no qual ela e os dados pessoais se relacionam[22], o que também pode ser observado no ordenamento jurídico brasileiro.

A Constituição Federal, no art. 5º, X, ocupou-se da privacidade fazendo menção específica a determinadas amplitudes do desenvolvimento de sua proteção, esferas que procuram delimitar os espaços da vida do indivíduo revelados ao público. Já no inciso XII, previu a inviolabilidade do sigilo das comunicações telefônicas, telegráficas e de dados.

A técnica legislativa utilizada pelo constituinte, a teoria das esferas e a função negativa de não intervenção estatal, todas conjuntamente

[22] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, n.p. (livro eletrônico).

influenciaram uma interpretação em que os dados pessoais seriam protegidos em relação à sua comunicação e não ao seu conteúdo em si, como apontou o Min. Gilmar Mendes em voto proferido no julgamento para referendar a liminar concedida na ADI 6387:

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

No julgamento do RE 418.416/SC, a Suprema Corte limitou o reconhecimento da proteção constitucional ao sigilo (art. 5º, XII) aos dados em comunicação (aos dados em fluxo) e não àqueles que estavam armazenados no suporte físico apreendido (dados estáticos), inexistindo violação ao dispositivo constitucional na relativização do sigilo destes.

Contudo, o Supremo Tribunal Federal, no julgamento para referendar a liminar concedida na ADI 6387, reconheceu a inexistência de dados insignificantes e, por isso, veio a entender que a segregação anteriormente adotada pela Corte poderia permitir violações à privacidade e ao sigilo de dados por meio da utilização abusiva de informações gravadas em bancos de dados.

Estavam em julgamento dispositivos da Medida Provisória nº 940/2020, que dispunha sobre o compartilhamento de dados por empresas de telecomunicações com a Fundação Instituto Brasileiro de Geografia e Estatística.

A Suprema Corte, então, apontou para a existência de um direito à proteção de dados e a necessidade de ser definido *(i)* mecanismos para proteção dos dados; *(ii)* o modo como eles serão utilizados; e *(iii)* a finalidade que se quer atingir ao manipulá-los, possibilitando avaliar a adequação, necessidade e proporcionalidade em sentido estrito.[23]

Ao final, reconheceu a desnecessidade, inadequação e desproporcionalidade da medida, pois *(i)* a finalidade estaria sendo atingida por outros meios menos intrusivos à privacidade e *(ii)* inexistiria previsão de mecanismos mínimos para proteção e anonimização dos dados coletados.

---

[23] Sobre o objeto de proteção constitucional do direito à proteção de dados, Laura Schertel Mendes aponta que *"é o processamento e a utilização dos dados e informações pessoais em geral. A relevância jurídica reside menos nos dados em si, mas no processo de coleta, armazenamento, utilização ou transferência, a partir do qual são extraídas informações pessoais a serem utilizadas em um determinado contexto para determinados fins. Assim, entra em ação a proteção constitucional se a informação for usada para uma finalidade que cause riscos aos cidadãos, ou para fins considerados ilícitos a priori (como é o caso, por exemplo, de bancos de dados criados para fins discriminatórios). Assim, somente uma análise do contexto do uso das informações (ou das hipóteses previstas para a sua utilização), do conteúdo da informação, da finalidade de sua utilização e dos riscos envolvidos para o cidadão pode determinar a legitimidade de uma ação de tratamento de dados ou informações pessoais"* (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, n.p., livro eletrônico).

A partir desses novos eixos definidores dos direitos à privacidade e à proteção de dados, torna-se possível avançar na identificação do conteúdo da dupla dimensão, subjetiva e objetiva, desses direitos. Em voto proferido no julgamento para referendar a liminar concedida na ADI 6387, o Min. Gilmar Mendes destacou que:

> *A dimensão subjetiva impõe que o legislador assuma o ônus de apresentar uma justificativa constitucional para qualquer intervenção que de algum modo afete a autodeterminação informacional. Nesse aspecto, a autodeterminação do titular sobre os dados deve ser sempre a regra, somente afastável de maneira excepcional. A justificativa constitucional da intervenção deve ser traduzida na* ***identificação da finalidade*** *e no* ***estabelecimento de limites*** *ao tratamento de dados em padrão suficientemente específico, preciso e claro para cada área.*
> *(…)*
> *Já em uma* ***dimensão objetiva****, a afirmação do direito fundamental à proteção de dados pessoais impõe ao legislador um verdadeiro dever de proteção (Schutzpflicht) do direito à autodeterminação informacional, o qual deve ser colmatado a partir da previsão de mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento (Recht auf Organisation und Verfahren) e normas de proteção (Recht auf Schutz).*

Tem-se que os direitos à privacidade e à proteção de dados, seja em seus *status* de direito de defesa, seja em suas dimensões de intervenção ativa, constituem elementos concretizadores do princípio da dignidade da pessoa humana e dos direitos à liberdade e à autodeterminação. Portanto, sua proteção passa por uma perspectiva teleológica e contextualizada de seus

limites, a ser densificada a partir de mecanismo de salvaguarda traduzidos em normas de proteção e de organização e procedimento.

5.2. A legislação infraconstitucional sobre proteção e tratamento de dados.

O art. 5º, XII, da Constituição Federal prevê a inviolabilidade das comunicações telefônica, telegráfica e de dados, protegendo o processo comunicativo intersubjetivo e seu conteúdo do conhecimento por parte do Estado ou de terceiros.

Previu também a possibilidade de afastamento do sigilo das comunicações e a necessidade de cumprimento de dois requisitos constitucionais: *(i)* ordem judicial (reserva de jurisdição); e *(ii)* destinação dos elementos para a investigação criminal ou para a instrução processual penal.

No ordenamento jurídico brasileiro, destacam-se três leis inseridas no microssistema de proteção de dados e comunicações: a Lei nº 9.296/96, a Lei nº 12.965/2014 e a Lei nº 13.709/2018.

Na análise desse microssistema para definição dos parâmetros de proteção adequados, ainda há de se distinguir entre o afastamento do sigilo das comunicações, em fluxo, e o acesso a banco de dados ou o tratamento de dados.

Em relação aos dados em fluxo, a Lei nº 9.296/96 disciplina a interceptação da comunicação telefônica, que será admitida quando houver indícios razoáveis de autoria ou participação em infração penal; quando a prova não puder ser feita por outros meios disponíveis; e quando o fato investigado constituir crime punido com pena de reclusão.

A interceptação da comunicação telefônica pressupõe a existência de processo comunicativo entre dois interlocutores: *(i)* o sujeito passivo, com indicação razoável de autoria ou participação em infração penal (art. 2º, I); e *(ii)* indivíduo que pode não ter qualquer relação com o fato investigado.

Observa-se que mesmo a interceptação envolverá qualquer interlocutor que se comunique com o sujeito passivo, atingindo número indeterminado de pessoas que estarão abrangidos pela autorização judicial.

Na situação em que existir a interceptação da comunicação de interlocutores não envolvidos com o fato investigado ou interceptação de conteúdo que não tenha relação com o fato investigado, há de ser decretado o sigilo do conteúdo interceptado (art. 8º) e posteriormente providenciada a sua inutilização (art. 9) para preservar a privacidade dos interlocutores.

Tem-se, ainda, que a interceptação da comunicação telefônica possui caráter subsidiário, e sua autorização há de considerar a gravidade do

fato investigado. Ela será admitida quando inexistir, à época da autorização judicial, outros meios idôneos e menos invasivos disponíveis para a investigação do fato punido com pena de reclusão e respectiva autoria (art. 2º, II e III).

Os critérios atinentes à interceptação da comunicação telefônica sinalizam parâmetros relevantes para a presente discussão na medida em que autorizam intervenção até mais gravosa do que o acesso a informações contidas em banco de dados. Ainda que em caráter subsidiário e restrito, tal intervenção é admitida e assegurada no contexto do dever de investigar e punir e do direito penal como sistema de proteção dos direitos fundamentais e bens jurídicos mais caros à sociedade.

Já a Lei nº 12.965/2014, conhecida como Marco Civil da Internet (MCI), inaugurou disciplina específica para os direitos e garantias do indivíduo nas relações estabelecidas no âmbito da internet e fundamenta-se em três pilares: *(i)* a neutralidade da rede; *(ii)* a liberdade de expressão; e *(iii)* a privacidade e a proteção de dados dos usuários.

Diante dos dispositivos que tratam da privacidade e da proteção de dados, tem-se a autodeterminação informativa como parâmetro normativo do MCI, pois *"todas as normas desembocam na figura do cidadão-usuário para que ele,*

uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento".[24]

O MCI dispõe sobre a necessidade de consentimento do usuário para coleta, uso, armazenamento e tratamento de seus dados e a transferência desses dados a terceiros (arts. 7º, VII e IX; e 16, II); prevê que o consentimento haverá de ser livre, expresso e informado, com especificação da finalidade que justifique a coleta de dados (art. 7º, VI, VIII, IX e XI); e, por fim, detalha a possibilidade de o usuário requerer a exclusão definitiva de seus dados (art. 7º, X).

O MCI também traz a possibilidade de afastamento do sigilo de dados e exceção ao seu não fornecimento, que estão previstos conjuntamente nos arts. 10 e 22.

No art. 10 há duas situações: *(i)* o fornecimento de registros de conexão e de acesso, de forma autônoma ou associadas a dados pessoais, mediante ordem judicial, observando o disposto no art. 22 (art. 10, § 1º)[25]; e

[24] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 130. (livro eletrônico).

[25] Art. 10. § 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.

(ii) o acesso a dados cadastrais (qualificação pessoal, filiação e endereço) pelas autoridades administrativas, na forma da lei (art. 10, § 3º)[26].

Usualmente, o motivo para o pedido na primeira situação é a própria tentativa de identificação do usuário ou do terminal. O fornecimento dos registros e dados busca proporcionar a descoberta da identidade do usuário que, em algum momento, fez uso de serviços de internet ou acessou aplicações de internet por meio de determinado terminal.

A ordem judicial haverá de preencher adequadamente os requisitos presentes no art. 22, parágrafo único, do MCI:

> *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.*

A inexistência de previsão, no referido artigo, de obrigatória demonstração de indícios de autoria tem razão de ser. Os autores de ilícitos

[26] Art. 10. § 3º O disposto no *caput* não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

cibernéticos, por exemplo, dificilmente revelam sua real identidade a fim de evitar responsabilização. Tal parâmetro, se exigido, poderia inviabilizar o cerne das investigações de crimes cibernéticos, em que o elemento a ser elucidado é exatamente a autoria.

Quanto à segunda previsão, contida no art. 10, § 3º, o acesso pelas autoridades administrativas prescinde de ordem judicial e, por isso, há de observar os requisitos previstos no art. 11 do Decreto nº 8.771/2016, diante da vedação em relação a pedidos coletivos genéricos ou inespecíficos:

> *Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.*
> *§ 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados.*
> *§ 2º São considerados dados cadastrais:*
> *I - a filiação;*
> *II - o endereço; e*
> *III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.*
> *§ 3º Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.*

Diferentemente da primeira situação – em que se pode buscar a identificação do usuário, sendo desnecessária a individualização –, no caso da

autoridade administrativa solicitar o acesso aos dados cadastrais, haverá de especificar o indivíduo titular dos dados solicitados.

Para além das situações e critérios previstos nos arts. 10 e 22 do MCI, há de se atentar para o art. 23[27], que prevê a necessidade de adotar mecanismos com o objetivo de garantir o sigilo das informações recebidas e a preservação da privacidade do usuário.

Aqui também os critérios atinentes à requisição judicial de registros de acesso e de conexão fornecem critérios relevantes para a presente discussão, na medida em que trazem parâmetros contextualizados para o acesso a bancos de dados, menos restritivos se comparados àqueles presentes na Lei nº 9.296/96.

A limitação à privacidade e à proteção de dados permitida pela Lei nº 9.296/96 é mais ampla e intensa do que a permitida pela Lei nº 12.965/2014. Naquela, a autoridade tem acesso aos dados dos interlocutores e ao conteúdo da comunicação em fluxo; ao passo que nesta a autoridade terá acesso aos números de *IPs* e de *Device IDs* sem indicação de qualificação dos usuários e de conteúdos das mensagens trocadas, ou outras informações identificativas, em ambos os casos já armazenadas.

[27] 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.

Com a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), os dados pessoais ganharam nova dimensão de proteção e as operações de tratamento desses dados hão de observar o disposto nos arts. 7º e 11. Trata-se de regime jurídico voltado a regular a circulação de dados pessoais diante do atual estágio em que a sociedade e a informática se encontram.[28]

Apesar do art. 4º, III, *d*, da LGPD[29] excetuar a sua aplicação quando envolver tratamento de dados pessoais realizados para fins exclusivos de atividades de investigação e repressão de infrações penais, os princípios previstos na própria lei (art. 6º) são referências relevantes que contribuem para a presente discussão, notadamente os da finalidade, adequação, necessidade, segurança, prevenção, responsabilização e prestação de contas[30]:

[28] ABREU, Jacqueline de Souza. **Tratamento de dados pessoais para segurança pública**: contornos do regime jurídico pós-LGPD. In: n: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otávio Luiz (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 592. (livro eletrônico).

[29] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
III – realizados para fins exclusivos de:
d) atividades de investigação e repressão de infrações penais.

[30] Nessa linha, recentemente, a Comitê Jurídico Interamericano (CJI) atualizou os princípios que tratam da gestão de dados pessoais, na perspectiva do Sistema Interamericano de Direitos Humanos. Observa-se que os direitos à privacidade e à proteção de dados também são protegidos pelo sistema interamericano – dentro de uma sistemática mais ampla de uma proteção de dados –, que prevê princípios que se coadunam com aqueles apresentados pela LGPD: (i) finalidade legítima e legal; (ii) transparência e consentimento; (iii) pertinência e necessidade; (iv) tratamento e conservação limitada; (v) confidencialidade; (vi) segurança dos dados; (vii) exatidão dos dados, acesso; (viii) acesso, retificação, cancelamento, oposição e portabilidade; (ix)

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

---

dados pessoais sensíveis; (x) responsabilidade; (xi) fluxo transfronteiriço dos dados e sua responsabilidade; (xii) exceções; e (xiii) autoridade de proteção de dados.

Desse tríduo legal, extrai-se a inexistência, no ordenamento jurídico, de impeditivo para que medidas investigativas em contexto criminal atinjam pessoas indeterminadas.

Em contrapartida, são previstas medidas garantidoras de sigilo e proteção, proporcionais à intensidade da medida interventiva em questão e às informações que passam a estar disponíveis, consoante as expectativas razoáveis de sigilo em cada contexto informacional.

6. O ESTADO DEMOCRÁTICO E O DIREITO À MEMÓRIA E À VERDADE DAS VÍTIMAS DE CRIMES E SEUS FAMILIARES: O DEVER DE INVESTIGAR E PUNIR E O AFASTAMENTO DO SIGILO DE DADOS.

A Constituição Federal estabeleceu, no art. 1º, o perfil político constitucional brasileiro como o de um Estado Democrático de Direito. Dessa definição decorre toda a ordem jurídico-principiológica do país.

A doutrina leciona que Estado Democrático de Direito é mais do que simplesmente Estado de Direito. Enquanto este assegura a igualdade formal entre as pessoas, aquele é investido de maior conteúdo social, proclamando não apenas a submissão de todos ao império da mesma lei, mas

com normas e princípios dotados de razoabilidade e adequação social que propiciem a construção de uma sociedade livre, justa e solidária.[31]

O conteúdo de adequação e razoabilidade e a busca pela efetivação da justiça, tendências do Estado Democrático de Direito, têm sua incidência também no direito penal, que há de ser justo e democrático, com normas que se balizem nos valores fundamentais da sociedade brasileira.

Em um Estado Democrático de Direito, o Direito Penal, ao exercer sua função primordial de proteção dos bens jurídicos essenciais ao indivíduo e à comunidade, há de se estabelecer como uma ordem de paz pública e de tutela das relações sociais, cuja missão é proteger a convivência humana, assegurando, por meio da intervenção estatal, a inquebrantabilidade da ordem jurídica.

Além de se traduzir no conjunto de normas que definem os delitos e as sanções que lhes correspondem e orientar sua aplicação, o direito penal tem sentido subjetivo, relacionado ao dever-poder de punir do Estado. Exatamente por isso, baseia-se no critério da necessidade e encontra limitações, especialmente nos princípios penais fundamentais, havendo de nortear-se, sobretudo, pelo princípio da dignidade da humana.

[31] CAPAZ, Fernando. **Curso de direito penal**. 23. ed. São Paulo: Saraiva Educação, 2019, n.p. (livro eletrônico).

A dignidade da pessoa humana, diante do qual partem inúmeros outros princípios relacionados à esfera criminal, há de orientar a formação de todo o direito penal. Qualquer norma ou interpretação que afronte o núcleo da dignidade humana mostrar-se-á incompatível com a ordem constitucional, visto que atentatória aos fundamentos do Estado Democrático de Direito.

Ao lecionar acerca dos princípios fundamentais do direito penal, a doutrina faz as seguintes ponderações sobre a dignidade da pessoa humana na perspectiva penal:

> *A noção de dignidade humana, como dado inerente ao ser humano enquanto tal, encerra, também, a promoção do desenvolvimento livre e pleno da personalidade individual, projetando-se, assim, culturalmente.*
> *Desse modo, e coerentemente com a sua finalidade maior, o Estado democrático de Direito e social deve consagrar e garantir o primado dos direitos fundamentais, abstendo-se de práticas a eles lesivas, como também propiciar condições para que sejam respeitados, inclusive com a eventual remoção de obstáculos à sua total realização.*
> *(…)*
> *A dignidade da pessoa humana – da natureza humana – antecede, portanto, o juízo axiológico do legislador e vincula de forma absoluta sua atividade normativa, mormente no campo penal.*
> *Daí por que toda lei que viole a dignidade da pessoa humana deve ser reputada inconstitucional. Assim, pode-se afirmar que, 'se o Direito não quiser ser mera força, mero terror, se quiser obrigar a todos os cidadãos em sua consciência, há de respeitar a condição do homem como pessoa, como ser responsável', pois, 'no caso de infração grave ao princípio material de justiça, de validade a priori, ao respeito à*

> *dignidade da pessoa humana, carecerá de força obrigatória e, dada sua injustiça, será preciso negar-lhe o caráter de Direito'.*
> *Observa-se, ainda, que a força normativa desse princípio supremo se esparge por toda a ordem jurídica e serve de alicerce aos demais princípios penais fundamentais. Desse modo, por exemplo, uma transgressão aos princípios da legalidade ou da culpabilidade implicará também, em última instância, uma lesão ao princípio constitucional da dignidade da pessoa humana.*[32]

Essa vinculação do direito penal ao princípio da dignidade da pessoa humana há de ter dupla acepção, balizando-se nos direitos fundamentais do acusado, bem como nos das vítimas e seus familiares e dos membros da comunidade que vivenciaram a experiência de violência.

O dever-poder de punir do Estado há de se efetivar tendo a proteção judicial como pilar do Estado Democrático de Direito, com enfoque também na vítima e seus familiares, propiciando-se aos prejudicados pela conduta criminosa amplo acesso à justiça, com os instrumentos inerentes à compreensão do ocorrido e suas consequências.

Na esteira do que significa Estado Democrático de Direito, com perspectiva na dignidade humana, incumbe ao Estado oferecer proteção judicial que assegure a devida apuração dos delitos, a punição dos responsáveis e a reparação às vítimas e sua família.

[32] PRADO, Luiz Regis. **Tratado de direito penal**: parte geral. 1. ed., v. 1, parte III. São Paulo: Revista dos Tribunais, 2017.

A jurisprudência da Corte Interamericana de Direitos Humanos reforça o entendimento de que a proteção judicial confere garantia de que a investigação e o processo ocorram de forma efetiva e que, comprovado o ilícito, sejam impostas as penas correspondentes:

> *130. En consecuencia, el artículo 8.1 de la Convención Americana, en conexión con el artículo 25.1 de la misma, confere a los familiares de las víctimas el derecho a que la desaparición y muerte de estas últimas sean efectivamente investigadas por las autoridades del Estado; se siga un proceso contra los responsables de estos ilícitos; en su caso se les impongan las sanciones pertinentes, y se reparen los daños y perjuicios que dichos familiares han sufrido. ("Caso Durand y Ugarte vs. Perú", de 16.8.2000.)*[33]

Surge daí o chamado direito à verdade e à memória, que também tem duas dimensões: uma individual, em prol do direito da vítima e de seus familiares; e outra coletiva, em prol do direito da sociedade.

A dimensão individual, como direito humano correlato ao dever-poder de investigar e punir do Estado, compreende o direito de as vítimas e de seus familiares conhecerem a verdade sobre os fatos que violaram seu direito fundamental, incluindo o reconhecimento das circunstâncias do crime, a apuração do ilícito e a responsabilização do infrator.

[33] Corte Interamericana de Derechos Humanos. *Caso Durand y Ugarte vs. Perú*. Sentencia de 16 de agosto de 2000 (Fondo). Pg. 40. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/Seriec_68_esp.pdf. Acesso em 8 de setembro de 2021.

Inegável vertente da dignidade da pessoa humana, o direito à verdade e à memória busca honrar a dor da vítima e de seus familiares, permitindo que tenham acesso aos fatos sobre determinado acontecimento e sobre as circunstâncias do delito que lhes afetou, bem como acerca da devida punição do responsável.

A dimensão coletiva do direito à verdade inclui o direito da sociedade à construção da memória, história e identidades coletivas, possibilitando-se que as pessoas conheçam os acontecimentos de sua localidade e a realidade de determinado fato criminoso em suas consequências jurídicas e sociais.

Ao Estado compete viabilizar mecanismos que promovam o conhecimento da verdade em relação aos crimes que porventura ocorram, para os parentes das vítimas em especial e para a sociedade em geral, possibilitando à família a reconstrução da sua narrativa e finalização do processo de luto e à coletividade a construção da memória do lugar.

Na dicção da Corte Interamericana de Direitos Humanos, no "*Caso de las Hermanas Serrano Cruz* vs. *El Salvador*", de 1ª.3.2005:

> *62. Por otra parte, este Tribunal se ha referido en reiteradas ocasiones al derecho que asiste a los familiares de las presuntas víctimas de conocer lo que sucedió y de saber quiénes fueron los*

> *responsables de los respectivos hechos. La Corte ha reiterado que toda persona, incluyendo a los familiares de víctimas de graves violaciones de derechos humanos, tiene el derecho a conocer la verdad. En consecuencia, los familiares de las víctimas, y la sociedad como un todo, deben ser informados de todo lo sucedido con relación a dichas violaciones. Este derecho a la verdad se ha venido desarrollando por el Derecho Internacional de los Derechos Humanos; al ser reconocido y ejercido en una situación concreta constituye un medio importante de reparación. Por lo tanto, en este caso, el derecho a conocer la verdad da lugar a una expectativa que el Estado debe satisfacer a los familiares de las presuntas víctimas.*[34]

A sentença criminal, além de proporcionar a devida punição do criminoso, há de funcionar como instrumento de resgate da memória e da verdade, também na perspectiva do direito das vítimas, correspondendo, o mais proximamente possível, àquilo que verdadeiramente ocorreu.

A investigação e o processo assumem, também, o papel de restauração simbólica da norma violada, em respeito aos atingidos pelo dano. Dentro de balizas mediadores e que contenham os excessos e arbítrios, hão de refletir a verdade e a memória, uma vez que é pressuposto para se ter como operada a justiça que a conclusão do julgamento equivalha à realidade dos fatos, ao comprovado no processo.

---

[34] Corte Interamericana de Derechos Humanos. *Caso de las Hermanas Serrano Cruz vs. El Salvador*. Sentencia de 1º de março de 2005 (Fondo). Pgs. 55-56. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_120_esp.pdf. Acesso em 8 de setembro de 2021.

Mais uma vez, apropriadas as conclusões da Corte Interamericana de Direitos Humanos:

> *78. El Tribunal ha resaltado que las decisiones que adopten los órganos internos que puedan afectar derechos humanos deben estar debidamente fundamentadas, pues de lo contrario serían decisiones arbitrarias. En este sentido, la argumentación de un fallo debe mostrar que han sido debidamente tomados en cuenta los alegatos de las partes y que el conjunto de pruebas ha sido analizado. Asimismo, la motivación demuestra a las partes que éstas han sido oídas y, en aquellos casos en que las decisiones son recurribles, les proporciona la posibilidad de criticar la resolución y lograr un nuevo examen de la cuestión ante las instancias superiores. Por todo ello, el deber de motivación es una de las "debidas garantías" incluidas en el artículo 8.1 para salvaguardar el derecho a un debido proceso. ("Caso Apit Barbera y otros vs. Venezuela", de 5.8.2008).*[35]

A fundamentação do ato decisório, que tem essa função restauradora da memória e da verdade, demanda que haja uma articulação entre a memória reconstituída nos autos e a verdade, incluído aí o dever de investigação efetiva.

A jurisprudência da Corte Interamericana de Direitos Humanos ressalta que, em certas circunstâncias, pode ser difícil a investigação de fatos que atentem contra os direitos da pessoa e que a obrigação estatal de investigar é uma

[35] Corte Interamericana de Derechos Humanos. *Caso Apit Barbera y otros vs. Venezuela.* Sentencia de 5 de agosto de 2008. (Fondo). Pgs. 22-23. Disponível em: https://www.corteidh.or.cr/corteidh/docs/casos/articulos/seriec_182_esp.pdf. Acesso em 8 de setembro de 2021.

obrigação de meio, não de resultado. Há de ser conduzida com seriedade, e não como simples formalidade condenada de antemão a ser infrutífera:

> *(…) debe tener un sentido y ser asumida por el Estado como un deber jurídico próprio y no como una simple gestión de intereses particulares, que dependa de la iniciativa procesal de la víctima o de sus familiares o de la aportación privada de elementos probatorios, sin que la autoridad pública busque efectivamente la verdad. Esta apreciación es válida cualquiera sea el agente al cual pueda eventualmente atribuirse la violación, aun los particulares, pues, si sus hechos no son investigados con seriedad, resultarían, en cierto modo, auxiliados por el poder público, lo que comprometería la responsabilidad internacional del Estado*[36].[37]

A Corte Interamericana de Direitos Humanos destaca, ainda, que, em uma sociedade democrática, a verdade sobre os fatos graves de violações dos direitos humanos hão de ser conhecidos:

[36] Corte Interamericana de Derechos Humanos. *Caso Velásquez Rodríguez Vs. Honduras*. Sentencia de 29 de julio de 1988 (Fondo). Pg. 37. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_04_esp.pdf. Acesso em 8 de setembro de 2021.

[37] Ainda nesse sentido, o Caso Durand y Ugarte Vs. Perú, de 16.8.2000:" (…) el artículo 8.1 de la Convención Americana, em conexión con el artículo 25.1 de la misma, confiere a los familiares de las víctimas el derecho a que la desaparición y muerte de estas últimas sean efectivamente investigadas por las autoridades del Estado; se siga un proceso contra los responsables de estos ilícitos; en su caso se les impongan las sanciones pertinentes, y se reparen los daños y perjuicios que dichos familiares han sufrido. ". Também no "Caso Maritza Urrutia Vs. Guatemala", de 27.11.2003: "(...) la Corte ha entendido que la impunidad es la falta, en conjunto, de investigación, persecución, captura, enjuiciamento y condena de los responsables de las violaciones de los derechos protegidos por la Convención Americana, y que el Estado tiene la obligación de combatir tal situación por todos los medios legales disponibles. La impunidad propicia la repetición crónica de las violaciones de derechos humanos y la total indefensión de las víctimas y de sus familiares."

> *(…) en una sociedad democrática se debe conocer la verdad sobre los hechos de graves violaciones de derechos humanos. Esta es una justa expectativa que el Estado debe satisfacer, por un lado, mediante la obligación de investigar las violaciones de derechos humanos y, por el otro, con la divulgación pública de los resultados de los procesos penales e investigativos. Esto exige del Estado la determinación procesal de los patrones de actuación conjunta y de todas las personas que de diversas formas participaron em dichas violaciones y sus correspondientes responsabilidades y reparar a las víctimas del caso*[38].

A Corte Internacional, em diversos julgados, destaca a importância do cumprimento da obrigação de investigar *com a devida diligência*. O órgão que investiga uma violação de direitos humanos tem a obrigação de utilizar todos os meios disponíveis para levar a cabo, dentro de um prazo razoável, as averiguações necessárias para a completa elucidação do delito.

Enfatiza que *"en aras de garantizar su efectividad, en la investigación de violaciones de los derechos humanos se deve evitar omisiones em la recaudación de prueba y en el seguimiento de líneas lógicas de investigación"*[39]. A investigação há de se valer de todos os meios legais disponíveis e estar orientada à determinação da verdade.

---

[38] Corte Interamericana de Derechos Humanos. *Caso de la Masacre de Las Dos Erres Vs. Guatemala.* Sentencia de 24 de novembro de 2009 (Fondo). Pg. 45. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_211_esp.pdf. Acesso em 8 de setembro de 2021.

[39] Corte Interamericana de Derechos Humanos. *Caso Velásquez Paiz y outros Vs. Guatemala.* Sentencia de 19 de noviembre de 2015 (Fondo). Pg. 64. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_307_esp.pdf. Acesso em 8 de setembro de 2021.

Salienta também:

> *(…) em cumplimiento de su obligación de investigar y, em su caso, sancionar a los responsables de los hechos, el Estado debe remover todos os obstáculos, de facto y de jure, que impidan la debida investigación de los hechos, y utilizar todos los medios disponibles para hacer expedita dicha investigación y los procedimientos respectivos, a fin de evitar la repetición de hechos tan graves (…).*
> *Al mismo tiempo, teniendo em cuenta la jurisprudencia de este Tribunal, el Estado debe asegurar que los familiares de las víctimas tengan pleno acceso y capacidad de actuar em todas las etapas e instancias de dichas investigaciones y procesos, de manera que puedan hacer planteamientos, recibir informaciones, aportar pruebas, formular alegaciones y, em síntesis, hacer valer sus intereses. La ley interna debe organizar el proceso respectivo de conformidad con la Convención Americana y esta Sentencia. Dicha participación deberá tener como finalidad el acceso a la justicia, el conocimiento de la verdad de lo ocurrido y el otorgamiento de una justa reparación.*[40]"

Uma vez constatada a infração penal, cabe, pois, ao Estado a apuração diligente e minuciosa do fato ocorrido, esclarecendo todas as suas circunstâncias e desvendando seus desdobramentos.

Para tanto há de se valer de todos os meios investigativos possíveis a fim de, inclusive, atender aos tratados de Direitos Humanos firmados pelo Brasil, especialmente no contexto de graves violações a bens jurídicos por eles protegidos.

[40] Corte Interamericana de Derechos Humanos. *Caso Valle Jaramillo y outros Vs. Colombia.* Sentencia de 27 de noviembre de 2008 (Fondo). P. 69. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_192_esp.pdf. Acesso em 8 de setembro de 2021.

As investigações que não são efetivas, isto é, feitas sem a devida diligência e sem a utilização, dentro da legalidade, de todos os meios disponíveis de apuração acabam afetando os direitos das vítimas, de seus familiares e da sociedade como um todo e, pela negativa do direito à verdade e a um recurso efetivo, poderão, inclusive, conduzir à responsabilização internacional do Estado brasileiro.

O descarte apriorístico de um meio de investigação legítimo, de modo arbitrário, quando possível seu emprego dentro de balizas que respeitem e se ajustem aos demais direitos fundamentais seria, em si, medida inconstitucional e incompatível com os deveres decorrentes dos tratados de Direitos Humanos assinados pelo Brasil, notadamente no contexto de graves violações a bens jurídicos protegidos por estes tratados.

7. MEDIAÇÃO ENTRE OS DIREITOS À PRIVACIDADE E O DIREITO À MEMÓRIA E À VERDADE, COMO DEVER DE INVESTIGAR E PUNIR, NO AFASTAMENTO DO SIGILO DE DADOS DE PESSOAS INDETERMINADAS.

7.1. A constitucionalidade, convencionalidade e legalidade do afastamento de sigilo de dados telemáticos de pessoas indeterminadas no âmbito de procedimentos penais.

Como já exposto nas sessões anteriores, os parâmetros constitucionais, convencionais e legais suficientes para o afastamento do sigilo em relação a pessoas indeterminadas já são previstos no ordenamento pátrio, notadamente a partir das disposições constantes do microssistema protetivo composto pelas três leis que tratam de dados: Lei nº 9.296/96, Lei nº 12.965/2014 e Lei nº 13.709/2018.

Esse microssistema normativo de proteção de dados e comunicações confere os rumos que hão de ser devidamente sopesados a partir das premissas constitucionais *(i)* de inviolabilidade do direito à privacidade, *(ii)* de dignidade da pessoa humana (sob ambas as dimensões, do acusado e das vítimas e seus familiares) e *(iii)* decorrentes dos deveres de investigar e punir do Estado, para que o Direito Penal seja aplicado também como instrumento cuja finalidade é a proteção dos direitos fundamentais.

A Lei nº 12.965/2014 autoriza a requisição de registros de conexão e acesso de pessoas indeterminadas, quando presentes fundados indícios da ocorrência de fato ilícito, também para produção de prova em processos judiciais cíveis e penais. Saliente-se que tal dispositivo já autoriza o afastamento do sigilo em relação a pessoas indeterminadas no âmbito penal, conferindo legalidade à medida.

Tal ponto é reforçado pelo fato de a Lei nº 9.296/96 permitir, de forma subsidiária, a interceptação da comunicação telefônica de qualquer interlocutor que se comunique com o sujeito passivo, atingindo número indeterminado de pessoas, para produção de prova em investigação criminal e em instrução processual penal. Trata-se de medida ainda mais gravosa do que o acesso a dados determinados, autorizada a bem das investigações criminais.

Já a Lei nº 13.709/2018 – que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural – traz amplo disciplinamento acerca do tratamento e da tutela aos dados pessoais e estabelece expressamente que suas disposições não se aplicam, entre outros, ao tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, III).

Tem-se, ainda, que a Lei nº 13.709/2018, em relação aos dados objeto de seu disciplinamento, prevê a possibilidade de acesso a informações privadas em algumas situações excepcionais como, por exemplo, pela administração pública, para o tratamento e uso compartilhado de dados

necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres e para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Se a legislação permite o tratamento de dados pessoais, excepcionalmente, em circunstâncias de demonstrado interesse público, tanto mais é justificável o afastamento do sigilo de dados telemáticos dessa mesma natureza, mesmo de pessoas indeterminadas, quando evidenciada a utilidade dos registros em investigação ou produção de prova em procedimentos criminais.

A partir das premissas estabelecidas pelo próprio ordenamento jurídico-constitucional, em especial sob os aspectos de concretização do Estado Democrático de Direito e da primazia da dignidade humana em dupla dimensão, conclui-se pela constitucionalidade, convencionalidade e legalidade do afastamento do sigilo telemático, no âmbito de procedimentos criminais, mesmo para pessoas indeterminadas.

Tal conclusão decorre seja do fato de, em linha com a experiência de direito comparado, vários diplomas legais brasileiros compatibilizarem e mediarem a proteção da privacidade com o uso de meios investigativos que atingem sujeitos indeterminados, seja das obrigações decorrentes dos deveres de investigar e punir do Estado.

Propõe-se como primeira tese para a presente repercussão geral o seguinte enunciado:

> É permitido o afastamento de sigilo de dados telemáticos, no âmbito de procedimentos penais, ainda que em relação a pessoas indeterminadas.

Assumida tal premissa, a discussão desloca-se da suposta impossibilidade de utilização dos meios investigativos para a elucidação dos parâmetros pelos quais o emprego de tais meios é possível.

7.2. O princípio da proporcionalidade e a ponderação de direitos fundamentais na elucidação dos parâmetros para o afastamento de sigilo de dados telemáticos de pessoas indeterminadas no âmbito de procedimentos penais.

Sabe-se que normas de direitos fundamentais têm, em geral, natureza principiológica e conteúdo aberto. Por assegurarem um conjunto amplo de posições jurídicas subjetivas, podem entrar em conflito com outras normas e necessitam ter seu alcance relativizado em juízo de ponderação, sendo despidas de caráter absoluto.[41]

Decorre dessa estrutura principiológica a possibilidade de direitos fundamentais virem a ser limitados em prol de outros bens e valores

[41] ALEXY, Robert. **Teoria dos direitos fundamentais**. 2. ed. São Paulo: Malheiros, 2015, p. 111.

fundamentais em um dado contexto. A aferição de qual valor ou direito há de preponderar passa pelo juízo de ponderação – ou teste de proporcionalidade –, que examine se a satisfação de um valor ou interesse constitucional justifica a limitação de outros que com ele colidam.

Em circunstâncias que envolvam conflito aparente de direitos fundamentais, há de se sopesar as desvantagens dos meios empregados com as vantagens a serem alcançadas pelo fim almejado, observadas adequação e necessidade das medidas, que devem ser aplicadas em extensão e alcance estritamente imprescindíveis.[42]

Ato restritivo de direito há de ser apropriado para atingir o fim almejado, e o meio há de ser o estritamente necessário, de modo a não ocasionar danos desproporcionais a direitos fundamentais.

A adequação pressupõe que determinado ato restritivo tenha idoneidade ou aptidão para produzir o efeito por ele almejado. Seu exame inicia-se pela apuração do objetivo do ato que interfere em uma norma de direito fundamental colidente, que há de ser um fim válido do ponto de vista constitucional. Existindo tal finalidade, uma medida será adequada caso apresente capacidade de alcançar o resultado pretendido.[43]

[42] SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. São Paulo: Malheiros, 2010, p. 174.

[43] BRANCO, Paulo Gustavo Gonet. **Juízo de ponderação na jurisdição constitucional**: pressupostos de fato e teóricos reveladores de seu papel e de seus limites. (tese).

O afastamento de sigilo de dados de pessoas indeterminadas ultrapassa os testes da adequação e necessidade, na medida em que permite colher provas para a investigação de fato grave e sua respectiva autoria por meio de ordem judicial adequadamente fundamentada (art. 93, IX, da Constituição Federal), notadamente em contextos de difícil elucidação de autoria, como os decorrentes dos desafios proporcionados pela utilização das tecnologias contemporâneas para o cometimento de crimes.

As limitações aos direitos fundamentais, ainda que admissíveis, necessitam circunscrever-se ao imprescindível para preservar outros direitos e interesses constitucionalmente protegidos. Ao analisar o chamado princípio da *proporcionalidade em sentido estrito*, J. J. Gomes Canotilho leciona:

> *Meio e fim são colocados em equação mediante um juízo de ponderação, com o objectivo de se avaliar se o meio utilizado é ou não desproporcionado em relação ao fim. Trata-se, pois, de uma questão de 'medida' ou 'desmedida' para se alcançar um fim: pesar as desvantagens dos meios em relação às vantagens do fim.*[44]

A ponderação entre os direitos à privacidade e à proteção de dados e o direito à memória e à verdade das vítimas e familiares, traduzido no dever de investigar e punir do Estado no contexto de proteção de bens jurídicos

Brasília: Faculdade de Direito da Universidade Nacional de Brasília (UnB), jul. 2008, p. 206.

[44] CANOTILHO, J. J. Gomes. **Direito constitucional e teoria da constituição.** 7. ed. Coimbra: Almedina, 2003, p. 270.

relevantes à sociedade, há de alcançar um ponto ótimo, em que a limitação de um bem jurídico seja a menor possível e na medida imperativa à salvaguarda do bem jurídico contraposto.

Para garantir tal ponto ótimo, e na linha do que rememorado pelo Ministro Gilmar Mendes quando do julgamento da ADI 6387 e já referido na neste parecer, o ordenamento jurídico, em leitura sistemática, prevê mecanismos de salvaguarda traduzidos em normas de proteção e de organização e procedimento, consistentes exatamente nos parâmetros que se busca elucidar no presente tema de repercussão geral.

No tocante ao primeiro conjunto de normas, é relevante, para os propósitos do presente tema de repercussão geral, a explicitação dos requisitos legais e sistêmicos para o pedido de afastamento de sigilo em relação a pessoas indeterminadas. Já em relação aos dois últimos, cumpre apontar as obrigações associadas aos manejos das informações obtidas pelos diversos atores envolvidos no processo penal.

7.3. Os requisitos necessários para o afastamento do sigilo de dados telemáticos de pessoas indeterminadas.

A elucidação dos parâmetros necessários para o afastamento do sigilo de dados em relação a pessoas indeterminadas passa por uma análise

conjunta dos arts. 10 e 22 do Marco Civil da Internet, contextualizada dentro do microssistema protetivo de dados pessoais e comunicações.

O confronto dos dois dispositivos conduz à diferenciação entre os registros de conexão ou de registros de acesso a aplicações de internet, previstos no *caput* do art. 22, e os dados pessoais e de conteúdo de comunicações privadas associados, cuja possibilidade de acesso é explicitada no art. 10, como se aprofunda adiante.

7.3.1. Os registros de conexão ou acesso a aplicações de internet (art. 22 do Marco Civil da Internet).

A requisição judicial dos registros de conexão ou de acesso a aplicações de internet está prevista no art. 22 da Lei nº 12.965/2014, o qual disciplina os requisitos mínimos para admissão do requerimento de afastamento do sigilo: ***(i)*** apresentação de fundados indícios da ocorrência do ilícito; ***(ii)*** justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e ***(iii)*** delimitação do período ao qual se referem os registros.

Tais exigências têm o objetivo de evitar requerimentos de acesso desprovidos de embasamento mínimo ou sem limitação temporal, de modo que o fornecimento dos registros seja a exceção, privilegiando-se, sempre que

possível, o sigilo das informações referentes à intimidade e à vida privada do usuário.

Poderá a autoridade investigante, com o propósito de formar conjunto probatório em processos criminais, requerer acesso a tais dados telemáticos desde que demonstre, nos termos da mencionada legislação, a existência de fundados indícios da ocorrência do crime, justificando de forma motivada a utilidade dos registros solicitados, além de delimitar o respectivo período ao qual se referem.

Observa-se que na presente discussão o risco de supostas *fishing expeditions* no fornecimento de registros de conexão ou acesso é afastado em virtude da exigência de conexão entre o afastamento de sigilo de dados de pessoas indeterminadas e o fato criminoso investigado, consistente na indicação de fundados indícios da ocorrência do ilícito (art. 22, parágrafo único, I, da Lei nº 12.965/2014).

Portanto, em relação aos registros de conexão ou acesso a aplicações de internet, o próprio legislador, no foro democrático do Congresso Nacional, já realizou a mediação entre os direitos fundamentais em aparente choque, dispensando a indicação de autoria como elemento necessário ao afastamento do sigilo.

Propõe-se a seguinte tese com relação ao ponto em análise:

> Aplica-se, no tocante aos requerimentos de registros de conexão ou acesso a aplicações de internet, os requisitos previstos no art. 22 da Lei nº 12.965/2014 (Marco Civil da Internet): a apresentação dos fundados indícios da ocorrência do ilícito; a justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e a delimitação do período ao qual se referem os registros.

7.3.2. A autodeterminação informativa, os princípios da finalidade, necessidade, adequação, segurança e prevenção e a obrigação de fundamentação agravada diante de dados pessoais e de conteúdo de comunicações privadas (o art. 10 do MCI).

Já a possibilidade do acesso aos dados pessoais e de conteúdo de comunicações privadas, de forma autônoma ou associada a outras informações que possam contribuir para a identificação do usuário ou do terminal, é prevista e autorizada pelo art. 10 do MCI, mediante ordem judicial (art. 10, *caput* e § 1º).

A proporcionalidade – em sentido estrito – do afastamento de sigilo de dados de pessoas indeterminadas decorre da constatação de que a intensidade em que se limita os direitos à privacidade e à proteção de dados (direitos contrapostos que sofrem a limitação) é inferior aos eventuais ganhos com a promoção do direito de investigar e punir do Estado na proteção de

bens jurídicos de relevância social e constitucional (direito fomentado pelo meio escolhido). É dizer, a valia da promoção do fim corresponde à desvalia da proteção diminuída.

Contudo, o tipo de informação disponibilizada conduz a que, no contexto do microssistema de proteção de dados e comunicações, a autoridade requisitante tenha um ônus agravado de fundamentação quando os solicita.

Esse ônus, conquanto não explícito no referido art. 10, decorre da leitura sistemática do microssistema protetivo de dados e comunicações e de seus princípios reitores dentro de um contexto em que envolvidos direitos de pessoas indeterminados e a preferência por meios investigativos que gerem menos riscos a terceiros não envolvidos no ilícito.

Essa subsidiariedade decorre, primeiramente, da própria função social da internet (art. 2º, VI, do MCI) e do princípio da finalidade na coleta e tratamento de dados pessoais (art. 6º, I, da LGPD), que implicam vetor teleológico na prática de atos de coleta e tratamento de dados telemáticos.

Trata-se, em uma perspectiva civil-constitucional, de uma cláusula legal de densificação da proporcionalidade em sentido estrito informada pelo objetivo de preservação de um espaço virtual harmônico com os fundamentos

constitucional e legal que regem a vida em sociedade, notadamente o respeito à liberdade de expressão (art. 2º do MCI), conformado com os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais (art. 2º, II, do MCI).

Daí que todo tratamento de dados há de ser regido pelos preceitos da adequação e necessidade, isto é, ser compatível com as finalidades informadas ao titular e se limitar ao mínimo necessário para alcançar estas, abrangendo os dados pertinentes, proporcionais e não excessivos (art. 6º, II e III, da LGPD).

Reforça essa restrição os axiomas da segurança e prevenção, isto é: o uso das medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão e a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VII e VIII, da LGPD).

Esse cenário conduz a que, na hipótese de os dados telemáticos solicitados serem associados a informações pessoais ou outras que possam contribuir para a identificação do usuário ou do terminal, cumpre à autoridade requerente uma obrigação de fundamentação agravada a fim de circunscrever a medida aos casos em que há efetiva necessidade e adequação,

prevenindo danos a terceiros e preservando a segurança destes, sem obstar o cumprimento dos deveres de investigar e punir.

Essa fundamentação agravada pode ser sintetizada na apresentação de duas justificativas:

> *(i)* A necessidade em concreto da medida para o prosseguimento da investigação, que há de ser subsidiária em relação a outros meios de prova menos gravosos a direitos de terceiros; vale dizer, os motivos pelos quais as informações cuja obtenção é pretendida não poderiam, no respectivo caso, ser razoavelmente alcançadas por outros meios investigativos com menor risco de exposição de terceiros;
>
> *(ii)* A pertinência das informações obtidas em relação ao fato investigado, isto é, a justificativa de cada um dos elementos limitadores dos dados a serem acessados em termos de tempo, espaço e outros elementos de especificação, que hão de ser especificadas ao mínimo imprescindível com base nos elementos do possível ilícito e na hipótese em investigação.

Ficam esclarecidos, assim, previamente os motivos pelos quais há a necessidade da adoção do meio investigativos e os limites em que a medida será empregada, evitando excessos na coleta dos dados a serem acessados.

Nesse contexto, propõe-se a seguinte tese quanto ao ponto:

> Quando os dados telemáticos solicitados forem associados a dados pessoais que possam contribuir para a identificação do usuário ou do terminal, cumpre à autoridade requerente também justificar fundamentadamente:
>
> a) A necessidade da medida para a investigação em concreto, que há de ser subsidiária em relação a outros meios de prova menos gravosos a direitos de terceiros;
>
> b) A pertinência das informações obtidas em relação ao fato investigado, que hão de ser especificadas no máximo possível com base em elementos identificativos e contextuais atinentes ao possível ilícito.

7.4. As obrigações específicas associadas ao pedido de afastamento do sigilo nas dimensões de guarda e inutilização: os princípios da segurança, da prevenção, da responsabilização e prestação de contas.

De forma complementar às normas de proteção já expostas, também normas de organização e procedimento se associam como mecanismos de salvaguarda do direito à privacidade.

Conquanto a própria existência das instituições e das normas procedimentais ligadas ao devido processo legal e ao Estado Democrático de Direito já sejam, em si, mecanismos de salvaguarda do regular acesso e emprego das informações obtidas a partir da transferência de sigilo, é relevante apontar de que modo certas garantias sistêmicas se densificam em obrigações específicas associadas ao afastamento do sigilo para os diversos atores envolvidos no processo penal.

Essas obrigações específicas se conjugam a outros deveres e obrigações gerais incidentes sobre a atuação do Estado, previstos nas diversas áreas do ordenamento jurídico, para proporcionar o conjunto de salvaguardas necessárias à proteção dos direitos fundamentais.

Duas categorias de obrigações específicas se destacam: as obrigações ligadas à guarda das informações obtidas e as obrigações ligadas à inutilização dos dados obtidos de terceiros após o encerramento das investigações.

7.4.1. As obrigações associadas atinentes à guarda das informações obtidas.

A legislação atribui aos atores envolvidos no afastamento do sigilo a obrigação de preservar o segredo dos dados individuais, relativizado apenas no estritamente necessário à continuidade da apuração criminal.

O MCI, por exemplo, além de estabelecer requisitos legais para o requerimento de acesso aos registros de conexão, estabelece, no art. 3º, VI, que é princípio da disciplina do uso da internet no Brasil a responsabilização dos agentes de acordo com suas atividades, nos termos da lei.

Complementa, em seu art. 23, que cabe ao juiz, ao decidir o pedido, 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 atribuir segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Também a Lei 9.296/1996 prevê a necessidade de preservação do sigilo das diligências, gravações e transcrições com base nela determinadas (art. 8º) e criminaliza a conduta do funcionário público que descumprir a determinação de sigilo das investigações que envolvam a captação ambiental ou revelar o conteúdo das gravações enquanto mantido o sigilo judicial (art. 10-A, § 2º).

Completa a análise do microssistema protetivo dos dados e comunicações, nessa perspectiva, as previsões da LGPD atinentes aos princípios da segurança, da prevenção, da responsabilização e prestação de contas (art. 6º, VII, VIII e X).

Apesar da inaplicação da Lei 13.709/2018 às atividades de investigação e repressão de infrações penais (art. 4º, III, *d*), sua principiologia é referência para a contextualização das garantias envolvidas no manejo de dados.

Deles extrai-se, respectivamente, a necessidade de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e de demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O tratamento de dados pela autoridade pública há de atender a finalidade que as justifica, na busca do interesse público (art. 23, da LGPD), havendo, ainda, de garantir a inocorrência de danos em virtude desse tratamento (art. 6º, VII, VIII e X, da LGPD).

No âmbito do Ministério Público Federal (MPF), por exemplo, a Secretaria de Pesquisa, Perícia e Análise (SPPEA) recebeu a delegação para

realizar o tratamento dos dados voltados à atividade-fim do Ministério Público[45], relativamente aos sistemas investigativos.

A SPPEA possui em sua estrutura orgânica uma unidade técnica própria com atribuições de efetuar o tratamento de dados recebidos pelo MPF no exercício de suas funções institucionais, zelando pela uniformidade metodológica no desenvolvimento, aquisição e utilização de softwares, soluções tecnológicas, bases de dados e serviços especializados para o desempenho de sua função de auxílio.

A robustez dos sistemas informáticos mantidos pela SPPEA, que são utilizados para o tratamento de dados pessoais, pode ser observado no Relatório Técnico nº 005/2021 – AATI/SPPEA/PGR. Os sistemas atendem, satisfatoriamente, aos requisitos de segurança e aos padrões de boas práticas e de governança, obedecendo tanto aos princípios da boa-fé, necessidade, segurança, prevenção, não discriminação e responsabilização e prestação de contas; como a dimensão objetiva do direito à autodeterminação informativa.[46]

---

[45] Conforme Portaria nº 532/2020, expedido pelo Procurador-Geral da República. Disponível em: http://bibliotecadigital.mpf.mp.br/bdmpf/handle/11549/205053. Acesso em 8 de outubro de 2021

[46] Recentemente, o Grupo de Trabalho criado no âmbito da SPPEA, com finalidade de elaborar documento a respeito do tratamento jurídico dispensado à obtenção de bases de dados pessoais para utilização em sistemas investigativos do MPF, proferiu nota técnica em que trata do tema, disponível em: https://portal.mpf.mp.br/novaintra/informa/2021/pgr/PGR00348550.2021.pdf.

Na eventualidade do emprego inadequado dos dados ou a quebra de sigilo, em violação ao art. 5º, X, da Constituição Federal e à legislação de proteção de dados, há de se reparar o dano causado. A responsabilização decorre da própria lógica do ordenamento jurídico para proteção da privacidade e de dados.

Na perspectiva jurisprudencial, a Suprema Corte já reconheceu que o respeito à garantia constitucional que protege a intimidade e a vida privada, de modo a preservar o sigilo das informações individuais, há de ser a regra no ordenamento jurídico pátrio, sendo as suas formas de mitigação a exceção.

Por outro lado, de modo geral, o Supremo Tribunal Federal tem admitido o compartilhamento de dados sigilosos com órgãos de controle e fiscalização, para tutelar interesse público.[47] Nessas hipóteses, consoante a jurisprudência, exsurge uma série de obrigações associadas aos atores envolvidos no processo penal, decorrentes dos fins específicos para os quais autorizado o afastamento do sigilo.

Recentemente, a Corte, ao apreciar o Tema 990 da sistemática da repercussão geral, apreciou a constitucionalidade do compartilhamento de

[47] São exemplos desse entendimento o decidido nos seguintes precedentes: RE 1.043.002, Rel. Min. Roberto Barroso, Primeira Turma, *DJe* de 14 dez. 2017; RE 1.108.725, Rel. Min. Edson Fachin, Segunda Turma, *DJe* de 27 nov. 2018; RE 906.381, Rel. Min. Dias Toffoli, Segunda Turma, *DJe,* de 14 fev. 2017; RE 1.041.285, Rel. Min. Roberto Barroso, Primeira Turma, *DJe,* de 13 nov. 2017; RE 1.058.429, Rel. Min. Alexandre de Moraes, Primeira Turma, *DJe,* de 5 mar. 2018.

dados bancários e fiscais de contribuintes com órgãos de investigação criminal (Ministério Público e Polícia Judiciária), sem intermediação do Poder Judiciário, tendo presentes os postulados constitucionais da intimidade e do sigilo de dados.

Na ocasião, afirmou-se a compatibilidade da prática com o texto constitucional, assinalando a possibilidade de se relativizar os sigilos, desde que de forma proporcional e razoável e com a finalidade de defesa da probidade e do combate à corrupção, bem como de outros valores constitucionais caros à sociedade brasileira.[48]

No julgado, a Corte destacou a importância do compartilhamento de informações para fins penais por órgãos administrativos de inteligência e de fiscalização que detêm informações protegidas por sigilo, ressaltando a

[48] RE 1.055.941/ SP, Min. Rel. Dias Toffoli, *DJe* 243, de 5 out. 2020, assim ementado: *"Repercussão geral. Tema 990. Constitucional. Processual Penal. Compartilhamento dos Relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil com os órgãos de persecução penal para fins criminais. Desnecessidade de prévia autorização judicial. Constitucionalidade reconhecida. Recurso ao qual se dá provimento para restabelecer a sentença condenatória de 1º grau. Revogada a liminar de suspensão nacional (art. 1.035, § 5º, do CPC). Fixação das seguintes teses: 1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil – em que se define o lançamento do tributo – com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; 2. O compartilhamento pela UIF e pela RFB referido no item anterior deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios."*

relevância da transferência de dados para o fortalecimento do sistema de combate à corrupção e à lavagem de dinheiro.

A propósito, por ocasião de julgamento do citado Tema 990, explicitou o Ministro Roberto Barroso em seu voto:

> *Assim, no meu entendimento, se a prova foi obtida pelo Fisco, pela Receita, licitamente, não deve haver fundamento jurídico que impeça esse compartilhamento com o Ministério Público, diante dos indícios de conduta criminosa.*
> *E, aqui, há um ponto muito importante e devemos insistir nele. A Receita compartilha os dados com o Ministério Público, mas não há quebra de sigilo aqui; há uma transferência de sigilo. E o Ministério Público tem o dever de preservar este sigilo. E constitui crime, seja pelo membro do Ministério Público, como por qualquer pessoa, vazar informação protegida por sigilo, fora daquelas exceções previstas na legislação.*
> *(…)*
> *É isso mesmo. Não há quebra de sigilo, mas há a transferência de sigilo de um órgão, a Receita Federal, para o Ministério Público, e ambos têm o dever de preservar esse sigilo.*

O Tribunal, ao final, fixou as seguintes teses de repercussão geral:

> *1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil – em que se define o lançamento do tributo – com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; 2. O compartilhamento pela UIF e*

> *pela RFB referido no item anterior deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.*

As razões adotadas pela Suprema Corte no referido *leading case* têm relevância para o estabelecimento das balizas que hão de ser fixadas no presente caso. Aqui, da mesma forma que se mencionou naquele julgado, importante salientar a impropriedade de se utilizar a expressão *"quebra de sigilo"*, mostrando-se mais apropriado falar, na verdade, em transferência de dados sigilosos para órgãos responsáveis pela persecução penal.

Isso porque, como explicitado nos termos do item dois da tese fixada no Tema 990, o compartilhamento dos dados se faz conjugado a uma série de obrigações associadas específicas – a formalidade das comunicações, com garantia do sigilo, a certificação do destinatário e o estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.

Nesse sentido, uma vez transferidos os dados sigilosos à autoridade pública requerente, passam também a ser de sua responsabilidade a preservação da privacidade das pessoas envolvidas e a obrigação de guarda de sigilo das informações obtidas, sob pena de responsabilização.

Propõe-se, em leitura sistemática do microssistema de proteção de dados e comunicações e na linha do que fixado quando da apreciação do Tema 990 da Repercussão Geral, a seguinte tese em relação ao ponto:

> A transferência de dados às autoridades requerentes há de ocorrer unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.

7.4.2. As obrigações associadas atinentes à inutilização das informações de terceiros obtidas após o encerramento das investigações.

Um segundo conjunto de obrigações associadas refere-se aos procedimentos que hão de ser tomados para a inutilização dos dados de terceiros obtidos nas investigações após o encerramento destas. Essas providências de exclusão também se extraem do conjunto de normas que compõe o microssistema protetivo dos dados e comunicações.

O MCI prevê no art. 7º, X, ser direito do usuário da internet a exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas na própria lei.

Essa previsão conjuga-se com o inciso VIII do mesmo artigo, no que dispõe que os dados somente poderão ser utilizados para finalidades que justifiquem sua coleta, a sinalizar que sua preservação se mantém apenas enquanto justificada pela necessidade que motivou a coleta e tratamento inicial.

O plexo de princípios da LGPD reforça essa conclusão, ao consagrar os princípios da segurança e prevenção como axiomas da proteção de dados, isto é, respectivamente: a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; e a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Uma das principais medidas para prevenir o emprego indevido é, exatamente, a inutilização dos dados após tornarem-se dispensáveis para o fim que justificou inicialmente sua coleta. Nessa linha, a Lei nº 9.296/1996, no seu art. 9º, previu incidente específico para a implementação de tal medida em relação aos dados coletados com base nela, nos seguintes termos:

> *Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.*

> *Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.*

Esse mecanismo de salvaguarda, concretizado no incidente do art. 9º da Lei 9.296/1996, é especialmente importante porque envolve obrigações para os diversos interessados no processo penal, como colaboradores da Justiça, notadamente por estarem em jogo direitos de terceiros que podem ter sido atingidos pela coleta de informações e sobre os quais recaem riscos de posteriores quebras dissociadas do propósito de interesse público que fundamentou a limitação da privacidade para fins de investigação criminal.

Três dimensões se destacam quanto à inutilização.

A primeira é a obrigação da autoridade requerente de postular a inutilização quando restar claro ser prescindível a informação coletada, evitando a possibilidade de vazamentos futuros, nos moldes do art. 9º da Lei 9.296/1996, aplicável analogicamente.

A segunda, de cariz procedimental, é a oitiva dos diversos interessados quando da inutilização, também nos moldes do art. 9º da Lei nº 9.296/1996. Recai precipuamente sobre o Estado-juiz, na atuação como magistrado de garantia, e visa a permitir eventuais requerimentos de produção de prova para os quais seja necessário o acesso aos dados coletados,

garantindo a fiscalização dos procedimentos investigativos e a responsabilização por eventuais medidas írritas.

A terceira, que recai eminentemente sobre as partes, é a obrigação de requerer, justificadamente, até a manifestação no contexto do procedimento de inutilização, a produção das provas que entendam necessárias e envolvam o acesso a dados de terceiros coletados no curso das investigações, sob pena de preclusão.

Essa previsão decorre da necessidade de equilibrar a preservação dos dados com a ampla liberdade probatória do processo penal e se justifica pelos padrões de boa-fé objetiva que também recaem sobre os litigantes e seus representantes, consagrada na perspectiva da vedação ao comportamento contraditório, nos termos do art. 565 do Código de Processo Penal, que prevê que *"[n]enhuma das partes poderá argüir nulidade a que haja dado causa, ou para que tenha concorrido*".

Sobre o tema, importante rememorar o que fez constar Vossa Excelência, Ministra Rosa Weber, na ementa do julgado no Agravo Interno no Recurso em Habeas Corpus nº 189.088:

> *AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. PENAL E PROCESSO PENAL. (…). PRINCÍPIOS DA BOA-FÉ E DA LEALDADE PROCESSUAIS. DEVER DE OBSERVÂNCIA.(…).*

> *(…).*
> *5. Vigoram, no processo penal brasileiro, como expressão imediata da cláusula do* due process of law, *os princípios da boa-fé objetiva e da lealdade processuais, o que torna imperativa a observância, tanto pelo órgão de acusação quanto pela Defesa, da cláusula* nemo potest venire contra factum proprium.

Complementou Vossa Excelência, no voto, reportando-se ao que já havia registrado quando da decisão monocrática no referido RHC:

> *Não se questiona que a essência do processo penal constitucional consiste em franquear ao acusado o exercício, em toda a sua plenitude, do amplo direito de defesa (CF, art. 5º, incisos LV e XXXVIII, a). Tão sublime esse direito que muitos, no passado, nele vislumbraram raízes religiosas, a situá-lo acima do próprio ordenamento positivo. Destaco, ilustrativamente, o conhecido debate entre canonistas e glosadores medievais, a identificar o fundamento do direito de defesa no próprio Gênesis, por Deus havê-lo oportunizado a Adão após o pecado original. Ora, se até mesmo Deus, onipotente e onisciente, garantira defesa a Adão, a conclusão extraída é a de que tal direito funda-se na lei divina, de modo que nem mesmo o príncipe - o legislador positivo da época – poderia suprimi-lo (sobre o tema: PENNINGTON, Kenneth. T*he Prince and the Law: 1200-1600: Sovereign and rights in the Western Legal Tradition. *Berkeley: University of California Press, 1993).*
>
> *Como consectário, essencial à validade do processo penal que se oportunize à Defesa, mediante citação/intimação, o exercício do contraditório, do direito à produção probatória e de confrontar as provas da Acusação. Mais do que isso, tratando-se de julgamento pelo Tribunal Popular, agrega-se a essa garantia o predicado da* ***plenitude*** *(CF, art. 5º, XXXVIII, a), cuja* amplitude e complexidade são muito maiores do que aquelas relativas às garantias da ampla defesa e do contraditório, visto que ela abrange uma argumentação que transcende a dimensão

meramente jurídica, na medida em que admite aspectos de ordem social, cultural, econômica, moral, religiosa, etc. *(STRECK, Lenio Luiz. In* ***Comentários à constituição do Brasil.*** *Coordenação J.J. Gomes Canotilho et al. 2ª ed. São Paulo: Saraiva Educação, 2018, p. 405).*

Acresça-se que, na linha de documentos internacionais subscritos pelo Estado brasileiro, nenhuma pessoa poderá sofrer prejuízo aos próprios interesses sem a efetiva celebração de um ***processo justo*** *(Giulio Ubertis.* Principi di procedura penale europea: le regole del giusto processo. *Milano: Raffaello Cortina, 2000. fls. 7-8).*

Diz-se que os princípios mínimos de configuração de um processo justo são a presença de julgador independente e imparcial, definido por lei, a proferir decisão em prazo razoável, em julgamento com contraditório e, de regra, público, respeitadas as garantias da presunção de inocência e de inviolabilidade da defesa. Nessa direção, inclusive, é o Artigo 14 do ***Pacto Internacional sobre Direitos Civis e Políticos*** *cujo teor projeta-se, de igual modo, no Artigo 8º* ***Convenção Americana de Direitos Humanos,*** *assim como no Artigo 6º da* ***Convenção Europeia dos Direitos do Homem****.*

Não obstante, no caso concreto, não se verifica ofensa ao direito de defesa. (…).

(…).

Em acréscimo, é importante registrar, na esteira do acórdão distrital, que não pode a Defesa do réu deliberadamente adotar, como estratégia exculpatória, uma determinada linha argumentativa e, somente após encerrado o julgamento plenário, com a condenação do acusado, arguir a deficiência do plano defensivo empregado – que teria sido inadequado ao réu ao criar histórias fantasiosas que só prejudicaram seu julgamento *(evento 12, fl. 61) –, sem, com isso, incidir em franco desrespeito aos princípios da boa-fé e da lealdade processuais. Daí a razão por que* é vedado à defesa se valer de suposto prejuízo a que deu causa, nos termos do artigo 565 do Código do Processo Penal *(HC 185.744/SP, Rel. Min. Luiz Fux, 1ª Turma, DJe 06.7.2020).*

> *Na realidade, tanto a Defesa quanto o órgão de acusação devem pautar suas atuações processuais pelos primados da boa-fé objetiva, da lealdade e da coerência, tal como adverte a jurisprudência deste Supremo Tribunal Federal[…].*

A limitação temporal da disponibilidade dos dados, além de significar proteção na linha dos princípios da segurança e prevenção, harmoniza os direitos e deveres dos diversos envolvidos no processo penal com a tutela do direito à privacidade dos terceiros.

Neste ponto, propõe-se as seguintes teses em relação ao ponto:

> Cumpre à autoridade requerente providenciar, ao final das investigações, a inutilização dos dados obtidos de terceiros que sejam desnecessários para a continuidade do processo-crime, mediante requerimento ao juízo competente, na forma do art. 9º da Lei nº 9.296/96, com a oitiva prévia dos demais interessados.
>
> Incumbe aos interessados no processo-crime, sob pena de preclusão, caso pretendam a produção de prova para a qual seja imprescindível ter acesso aos dados telemáticos de terceiros coligidos nas investigações, postular sua realização até a intimação para manifestar-se sobre a inutilização dos dados, de modo fundamentado, a fim de serem preservados os elementos imprescindíveis à diligência.

7.5. O devido processo legal na perspectiva da justa causa: a conjugação de dados possivelmente aleatórios com outros elementos indiciários.

O devido processo legal é um princípio constitucional explícito que, no entendimento de vários estudiosos, abrange os demais princípios e garantias processuais assegurados pela Constituição Federal e traz em si a premissa de procedimentos investigativos e julgamento justos.

O princípio do devido processo legal, em seu aspecto processual, é um princípio síntese, de forma que se afirma até mesmo que seria suficiente que a Constituição assegurasse tão somente o devido processo legal, eis que os demais princípios processuais dele decorreriam.[49]

É inviável pensar em um *due process* que se desenvolva perante tribunais de exceção ou perante juízes diversos daqueles definidos pela legislação, bem como será o processo indevido se inobservados o contraditório, a ampla defesa e a paridade de armas, com decisões imotivadas e com o processo sem desenvolvimento em prazo razoável.

Apesar de pensado frequentemente apenas como um preceito ligado ao aspecto procedimental, atualmente, o devido processo legal tem contornos mais amplos, podendo-se falar em devido processo substantivo (*substantive due process*).

[49] Nesse sentido: BADARÓ, Gustavo Henrique. *Processo penal.* 6. ed. São Paulo: Thomson Reuters Brasil, 2020. (Livro eletrônico).

O devido processo substantivo traz a determinação de adequação para o aspecto material dos conflitos, tendo por finalidade assegurar que as leis e os atos estatais em geral sejam justos e razoáveis. A doutrina, quanto ao viés substantivo do princípio, faz as seguintes considerações:

> *O devido processo legal substantivo assegura que as leis sejam razoáveis. Nos dizeres de Carlos Alberto de Siqueira Castro, o* substantive due process *é "capaz de condicionar, no mérito, a validade das leis e da generalidade das ações (e omissões) do Poder Público. A cláusula erigiu-se, com isso, num requisito de 'razoabilidade' (*rasonableness*) e de 'racionalidade' (*rationality*) dos atos estatais, o que importa num papel de termômetro axiológico acerca da justiça das regras de direito". Em consequência, também entende que "uma lei (ou outro ato normativo qualquer) que não atenda à razoabilidade (*reasonabless*) é inconstitucional, por ferir a cláusula do* due process. *E cabe ao Poder Judiciário, desde que foi concebido o* judicial review of legislation, *a tarefa de aferir a 'justiça' da lei.*[50]

Esse viés substantivo do devido processo legal, corolário do Estado Democrático de Direito e também da dignidade humana, de compreensão mais abrangente e ligada às noções de Justiça e equidade, constitui verdadeiro preceito de proteção dos sujeitos do processo e legitima o exercício do poder punitivo do Estado.

Tendo em vista a natureza demeritória do processo penal, em que o simples fato de figurar como réu inevitavelmente já traz em si certo

[50] BADARÓ, Gustavo Henrique. *Processo penal.* 6. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 1. (Livro eletrônico).

apenamento ao indivíduo, há de a atuação estatal se guiar nos limites daqueles ditames, com razoabilidade e justiça.

A ideia de justa causa passa pela existência de elementos de convicção que demonstrem a razão de ser do processo penal, exigindo-se a existência de um suporte probatório mínimo de materialidade e autoria delitiva. A ausência desse lastro probatório macula a iniciativa acusatória, que carecerá de justa causa, consubstanciando constrangimento ilegal apto a ensejar o trancamento da ação penal.

A razão de existir da justa causa é precisamente evitar que o acusado passe pelo constrangimento de responder a um processo penal a partir de denúncias infundadas e sem viabilidade aparente, situação que representaria afronta ao devido processo substantivo, visto que injusta e afrontosa à dignidade humana.

O processo penal se norteia pela justa causa na medida em que se faz necessária a apresentação de elementos mínimos de informação – indícios mínimos de autoria e prova da materialidade do fato delitivo – para o recebimento da denúncia, não sendo *"possível admitir denúncias absolutamente temerárias, desconectadas dos elementos concretos de investigação que tenham sido colhidos na fase pré-processual"*[51]:

[51] BADARÓ, Gustavo Henrique Righi Ivahy. **Processo penal.** Rio de Janeiro: Elsevier, 2012, p. 105. Nesse sentido, Fernando da Costa Tourinho Filho aponta a necessidade do

> *Desta forma, torna-se necessário ao regular exercício da ação penal a demonstração,* prima facie, *de que a acusação não é temerária ou leviana, por isso que lastreada em um mínimo de prova. Este suporte probatório mínimo se relaciona com os indícios de autoria, existência material de uma conduta típica e alguma prova de sua antijuridicidade e culpabilidade. Somente diante de todo este conjunto probatório é que, a nosso ver, se coloca o princípio da obrigatoriedade da ação penal.*[52]

A jurisprudência da Suprema Corte aponta que a análise da justa causa perpassa pela tipicidade, pela punibilidade e pela viabilidade, de maneira a verificar a presença de um *"suporte probatório mínimo a indicar a legitimidade da imputação e se traduz na existência, no inquérito policial ou nas peças de informação que instruem a denúncia, de elementos sérios e idôneos que demonstrem a materialidade do crime e de indícios razoáveis de autoria".*[53]

A busca de termos na rede mundial de computadores, por si só, desvinculada de outros elementos, por não constituir ilícito, não pode gerar suspeita, sob pena de indevida limitação ao direito de acesso à informação, potencialmente discriminatória diante de estigmas e vieses que podem influenciar a construção da figura do "suspeito".

---

exercício regular da ação penal estar amparada por "elementos sérios, idôneos, a mostrar que houve uma infração penal, e indícios, mais ou menos razoáveis, de que o seu autor foi a pessoa apontada" (TOURINHO FILHO, Fernando da Costa. **Processo penal**. 11. ed. São Paulo: Saraiva, 1989, p. 445.

52 JARDIM, Afrânio Silva. **Direito processual penal**. 9. ed. Rio de Janeiro: Forense, 2000, p. 97.

53 Voto proferido pelo Min. Dias Toffoli no Inq 3719/DF.

A pesquisa por palavras aleatórias na *internet*, por si só, não é um ato ilícito e, por isso, insuficiente para o oferecimento da denúncia em face de qualquer pessoa.

Portanto, para o oferecimento da denúncia, mostra-se necessário, em atenção ao instituto da justa causa, corroborar os dados telemáticos obtidos a partir da decretação do afastamento do sigilo com outros indícios que apontem a ocorrência do crime e a participação do investigado no delito apurado.

Desse modo, como salvaguarda geral ligada aos deveres-poderes investigativos, é de se salientar que é insuficiente para a instauração do processo-crime apenas o dado telemático possivelmente aleatório, destituído de outros indícios de materialidade e autoria, sendo necessário que seja corroborado por outros elementos colhidos na investigação.

Em relação a tal ponto, propõe-se a seguinte tese:

> É necessário para o oferecimento da denúncia que o dado telemático, possivelmente aleatório, seja corroborado por outros elementos colhidos na investigação.

8. MODULAÇÃO DE EFEITOS: A EXPLICITAÇÃO DE REQUISITOS SISTÊMICOS, O REGIME DE TRANSIÇÃO E A PRESERVAÇÃO DOS ATOS JÁ PRATICADOS.

O presente julgamento, que já é paradigmático no tocante ao tratamento dos dados telemáticos no âmbito do processo penal, certamente terá impacto importante nas investigações e processos em curso, dada a amplitude do tema tratado.

Em virtude das teses que ora se propõe, notadamente da explicitação dos mecanismos de salvaguarda que decorrem da leitura sistemática do microssistema protetivo de dados e comunicações, é recomendável, na linha do que preceituado no art. 927, § 3º, do Código de Processo Civil, que haja a modulação dos efeitos das teses, possibilitando regime de transição consentâneo com a segurança jurídica e com a confiança dos diversos atores nos procedimentos criminais.

O art. 927, § 3º, do Código de Processo Civil prevê a possibilidade, diante de alteração de jurisprudência dominante, da modulação dos efeitos da alteração no interesse social e no da segurança jurídica.

O referido dispositivo é de ser articulado com a Lei 13.655/2018, que, em abril de 2018, inseriu dez novos artigos na Lei de Introdução às Normas do Direito Brasileiro – LINDB. Os novos artigos (20 a 30) prevêem

regras sobre segurança jurídica e eficiência na criação e na aplicação do direito público e regulando a compensação de prejuízos e benefícios nos processos estatais[54].

Interessam em especial ao presente caso os arts. 23 e 24 da Lei de Introdução.

O primeiro consigna que a "*decisão administrativa, controladora ou judicial que estabelecer interpretação ou orientação nova sobre norma de conteúdo indeterminado, impondo novo dever ou novo condicionamento de direito, deverá prever regime de transição quando indispensável para que o novo dever ou condicionamento de direito seja cumprido de modo proporcional, equânime e eficiente e sem prejuízo aos interesses gerais.*"

Já o segundo preceitua que a "*revisão, nas esferas administrativa, controladora ou judicial, quanto à validade de ato, contrato, ajuste, processo ou*

[54] De um ângulo objetivo, os novos arts. 20 a 30 da LINDB têm como âmbito de incidência situações envolvendo normas dos ramos do direito público sob a tutela primária da Administração Pública como um todo. Já sob a ótica subjetiva, o dispositivo alcança as partes em processos nas esferas administrativa, controladora e judicial em todos os níveis federativos (federal, estadual, distrital e municipal).
Acerca de tais preceitos, a ementa da Lei 13.655/2018 não deixa dúvidas: esclareceu trata-se de *"disposições sobre segurança jurídica e eficiência na criação e aplicação do direito público"*. Vê-se que as disposições não são de direito administrativo em sentido estrito (ou seja, não versam sobre institutos específicos desse ramo do direito, a exemplo dos contratos administrativos, servidores públicos e outros temas), mas constituem lei geral de direito público.

norma administrativa cuja produção já se houver completado levará em conta as orientações gerais da época, sendo vedado que, com base em mudança posterior de orientação geral, se declarem inválidas situações plenamente constituída".

Entende-se que, no mister de guarda da Constituição Federal, o STF, fixando a orientação constitucional acerca do tema e concretizando o direito material, pode examinar os atos e fatos processuais para se identificar a eventual ocorrência de efeitos negativos e surpreendentes dos quais possam resultar, em vez da efetivação do projeto constitucional, situações que agravem em concreto a harmonia dos fatos com o ordenamento jurídico posto.

É esta a lógica que fundamenta a previsão pelos dispositivos da necessidade de um regime de transição e de preservação dos atos praticados no contexto das orientações pretéritas e agora superadas.

O pressuposto lógico que inspira os dispositivos é a ideia de que processos estatais de todas as esferas envolvem atividade de risco para os direitos dos envolvidos e hão de servir como instrumento de promoção da efetividade do ordenamento jurídico, sem imposição de prejuízos anormais ou injustos.

Conjugam-se nesse cenário a modulação e a mitigação de efeitos excessivamente danosos e onerosos, viabilizando que o Judiciário, em seu mister, evite que a tramitação do processo seja em si motivadora do oposto a que se presta o direito processual: a promoção do equilíbrio de interesses e a distribuição da justiça.

No caso ora em análise, tem-se que a solução mais adequada é a modulação dos efeitos da decisão embargada.

Apresenta-se o requisito objetivo da alteração da jurisprudência dominante na medida em que ainda estava pendente de pacificação a questão dos parâmetros a serem observados no afastamento do sigilo sobre dados telemáticos de pessoas indeterminadas.

Já resulta como de patente interesse social harmonizar, na medida do possível, os ônus suportados pelos interessados no processo-crime, notadamente ante a amplitude da tese e o impacto sobre número expressivo de investigações e processos em curso.

A modulação surge como medida de equilíbrio para que os efeitos das teses fixadas, em especial das teses que explicitam salvaguardas sistêmicas na proteção dos dados, ocorram a partir da data do julgamento pelo STF, momento em que se pacificou a premissa a ser adotada,

excetuando-se os casos já encerrados e permitindo às investigações em curso adaptarem-se aos preceitos fixados.

Tal solução leva em conta a inteligência dos arts. 23 e 24 da LINDB, evitando prejuízo ou benefício anormal aos interessados no processo criminal.

A medida permite que não sejam atingidas as investigações já realizadas até o presente momento, tutelando o direito das vítimas e familiares à memória e à verdade na perspectiva da investigação com a devida diligência, evitando a repetição desnecessária de atos ou mesmo a impunidade em contextos nos quais não houve prejuízo aos investigados, e, nas em curso, possibilita à autoridade requerente a complementação das informações necessárias às medidas requeridas consoante os parâmetros a serem definidos pela Suprema Corte.

Em face do exposto, requer-se, desde já, que as salvaguardas eventualmente fixadas pela Suprema Corte, notadamente aquelas que não correspondam à literalidade explícita das normas hoje vigentes, sejam aplicadas apenas aos pedidos de afastamento de sigilo em curso ou futuros, possibilitando às autoridades requerentes a complementação dos pedidos, nos moldes a serem fixados pelo STF.

9. APLICAÇÃO DO DIREITO AO PROCESSO

Os recorrentes defendem que inexistiria autorização constitucional e legal que possibilite o afastamento do sigilo de dados telemáticos de indivíduos indeterminados, pois a premissa básica, no ordenamento jurídico nacional, que permite o afastamento de sigilo é a demonstração de indícios de envolvimento do indivíduo na prática da infração penal investigada. Desse modo, a manutenção da determinação judicial de afastamento do sigilo de dados telemáticos de indivíduos indeterminados configuraria uma nova modalidade, inconstitucional, de *fishing expedition*.

Conforme explicitado no item de exame do tema, mostra-se compatível com a Constituição Federal a possibilidade de afastamento de dados telemáticos, no âmbito de procedimentos penais, ainda que em relação a pessoas indeterminadas.

Na realidade, mostrar-se-ia incompatível com a ordem jurídico-constitucional entendimento pelo qual fosse vedada a transferência de dados que possam contribuir para a efetivação da persecução penal e para a elucidação de crimes, sobretudo quando se sabe que tais dados hão de ter o sigilo preservado pela autoridade pública.

Afirmar que o uso de um determinado meio investigativo seria, por si, uma *fishing expedition* é inadequado, na medida em que esta depende menos do instrumento adotado e mais dos parâmetros nos quais ele é utilizado no caso concreto.

Na hipótese de uso em análise, não se trata de subterfúgio para *full discovery*, como vedado no sistema norte-americano, ou de demanda ampla baseada em palpites ou ilações. Trata-se, ao contrário, de acesso a material relevante à linha investigativa – delimitado, especificamente, por expressões precisas de busca, área geográfica e período – em posse de empresa estrangeira, com representação oficial no Brasil, que se submete às disposições do artigo 12 da Lei nº 12.965/2014 (Marco Civil da Internet).

Os parâmetros constitucionais e legais suficientes para o uso da medida já são previstos no ordenamento pátrio, notadamente a partir das disposições constantes do microssistema protetivo composto pelas três leis que tratam de dados: Lei nº 9.296/96, Lei nº 12.965/2014 e Lei nº 13.709/2018.

Em especial, o Marco Civil da Internet, nos arts. 10 e 22, expressamente autoriza o afastamento do sigilo sem a necessidade de individualização da pessoa atingida.

A Lei nº 12.965/2014, no art. 22, traz os requisitos para admissão do requerimento de afastamento no caso dos registros de conexão ou de registros de acesso a aplicações de internet: ***(i)*** apresentação de fundados indícios da ocorrência do ilícito; ***(ii)*** justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e ***(iii)*** delimitação do período ao qual se referem os registros.

Tais exigências têm o objetivo de evitar requerimentos de acesso desprovidos de embasamento mínimo ou sem limitação temporal, de modo que o fornecimento dos registros seja a exceção, privilegiando-se, sempre que possível, o sigilo das informações referentes à intimidade e à vida privada do usuário.

Quando os dados telemáticos solicitados forem além dos já referidos e abrangerem informações pessoais ou outras que possam contribuir para a identificação do usuário ou do terminal, na forma do art. 10 do MCI, cumpre à autoridade requerente, em leitura sistêmica, também justificar fundamentadamente: *(i)* a necessidade da medida para a investigação em concreto, que há de ser subsidiária em relação a outros meios de prova menos gravosos a direitos de terceiros; e *(ii)* a pertinência das informações obtidas em relação ao fato investigado, que hão de ser especificadas no máximo possível com base em elementos identificativos e contextuais atinentes ao possível ilícito.

No presente caso, apenas pelas peças coligidas no mandado de segurança, não é possível desde logo se aferir, diante dos dados requeridos[55] e do avançar das investigações pela própria passagem do tempo, se as condicionantes ora apontadas no presente parecer e que se relacionam ao juízo acerca da necessidade e subsidiariedade da medida foram observadas e ainda se revelam em relação ao requerimento.

Desse modo, preconiza-se a devolução do processo ao Tribunal de origem, para que o reaprecie à luz das diretrizes a serem fixadas pela Suprema Corte, permitindo-se, ainda, caso a autoridade policial entenda necessário, a renovação do requerimento, nos moldes estabelecidos pelo STF.

Em face do exposto, opina o PROCURADOR-GERAL DA REPÚBLICA pelo provimento parcial do recurso, com devolução do processo para reapreciação pelo Tribunal de origem à luz dos parâmetros a serem fixados pelo STF e, considerados a sistemática da repercussão geral e os efeitos do julgamento deste recurso em relação aos demais casos que tratem ou venham a tratar do mesmo Tema 1148, sugere a fixação da seguinte tese, com a modulação de efeitos proposta no item 7 do presente parecer:

---

[55] O juízo de primeiro grau determinara às duas sociedade empresariais o fornecimento da *"identificação dos IP's ou 'Device IDs' que tenham se utilizado do Google Busca (seja através do aplicativo ou sua versão WEB) no período compreendido entre o dia (…), para realizar consultas dos seguintes parâmetros de pesquisa (…)"*.

É permitido o afastamento de sigilo de dados telemáticos, no âmbito de procedimentos penais, ainda que em relação a pessoas indeterminadas, nos seguintes parâmetros:

I – Aplica-se, no tocante aos requerimentos de registros de conexão ou acesso a aplicações de internet, os requisitos previstos no art. 22 da Lei nº 12.965/2014 (Marco Civil da Internet): a apresentação dos fundados indícios da ocorrência do ilícito; a justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e a delimitação do período ao qual se referem os registros.

II – Quando os dados telemáticos solicitados forem associados a dados pessoais ou outras que possam contribuir para a identificação do usuário ou do terminal, cumpre à autoridade requerente também justificar fundamentadamente:

a) A necessidade da medida para a investigação em concreto, que há de ser subsidiária em relação a outros meios de prova menos gravosos a direitos de terceiros;

b) A pertinência das informações obtidas em relação ao fato investigado, que hão de ser especificadas no máximo possível com base em elementos identificativos e contextuais atinentes ao possível ilícito.

III – A transferência de dados às autoridades requerentes há de ocorrer unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.

IV – Cumpre à autoridade requerente providenciar ao final das investigações a inutilização dos dados obtidos de terceiros que sejam desnecessários para a continuidade do processo-crime, mediante requerimento ao juízo

competente, na forma do art. 9º da Lei nº 9.296/96, com a oitiva prévia dos demais interessados.

V – Incumbe aos interessados no processo-crime, sob pena de preclusão, caso pretendam a produção de prova para a qual seja imprescindível ter acesso aos dados telemáticos de terceiros coligidos nas investigações, postular sua realização até a intimação para manifestar-se sobre a inutilização dos dados, de modo fundamentado, a fim de serem preservados os elementos imprescindíveis à diligência.

VI – É necessário para o oferecimento da denúncia que o dado telemático, possivelmente aleatório, seja corroborado por outros elementos colhidos na investigação.

Brasília, data da assinatura digital.

Augusto Aras
Procurador-Geral da República
Assinado digitalmente

GB/VCM/FS/MC/PDX/LDCF