Nota Técnica - Ação Direta de Constitucionalidade nº 51

Alexandra Krastins Lopes
Gabriel Araújo Souto
José Renato Laranjeira de Pereira
Nayara Fatima Macedo de Medeiros Albrecht
Paulo Henrique Atta Sarmento
Thiago Moraes

Introdução

O **Laboratório de Políticas Públicas e Internet - LAPIN**, projeto de extensão da Universidade de Brasília, vem à presença de Vossa Excelência manifestar seu interesse em participar da audiência pública relativa à **Ação Direta de Constitucionalidade nº 51,** proposta pela Federação das Associações das Empresas Brasileiras de Tecnologia da Informação - ASSESPRO NACIONAL e que versa sobre o Decreto Executivo Federal nº 3.810, de 2 de maio de 2001 (Decreto 3.810/2001).

O referido Decreto promulgou o Acordo de Assistência Judiciário-penal entre o Brasil e os Estados Unidos da América, mecanismo conhecido como "*Mutual Legal Assistance Treaty*", doravante "MLAT". Destarte, a ADC em questão versa sobre a constitucionalidade de normas de cooperação jurídica internacional entre autoridades brasileiras e estrangeiras. Alega a requerente que o Tratado tem recebido recusa de aplicabilidade relativa às empresas de tecnologia sob o argumento de violação da soberania nacional. Fato é que a questão incide sobre diferentes temas relacionados à área de tecnologia, entre eles a proteção e o compartilhamento de dados pessoais. Dessa forma, a ADC diz respeito ao objeto de estudo do LAPIN, a saber, os impactos sociais da relação entre tecnologia e direito.

Cumpre, portanto, destacar a importância da admissão do LAPIN/UnB na audiência pública sobre a ADC nº 51. Preliminarmente, cabe discorrer sobre as atividades do LAPIN e seu papel na geração e difusão de dados e evidências acerca de políticas públicas que afetam a Internet. O LAPIN é um projeto de extensão da Universidade de Brasília que reúne pesquisadores, estudantes e especialistas em questões afetas às tecnologias em uma perspectiva voltada à compreensão do impacto de políticas sobre direitos digitais na sociedade. O LAPIN tem origem na Faculdade de Direito da UnB e reúne estudantes de diversas áreas de formação, sobretudo do Direito e da Tecnologia da Informação. Assim,

resta evidente a pertinência temática do objeto da ADC para os estudos e as demais ações desenvolvidas pelo LAPIN/UnB.

Adicionalmente, o LAPIN destaca sua contribuição acadêmica à questão discutida na presente arguição. A contribuição consistiu na realização de debates, participação de conferências, organização de eventos e coleta e análise de informações sobre temas diretamente atingidos pelos dispositivos legais que a requerente visa declarar a constitucionalidade. Sobretudo, o LAPIN é um grupo independente de financiamento privado, o que corrobora seu caráter técnico.

Considerando a complexidade do tema da audiência convocada, o LAPIN acredita na importância da participação de especialistas em tecnologia da informação, tendo em vista os impactos da decisão em questão na área de tecnologia e na promoção dos direitos digitais. Disso resulta que suas exposições serão de extrema relevância para a solução da controvérsia jurídica discutida na ADC. Ante o exposto, o LAPIN tem plena convicção de que poderá contribuir para a discussão da audiência convocada mediante a indicação de seus representantes.

1. A relação entre segurança pública e privacidade

A presente ação trata do impacto das novas tecnologias na privacidade dos cidadãos e quais os limites do Estado na esfera individual ao priorizar a segurança pública sobre o direito à privacidade. Este debate é de grande importância no contexto constitucional, pois irá servir como paradigma que repercutirá em toda formação da cultura de proteção de dados pátria.

Para melhor elaborar este tema, será tratado inicialmente o **conceito atual de privacidade** e como a doutrina delimita o espectro acobertado por este. Posteriormente, serão apresentados parâmetros cabíveis para aferir o limite da atuação Estatal em prol do interesse coletivo visando a segurança pública, e, por fim, será realizada uma ponderação de eventuais colisões do direito à privacidade e o interesse legítimo estatal à segurança pública.

a) Privacidade Contextual e a Expectativa Razoável de Privacidade

O conceito de privacidade passou por diversas mutações com o desenvolvimento do convívio social. Inicialmente, limitou-se a um confronto entre esfera pública, onde as informações são de livre tráfego, e privada, onde é resguardada a intimidade. Contudo, esta definição se mostrou defasada, acentuando-se com os avanços de novas tecnologias, a partir das quais o âmbito da esfera pessoal passa a se intercalar em diversos aspectos com o que outrora se

considerava público. Tornou-se assim obsoleta qualquer definição estanque de privacidade intercambiável a diferentes contextos.[1]

Posto este dilema, a autora canadense Helen Nissenbaum cunhou o conceito de **Privacidade Contextual**, onde a definição de privacidade se amolda a diferentes cenários[2]. De acordo com esta doutrina, as normas que regulam as trocas de informação somente farão sentido caso analisadas de maneira holística, em conjunto com o sistema em que estejam inseridas.

Ao se analisar uma relação de troca de informações, quatro itens devem ser aferidos para se delimitar como deverá ser feito o tratamento destas:[3] (i) o contexto que esta relação está inserida; (ii) os atores envolvidos nesta; (iii) o conteúdo desta informação e; (iv) o princípio de transmissibilidade desses dados , item referente a qual o vetor desta troca de informação, a possibilidade de transmissão destes a terceiros, dentre outros aspectos.

Para melhor visualização destes conceitos, abordamos uma situação hipotética. Em uma relação de saúde entre o paciente e seu médico, podemos aferir neste quadro (i) o contexto, transcorrendo no âmbito da saúde; (ii) os agentes envolvidos, sendo estes paciente e médico; (iii) seu conteúdo, referentes à saúde do paciente; e (iv) o princípio de transmissibilidade, sendo preconizado o sigilo das informações obtidas, salvo por motivo justo, dever legal ou consentimento por escrito do paciente.

Ainda no exemplo médico, o ordenamento jurídico pátrio cunhou a norma informacional reguladora da relação, o Código de Ética Médica, previsto na Resolução do Conselho Federal de Medicina nº 2.217, de 2018, que, em seu art. 73, estabelece as normas que devem pautar a conduta médica no que tange à privacidade das informações prestadas pelo paciente.[4] Se a expectativa de privacidade não for respeitada, tem-se a violação da privacidade contextual.

O autor americano Daniel Solove é igualmente aderente desta concepção de privacidade contextual.[5] Contudo, assevera que a construção de normas informacionais não pode se ater

---

[1] DECEW, Judith Wagner. **In Pursuit of Privacy**: Law, Ethics, and the Rise of Technology. Ithaca, NY: Cornell University Press, 1997, p. 10.

[2] NISSENBAUM, Helen. **Privacy in Context**: Technology, Policy, and the integrity of Social Life. Stanford,CA: Stanford Law Books, 2010, p. 140.

[3] Ibidem, pp. 140-145.

[4] É vedado ao médico:

Art. 73. Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente.

§ único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha (nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento); c) na investigação de suspeita de crime, o médico estará impedido de revelar segredo que possa expor o paciente a processo penal.

[5] SOLOVE, Daniel J. **Understanding Privacy**. Cambridge, MA: Harvard University Press, 2008, pp. 48-49.

somente à privacidade contextual, devendo haver igualmente um certo grau de generalidade, de modo a equilibrar estas duas visões. Ao se priorizar observação contextual, a visão holística torna-se distorcida, assim como, priorizando observação generalista, prejudica-se a efetividade da norma, afastando-a da realidade.

A Teoria da Privacidade Contextual está intrinsecamente conectada à da **Expectativa Razoável de Privacidade** (*Reasonable Expectation of Privacy*, no original), desenvolvida pela Suprema Corte dos Estados Unidos da América no contexto da vigilância.

O conceito foi introduzido em *Katz*,[6] e mais recentemente aprimorado em *Jones*,[7] onde foi decidido que um mandado judicial para coleta de dados pessoais para fins de vigilância só pode ser concedido se a expectativa razoável de privacidade for verificada em dois aspectos: (i) no aspecto subjetivo, onde se leva em consideração as expectativas de privacidade do indivíduo vigiado; e (ii) no aspecto objetivo, onde a sociedade estaria disposta a reconhecer aquela expectativa individual como razoável.

Para ilustrar a aplicação do teste da Expectativa Razoável de Privacidade, trazemos o exemplo de um indivíduo que se comunica com alguém utilizando um aplicativo de mensagens instantâneas como WhatsApp, Facebook Messenger, Telegram e Wire.

A nível individual, um cidadão brasileiro, confiante da proteção que lhe é garantida pelo art. 5º, XII, da CF/1988,[8] terá uma expectativa de que sua comunicação ocorrerá sob sigilo. Nesse sentido, o fato de seus dados pessoais eventualmente serem transferidos para bases de dados estrangeiras não é relevante aqui, pois o que este indivíduo espera é que o ordenamento jurídico brasileiro irá protegê-lo sempre que utilizar serviços de comunicação oferecidos no território nacional.

A nível social, por sua vez, as pessoas naturais localizadas no território nacional provavelmente reconheceriam a expectativa daquele indivíduo como razoável, uma vez que elas mesmas esperam possuir o mesmo nível de proteção ao utilizar essas ferramentas de comunicação. Contudo, a sociedade também pode reconhecer que o direito à privacidade pode vir a ser limitado devido aos interesses de segurança pública, que, em tese, visa proteger os cidadãos. Dessa forma, o contexto em que essa comunicação ocorre será fundamental para alcançar uma conclusão de qual seria a expectativa razoável de privacidade no nível social.

---

[6] *Katz v. United States*, 389 US 347 (1967).
[7] *United States v. Jones*, 565 US 400 (2012).
[8] XII - é **inviolável o sigilo da correspondência** e das **comunicações** telegráficas, **de dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (grifos nossos)

Nos próximos parágrafos, apresentaremos elementos que ajudarão essa Suprema Corte a refletir sobre qual seria a Expectativa Razoável de Privacidade das pessoas naturais que usam serviços de comunicação online sob a proteção do ordenamento jurídico brasileiro. Desde já, sugerimos que a leitura seja realizada sob a ótica da proteção à privacidade: o art. 5º, XII, da CF/1988, que deixa explícito que a limitação desse direito para fins de investigação criminal deve ser sempre a exceção. Logo, espera-se que salvaguardas sejam estabelecidas nas situações em que essas restrições ocorram.

b) Ponderação da busca por segurança pública frente a privacidade

Ao abrir mão do poder de autotutela para o Estado, a sociedade concedeu ao poder público a atribuição de resolução de conflitos originados desta, devendo o poder público utilizar-se de suas prerrogativas para a melhor resolução de tensões sociais.

Para alcançar este objetivo, fora outorgado ao Estado atribuições de investigação, onde órgãos competentes deveriam prosseguir com todas ações quais lhe fossem cabíveis e legais. Caso fossem necessárias intromissões a direitos fundamentais de cidadãos, estes deveriam ser anuídos por outro órgão do poder público, mais comumente o poder judiciário, que, ao conceder ao agente público um mandado judicial, autorizaria a infração momentânea de direitos contidos na esfera privada do investigado.

Todavia, para que a autoridade judicial autorize essa conduta, **os ordenamentos estabeleceram requisitos mínimos para fundamentar esta intromissão na esfera pessoal.** No ordenamento pátrio, podemos encontrar exemplo desta limitação no art. 5º, Inciso XI, onde, no âmbito criminal, somente é permitida a invasão do lar em caso de flagrante delito ou por determinação judicial.

Como já mencionado, a Constituição Federal, em seu art. 5º, XII, prevê a inviolabilidade dos dados, direito que repercute no ordenamento no art. 1º, § único da lei nº 9.296, de 1996,[9] e, mais recentemente, no art. 7º, incisos II e III, do Marco Civil da Internet, Lei nº 12.965/2014. [10] Nestes termos, a norma informacional da troca de informações pela internet no Brasil

[9] Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

[10] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

possui requisitos rígidos, gerando assim uma expectativa de inviolabilidade desses dados ao cidadão.

Estabelecidos estes parâmetros, a doutrina traz duas dimensões que devem ser ponderadas no momento de intromissão do poder público na esfera privada. Primeiramente, deve ser questionado o respaldo deste amparo legal, se este é ou não capaz de resguardar o cidadão de excessos estatais. Posteriormente, deve ser questionado qual o instrumento normativo que regulará esta intromissão estatal[11].

Sendo assim, resta evidenciado que o ordenamento possui dispositivos normativos aptos a resguardar o direito dos indivíduos ao sigilo e à inviolabilidade de seus dados e sua comunicação pela internet, salvo para fins específicos de investigação criminal, onde salvaguardas sejam estabelecidas, em particular a prévia autorização judicial. Passaremos agora à análise do instrumento normativo que deve regular esta intromissão.

c) Ponderação do direito à privacidade e o interesse legítimo à segurança pública

A ponderação entre o direito à privacidade e o interesse legítimo à segurança pública vem sendo travado constantemente em diversos ordenamentos jurídicos. Em sociedades que anseiam por menos violência e maior proteção por parte do poder público, a segurança pública ganha apelo e, paulatinamente, conquista espaço sobre a privacidade. Entendemos que este possa ser o caso brasileiro, devido ao seu quadro socioeconômico marcado por desigualdade e violência. Neste contexto, , a privacidade não desaparece imediatamente, mas sim erode-se gradativamente, até o momento em que a sociedade percebe a gravidade deste dano (*slippery slope*).[12]

O maior instrumento para que se evite uma erosão plena da privacidade dos cidadãos é o **devido processo legal.** Restou inequívoco que, por não ser absoluto, o direito à privacidade, para que seja encurtado pelo poder público, deve ser resguardado pelo mandado judicial. E, uma vez concedida permissão judicial, deverá esta intromissão ser a menos danosa para o indivíduo.

Em *Carpenter*,[13] um caso em que autoridades policiais estadunidenses solicitaram a informação locacional de torres de celulares (*Cell-Site Location Information* - CSLI), a Suprema Corte dos EUA afirmou que mandados judiciais dessa espécie devem possuir uma

[11] SOLOVE, Daniel J. **Nothing to Hide: The False Tradeoff Between Privacy and Security**. New Haven, CT: Yale University Press, 2011, p. 115.
[12] Ibidem, p. 30.
[13] *Carpenter v. United States*, 585 US (2018).

causa provável e ser específicos, dado o teor de invasividade desse tipo de informação. Um raciocínio similar deve ser considerado na coleta de dados de usuários de serviços de mídias sociais, que armazenam diversas informações sobre a vida privada de indivíduos.

Um exemplo de limitação desta intromissão são os entraves previstos na lei nº 9.296, de 1996, que regula o procedimento de interceptações telefônicas e que se aplica à interceptação do fluxo de comunicações em sistemas de informática.[14] Dentre as previsões, são constatáveis a preocupação quanto à exatidão do limite temporal,[15] assim como o limite do escopo da interceptação, devendo ser descartado aquilo que não tenha correlação com a investigação.[16]

Definida essa necessidade de observação do devido processo legal, assim como a preservação dos direitos fundamentais, passemos à análise das normas procedimentais reguladoras desta incursão do poder público na esfera pessoal da privacidade.

2. Aplicação do MLAT à transferência internacional de dados

(i) Ausência de conflito entre o MLAT e o Marco Civil da Internet.

Em sua peça memorial, o Instituto de Referência em Internet e Sociedade de Belo Horizonte, IRIS-BH, sabiamente argumentou que o conflito normativo aqui discutido entre o MLAT e o Marco Civil da Internet (MCI) é apenas aparente.

O art. 11 do Marco Civil da Internet, consiste em norma de direito **material**, ao tratar da noção de que provedores de serviços de internet devem seguir as leis brasileiras no que diz respeito ao tratamento de dados realizado em território nacional. Já o MLAT estabelece parâmetros **procedimentais** para uma atividade específica: a requisição de informações, documentos e outras atividades em território externo ao nacional.

A alegação de que haveria colisão entre as duas normas perde força ao se considerar que tratam de elementos distintos no ordenamento jurídico nacional. Certo é que, uma vez que

---

[14] Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

[15] Art. 5° A decisão será fundamentada, sob pena de nulidade, indicando também a **forma de execução da diligência**, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova. (grifos nossos)

[16] 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. (grifos nossos)

determinada empresa estrangeira estabelece subsidiária em território nacional, uma série de obrigações jurídicas brasileiras passam a incidir para que aquela proceda à prestação de bens ou serviços de que disponha. É isso o que determina o art. 11 do Marco Civil da Internet.

Tratam-se de elementos complementares, pois, uma vez que, se determinado caso concreto depende de informações e documentos localizados em terra estrangeira para fundamentar a decisão de um julgador, é natural que outras normas de direito internacional passem a incidir.

Afinal, ainda que o tratamento de dados que determinada subsidiária tenha realizado obedeça às normas nacionais, uma vez que a empresa tenha realizado a transferência desses dados para território estrangeiro, é plausível que se utilize, para o caso de requerer o retorno desses dados para o Brasil, norma procedimental que preveja a realização de cooperação internacional.

Por conta disso, não será aqui considerada a constitucionalidade ou não do MLAT. O tratado bilateral seguiu, ao que toda evidência indica, o procedimento formal adequado para sua recepção pelo ordenamento brasileiro e não foi identificada eventual colisão com o texto constitucional.

O que este Laboratório identifica, por outro lado, é que a questão aqui debatida gira em torno de outro eixo: **podem autoridades brasileiras exercer jurisdição sobre dados coletados em território brasileiro por empresas com um ou mais estabelecimentos situados no país ainda que estes dados tenham sido armazenados em território estrangeiro?**

(ii) O problema da territorialidade dos dados

Demonstrada a ausência de conflito entre o art. 11 do Marco Civil da Internet e o MLAT, vale trazer à luz decisão do Superior Tribunal de Justiça - STJ proferida nos autos do **INQ 784/DF**, que tratou da quebra de sigilo telemático em inquérito policial. No caso, foi determinado, em primeira instância, à subsidiária da Google no Brasil que entregasse ao Poder Judiciário informações existentes na conta de e-mail de um investigado.

A Google do Brasil afirmou que tais dados estariam armazenados em sua sede nos Estados Unidos, a Google Inc., e que portanto não teria acesso a seu conteúdo. Para solução da questão, a empresa sugeriu que fosse usada a via diplomática para obtenção desse conteúdo via MLAT.

Pela via recursal, o caso chegou ao STJ, que afirmou que a recusa da empresa representaria afronta à soberania nacional, uma vez que "dados que constituem elemento de prova não

podem se sujeitar à política de Estado ou empresa estrangeiros". Nesse sentido, alguns trechos da Questão de Ordem levantada pela Ministra Laurita Vaz chamam atenção:

> "Ora, o que se pretende é a entrega de mensagens **remetidas e recebidas por brasileiros em território brasileiro**, envolvendo supostos **crimes submetidos induvidosamente à jurisdição brasileira**.
>
> Nesse cenário, é irrecusável que o fato de esses dados estarem armazenados em qualquer outra parte do mundo não os transformam em material de prova estrangeiro, a ensejar a necessidade da utilização de canais diplomáticos para transferência desses dados.
>
> (…)
>
> Cumpre observar que a mera transferência reservada – poder-se-ia dizer interna corporis – desses dados entre empresa controladora e controlada não constitui, em si, quebra do sigilo, o que só será feito quando efetivamente for entregue à autoridade judicial brasileira, aqui.
>
> Insisto: **a simples transmissão de dados, resguardado seu conteúdo, entre as entidades pertencentes ao mesmo grupo empresarial, com a exclusiva finalidade de entrega à autoridade judiciária competente, no caso a brasileira, não tem o condão de sequer arranhar a soberania do Estado estrangeiro**.*"* (Grifos originais)

Dos pontos ressaltados, chamam atenção os argumentos levantados pela Ministra para definição da jurisdição sobre os dados. De acordo com sua fala, uma vez que as mensagens foram remetidas e recebidas por **brasileiros** em **território brasileiro** envolvendo supostos crimes submetidos à **jurisdição brasileira**, esses dados seriam obrigatoriamente acessíveis pelas autoridades nacionais sem a necessidade da utilização de canais diplomáticos. Soma-se a isso o fato de a empresa que detém esses dados ter subsidiária no Brasil.

Isso significa que, para o tribunal brasileiro, o que determina a jurisdição sobre um dado é o local de sua **coleta** e a **nacionalidade** de seu titular, não seu local de armazenamento. Além disso, a Questão de Ordem ressalta que a transferência de dados entre controladora e controlada não constitui invasão da soberania de Estado estrangeiro.

Em situação semelhante, em *Estados Unidos vs Microsoft,*[17] a Suprema Corte estadunidense lidou com o tema da utilização do MLAT para obtenção de dados objeto de investigação criminal. Os dados pessoais haviam sido coletados pela Microsoft nos Estados Unidos, mas

[17] United States v. Microsoft Corp., 584 U.S. (2018).

armazenados na Irlanda. Na ação, discutiu-se a necessidade de aplicação do MLAT para que as informações fossem acessadas pelas autoridades dos EUA.

Para os representantes do Governo dos Estados Unidos, a obtenção desses dados não faz com que o mandado de busca emitido pelas autoridades tenha reflexos extraterritoriais, uma vez que os dados poderiam ser acessados a partir do território norte-americano. Por isso, não haveria necessidade de recorrer à via diplomática para acessá-los. A Microsoft, por sua vez, alegou que a transmissão dos dados a partir da Irlanda significaria uma afronta à soberania do país europeu, e que o MLAT deveria ser invocado para obtenção dessas informações.

O caso Microsoft foi objeto de decisões diametralmente opostas em primeira e segunda instâncias. Pela falta de definição sobre o assunto, o processo alcançou a Suprema Corte, que aceitou decidir sobre seu conteúdo. Em paralelo, o Congresso dos EUA aprovou o CLOUD Act,[18] permitindo que autoridades estadunidenses tivessem acesso a dados armazenados no exterior de empresas que funcionem em seu território. O advento da legislação levou à perda de objeto da ação.[19]

Levando em conta os casos ocorridos no Brasil e nos Estados Unidos, podemos concluir que a **decisão quanto à requisição por autoridades investigativas nacionais de dados armazenados em território estrangeiro pode ser tomada com base em um dos seguintes critérios**:

a) **critério da coleta** - a jurisdição é definida pelo local em que houve a coleta dos dados e, portanto, onde foi ofertado o serviço que motivou essa coleta. Nos casos concretos, dispensaria o MLAT;
b) **critério pessoal** - a jurisdição é definida pelo local de residência do titular do dado. Nos casos concretos, dispensaria o MLAT;
c) **critério do local de acesso** - a jurisdição é definida pelo local em que haverá o acesso e a quebra de sigilo dos dados pelas autoridades. Nos casos concretos, dispensaria o MLAT;
d) **critério da localidade de armazenamento do dado** - o que define a jurisdição é o local em que os dados estão armazenados. Nos casos concretos, exigiria o MLAT.

Os três primeiros critérios, que concluem pela inaplicabilidade do MLAT, são muitas vezes tomados como anomalias pelo fato de consistirem em declarações unilaterais de jurisdição extraterritorial. Por outro lado, o último critério é visto como um óbice à eficiência da

[18] U.S. *Clarifying Lawful Overseas Use of Data Act,* H.R. 4943, 2018.
[19] ABREU, Jacqueline de Souza. **Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience**. RIL Brasília a. 55 n. 220 out./dez. 2018 pp. 233-257. Disponível em: <https://www12.senado.leg.br/ril/edicoes/55/220/ril_v55_n220_p233>. Acesso em: 02 de dezembro de 2019.

investigação penal, por determinar a obrigatoriedade de uso do lento MLAT e pela dificuldade em determinar a localidade de armazenamento do dado.

Tendo isso em vista, vale revisitar os conceitos de soberania e extraterritorialidade para acessar qual dos critérios seria o mais condizente com o direito doméstico e com normas internacionais sobre o tema.

Soberania é o princípio de direito internacional que prevê que cada Estado exerce autoridade suprema sobre seu território.[20] Por outro lado, **extraterritorialidade** pode ser concebida como a competência de um Estado de fazer, aplicar e executar normas sobre pessoas, propriedades ou eventos fora de seu território.[21] O exercício desse tipo de jurisdição extraterritorial é extremamente delicado justamente por poder interferir na noção de soberania estatal de outro território[22].

Em casos distintos, tanto o STJ quanto o governo estadunidense consideraram que suas ações não implicavam exercício de jurisdição extraterritorial. Apesar de a corte superior brasileira ter usado o argumento adicional de que o dado se referia a pessoa residente ou a acontecimento ocorrido em seu território e que por isso teria jurisdição sobre ele, ambos se pautaram no critério de local de acesso. Isso significa que o local de acesso ao dado definiria a autoridade de um país ou outro sobre ele.

Em parecer enviado à Suprema Corte dos EUA, Théodore Christakis fez uma análise dos critérios para determinação de jurisdição apresentados pelas partes no caso *Microsoft*, referentes ao critério do acesso e ao critério da localidade de armazenamento do dado. De acordo com ele, em contraposição ao argumento de que não haveria extraterritorialidade na

---

[20] BESSON, Samantha. **Sovereignty**. Oxford Public International Law. Disponível em: <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?rskey=FC7cA7&result=1&prd=OPIL>. Acesso em: 02 de dezembro de 2019.

[21] KAMMINGA, Menno T. **Extraterritoriality.** Oxford Public International Law. Disponível em: <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040?rskey=AXBMkf&result=1&prd=EPIL>. Acesso em: 02 de dezembro de 2019.

[22] CHRISTAKIS, Théodore. **Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States) (November 29, 2017)**. The White Book: Lawful Access to Data: The US v. Microsoft Case, Sovereignty in the Cyber-Space and European Data Protection, CEIS & The Chertoff Group White Paper, 2017. Disponível em: <https://ssrn.com/abstract=3086820>. Acesso em: 02 de dezembro de 2019. Doravante referenciado como "CHRISTAKIS, 2017".

pretensão do governo de acessar dados armazenados no exterior, tanto União Europeia,[23] quanto Irlanda afirmaram ser devido, no caso concreto, seguir o MLAT para solução da controvérsia.

O Article 29 Working Party,[24] antiga entidade de proteção de dados multilateral da União Europeia, recentemente substituída pelo Comitê Europeu para a Proteção de Dados, que estabeleceu diretrizes para proteção de dados no bloco regional, chegou a declarar que a coleta de dados pretendida pelo governo dos EUA configuraria interferência na soberania territorial de um Estado Membro europeu. A utilização do MLAT seria, portanto, necessária para a transferência internacional pretendida. Tal opinião foi a mesma do governo dos EUA em 2010, quando assinou seu MLAT com a União Europeia.

Com isso, o critério do local de acesso do dado poderia levar a consequências prejudiciais para a proteção de dados no plano internacional, como a possível adoção do mesmo mecanismo por outros países, independentemente de seu grau de proteção de direitos humanos como privacidade e liberdade de expressão.

Tal cenário conduziria a um enfraquecimento dos MLATs não só para a transferência de dados, mas de qualquer tipo de documento, bem ou pessoa investigada no plano internacional. Além disso, poderia gerar um grave conflito jurídico para as empresas, que não saberiam sobre as normas de qual país estariam obrigadas a seguir em suas operações de tratamento de dados[25].

O resultado disso poderia ser a **balcanização da internet**, pela qual empresas nacionalizariam seus servidores de modo a impedir que dados que dados saiam dos países em que são coletados, em um esforço de se protegerem de penalizações por violarem regras de proteção de dados em diferentes países.[26] Esses prestadores de serviços teriam seus modelos de negócio radicalmente afetados, e a consequência dessa posição seria uma dificuldade

---

[23] REDING, Viviane. **Carta de 24 de junho de 2014**. European Commission, 2014. Disponível em: <https://blogs.microsoft.com/wp-content/uploads/sites/149/2017/02/Scan-Ares-MEP-int-Veld-.pdf>. Acesso em: 02 de dezembro de 2019.

[24] ART 29 WP. **Data protection and privacy aspects of cross-border access to electronic evidence**. e-Evidence Statement, p. 9. Disponível em: <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801>. Acesso em: 02 de dezembro de 2019.

[25] CHRISTAKIS, 2017, p. 32.

[26] Idem, pp. 32-33.

muito maior de investigadores acessarem dados armazenados na nuvem quando buscassem provas em procedimentos penais.

Os efeitos mais sérios desse processo, no entanto, incidiriam sobre os usuários de internet. O processo de balcanização aumentaria a chance de indivíduos se isolarem de visões de mundo antagônicas para selecionarem ver cada vez mais somente o que está de acordo com seus interesses[27], tornando-se menos capazes de aceitar decisões importantes cujos valores diferem dos seus próprios[28]. O resultado dessa política de ciber-protecionismo seria a redução da internet a um fenômeno local, sem a troca de informações transfronteiriça com a qual estamos acostumados.[29]

Com isso, identifica-se que o conflito referente à identificação da jurisdição incidente sobre determinado dado é resultado da aplicação de um paradigma do mundo físico ao digital. É o **esforço de responder a um fenômeno novo utilizando imagens do passado que desencadeia a confusão que circunda a aplicação do MLAT a dados pessoais**.

MLATs funcionam relativamente bem para o compartilhamento internacional de provas físicas. Caso determinado documento físico necessário para a condução de uma investigação penal esteja em território estrangeiro, é necessário de fato que alguém vá buscá-lo em determinado ponto, o que exige a movimentação de um indivíduo em espaço sobre o qual incide outra jurisdição.

O mesmo, porém, não ocorre com dados. Sua natureza fluida, a possibilidade de sua transferência simultânea de uma fronteira a outra e sua divisibilidade (como ocorre na separação de dados e metadados, por exemplo) são fatores que levantam dúvidas a respeito de qual jurisdição tem poder sobre dados digitais.[30]

---

[27] SUNSTEIN, Cass. **Reuplic.com 2.0**. Princeton University Press, 2007, p. 215.
[28] ALSTYNE, Marshall Van; BRYNJOLFSSON, Erik. **Electronic Communities: Global Village or Cyberbalkans?**. Working paper, current version 96/09/20, 1997, p. 24. Disponível em: <http://web.mit.edu/marshall/www/papers/CyberBalkans.pdf>. Acesso em: 03 de dezembro de 2019.
[29] The Chertoff Group. **Microsoft V. United States: A Critical Inflection Point**. *In* Lawful Access to Data, 2017. Disponível em: <https://ceis.eu/wp-content/uploads/2017/12/Whitepaper_EN_WEB.pdf>. Acesso em: 03 de dezembro de 2019.
[30] CHRISTAKIS, 2017, p. 24.

Ao contrário do que ocorre com documentos físicos, dados armazenados na nuvem são muitas vezes tratados como a-territoriais, ou seja, desvinculados de territórios físicos.[31] A esse respeito, Jennifer Daskal considera esse tipo de dado como intangível, divisível e móvel, o que torna difícil determinar onde de fato está.[32] O usuário, na maioria das vezes, não tem a menor ideia de onde seus dados estão, porque eles são transportados de um servidor para outro na nuvem de maneira indiscriminada quando uma questão técnica surge.[33]

Um simples e-mail pode demonstrar como dados são muitas vezes desvinculados de qualquer fronteira. **Uma mensagem muitas vezes transita por diferentes países em seu caminho desde o remetente até o destinatário, ainda que os dois estejam localizados no mesmo território estatal.**[34] Isso demonstra que a localização física de dados segue meramente o arbítrio de quem oferece o serviço, e segue percursos completamente distintos dos utilizados por pessoas ou documentos físicos.

No que diz respeito à sua divisibilidade, dados armazenados em nuvem são regularmente copiados e armazenados em diferentes locais, para proteger o servidor de problemas técnicos. Apesar de essa prática de criar cópias não ser exclusiva de dados digitais, a a-territorialidade se complexifica pela agilidade de transferir dados de um país a outro de forma quase simultânea.

Outra técnica usada é a quebra de dados em múltiplas partes para facilitar sua administração por servidores. Isso significa que uma empresa que oferece serviço virtual poderia repartir um mesmo dado em diferentes partes e armazená-lo em locais distintos. Essa prática acrescenta mais uma camada de complexidade à determinação do paradeiro físico do dado.[35]

A dificuldade de se definir a localização exata em que dados são armazenados, bem como a desconexão entre o local de acesso e o local do dado, são elementos que demonstram a

---

[31] DASKAL, Jennifer C. **The Un-Territoriality of Data**. 125 Yale Law Journal 326; American University, WCL Research Paper No. 2015-5, 2015, pp. 366-367. Disponível em: <https://ssrn.com/abstract=2578229>. Acesso em: 02 de dezembro de 2019. Doravante referenciado como DASKAL, 2015.

[32] DASKAL, Jennifer C. **Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues**, 8 J. NAT'L SEC. L. & POL'Y, 2016, pp. 473-477. Disponível em: <http://jnslp.com/wp-content/uploads/2017/10/Law-Enforcement-Access-to-Data-Across-Borders_2.pdf>. Acesso em: 02 de dezembro de 2019. Doravante referenciado como DASKAL, 2016.

[33] CAUTHEN, John M. **Executing Search Warrants in the Cloud**, FBI L. ENFORCEMENT BULL, 2014. Disponível em: <http://leb.fbi.gov/2014/october/executing-search-warrants-in-the-cloud>. Acesso em: 02 de dezembro de 2019.

[34] Idem.

[35] DASKAL, 2015, (n 31), p. 368.

particularidade com que deve ser discutida a definição de jurisdição sobre dados. Isso exige que o direito trate essa matéria sob um paradigma diverso do qual documentos físicos são analisados. No entanto, a forma como a comunidade internacional vê o problema deve ser levada em conta.

Essa dificuldade também se reflete na **inviabilidade de se aplicar o critério da localidade de armazenamento do dado** para concluir sobre o poder de requisição de dados digitais pelas autoridades investigativas brasileiras.

(iii) Aplicabilidade e insuficiência do MLAT no contexto de fluxo transfronteiriço de dados.

Ao analisar o caso *Microsoft*, Daskal[36] ressalta como as posições tanto do governo estadunidense quanto da própria empresa são preocupantes. Ao buscar liberdade para obter dados localizados em outros países sem usar a via diplomática - **fazendo uso do critério do local de acesso**, pois -, afirma o governo dos Estados Unidos abriria precedentes para que outras jurisdições fizessem o mesmo.

Por um lado, isso tornaria o trabalho das autoridades mais célere no mundo inteiro. Entretanto, o critério da **requisição governamental direta aos provedores pode colocá-los em situações de conflito com legislações de outras jurisdições que lhe sejam aplicáveis.**

Conforme alegado pelo Facebook em seu requerimento de admissão nos autos da ADC 51, há conflito de normas domésticas entre Brasil e EUA no que se refere à revelação de comunicações eletrônicas. Nos termos da Seção 2702 do Stored Communications Act (SCA), legislação aplicável às empresas norte-americanas, é vedado aos provedores a divulgação de conteúdo de usuário de comunicação. Isso inclui o acesso a e-mails armazenados por qualquer terceiro exceto pelo Estado, desde que por meio do devido processo legal.

Portanto, caso uma subsidiária brasileira atenda à requisição governamental direta sem a utilização de meios de cooperação diplomática e forneça tais dados à Justiça brasileira, consoante o entendimento atual do STJ, sua matriz norte-americana estaria descumprindo a legislação estadunidense que lhe é aplicável ao fornecer tais dados.

[36] DASKAL, (n 32), 2016.

Tal forma de obtenção direta de dados **sem mecanismos de salvaguardas** pode também acarretar invasões de privacidade e ofensas a outros direitos humanos. Governos com pouco ou nenhum histórico de proteção de dados, privacidade e outros direitos humanos poderiam acessar os dados pessoais localizados em qualquer país e utilizá-los contra seus cidadãos sem respeitar princípios de proteção de dados e privacidade[37].

Em contraponto, uma vez prevalecendo a posição da Microsoft - **critério da localidade de armazenamento do dado** -, o **exercício da segurança pública seria radicalmente afetado**. Para cada crime ocorrido em um país que envolvesse somente indivíduos nele residentes cujos dados utilizados como provas estivessem armazenados em servidores externos, seria exigido o uso da via diplomática para resolução do caso.

Isso retardaria a solução de investigações que muitas vezes poderiam dizer respeito a interesses integralmente locais.[38]Além disso, consoante exposto, entende-se inviável definir a correta localidade de armazenamento do dado para fins de definição de jurisdição.

Apesar disso, deve-se admitir que, enquanto dados continuarem a ser considerados como elementos paralelos a documentos físicos, Estados continuarão a exigir a utilização de MLATs para que dados saiam de suas fronteiras com destino às autoridades dos países requisitantes.

Assim, a **via diplomática** é, apesar de mais onerosa e lenta para obtenção de dados armazenados extraterritorialmente, o único **meio** reconhecido internacionalmente para entrega de informações em meio eletrônico que hoje é **capaz de respeitar as diversas jurisdições internacionais, cujo eixo balizador são os direitos humanos**, conforme preconizado na Declaração Universal de Direitos Humanos das Nações Unidas.

A fixação jurídica de procedimentos para a investigação e para a persecução criminal é um tema muito importante para o Estado moderno, uma vez que a segurança jurídica na obtenção

---

[37] BARTON, Joe. **Reforming the Mutual Legal Assistance Treaty Framework To Protect the Future of the Internet**. Ohio State Law Journal Furthermore, 2018. Disponível em: <https://kb.osu.edu/bitstream/handle/1811/86110/OSLJ_Furthermore_V79_091.pdf?sequence=1>. Acesso em: 04 de dezembro de 2019.

[38] DASKAL, 2016, p. 489.

de provas ajudará a garantir a produção de resultados mais sólidos e, portanto, menos passíveis de serem considerados nulos[39].

Caso o Brasil continue a ignorar o MLAT para informações digitais, outros países poderão agir de forma recíproca e reivindicar a mesma autoridade para coletar dados localizados no Brasil. Isso levará a uma situação em que dificilmente o Estado brasileiro terá condições de fiscalizar quais dados estão saindo de seu território, o que pode afetar não só cidadãos de outros países, como os próprios residentes no Brasil. Desta forma, diversos direitos fundamentais das pessoas naturais protegidas pelo ordenamento jurídico brasileiro, em particular o da privacidade, correrão risco de violação.

Portanto, **o LAPIN considera que, por mais ineficiente e defasado, o MLAT é atualmente o único mecanismo pelo qual a requisição internacional de dados passa por um procedimento de devido processo legal, necessário para garantir a proteção de direitos fundamentais.**

Há **propostas de modernização dos MLATs**, tais como torná-los eletrônicos, promover ações educacionais aos países solicitantes, provimento de pessoal qualificado para os países requeridos, entre outras medidas.[40] Existem entendimentos sobre a execução de outros tipos de acordos internacionais bilaterais, nos quais os Estados envolvidos poderiam estruturar um conjunto de princípios jurisdicionais e estabelecer procedimentos padrão para operar como pré-condições para que seja permitida a requisição direta dos dados armazenados em território estrangeiro[41]. Nesse sentido, recentemente Estados Unidos e Reino Unido firmaram o ***US-UK Bilateral Agreement,***[42] que vigerá sob as regras estruturais do CLOUD Act.

Isto posto, ultrapassada a análise a respeito do atual estado da arte a respeito da transmissão internacional de dados para contextos de segurança pública, **vale considerar outras opções**

---

[39] VERONESE, Alexandre. **Cooperação jurídica e proteção de dados pessoais**. Disponível em: <www.jota.info/opiniao-e-analise/colunas/judiciario-e-sociedade/cooperacao-juridica-e-protecao-de-dados-pessoais-12042019>. Acesso em: 04 de dezembro de 2019.

[40] ABREU, Jaqueline de Souza. Op. cit., p. 248.

[41] DASKAL, Op. cit., p. 493.

[42] ESTADOS UNIDOS DA AMÉRICA. **Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime**. Government Publisher, 2019. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf>. Acesso em: 04 de dezembro de 2019.

para superação desse impasse que dependem inclusive de ações do Poder Legislativo. As alternativas evitariam os aspectos negativos que envolvem o funcionamento de MLATs e a problemática sobre a requisição direta de governos aos provedores da forma como é feita hoje.

Uma solução possível para promover o equilíbrio entre a efetivação do direito à segurança pública e à privacidade reside na **promoção da requisição direta pelo Poder Judiciário a provedores estabelecidos no país desde que** os **Estados envolvidos adotassem princípios gerais de proteção de dados e privacidade adequados.** Atendidos tais princípios, a requisição poderia ser efetuada diretamente, pois estariam garantidas as salvaguardas para proteção de direitos e garantias fundamentais.

Seria o caso se o ordenamento jurídico brasileiro hoje fosse capaz de oferecer um sistema bem estruturado para a proteção de dados no contexto da segurança pública. Infelizmente, a Lei 13.709/2018, a Lei Geral de Proteção de Dados, não será capaz de oferecer salvaguardas para esse tipo de situação, dado que seu art. 4º, III, declara sua inaplicabilidade a contextos de segurança pública.[43]

Recentemente, a Câmara dos Deputados criou uma comissão de juristas para a elaboração do anteprojeto de lei sobre **tratamento de dados pessoais para fins de segurança pública,** defesa nacional e atividades de investigação de infrações penais[44]. A medida acende as expectativas de que finalmente o tema possa ser regulamentado no país, de modo a garantir maior segurança jurídica.

De todo modo, até que uma lei federal específica para tratar sobre o tratamento de dados no contexto do direito criminal seja criada, cabe a esta Suprema Corte preencher o vácuo legislativo a partir das matrizes principiológicas estabelecidas por nossa Constituição Federal.

---

[43] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: (...)
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais.

[44] CÂMARA DOS DEPUTADOS. **Maia cria comissão de juristas para propor lei sobre uso de dados pessoais em investigações**. Notícias da Câmara, 2019. Disponível em: <www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/>. Acesso em: 02 de dezembro de 2019.

(iv) O princípio da dignidade da pessoa humana refletido no direito à privacidade

A estrutura dos direitos fundamentais é composta por duas dimensões: uma de cunho subjetivo e outra de cunho objetivo. A dimensão subjetiva faz menção às posições juridicamente protegidas por um direito fundamental as quais são direcionadas ao seu titular, dando-lhe a possibilidade de impor[45] judicialmente os seus interesses.[46] Já a dimensão objetiva deriva do reconhecimento de que direitos fundamentais consagram valores primordiais em uma comunidade política, não sendo apenas poderes que os indivíduos possuem em face do Estado, na medida em que impõem um dever de proteção por parte do poder público.[47]

Dessa forma, os direitos fundamentais devem preencher duas condições: a primeira é que "deve[m] tratar de interesses e carências que, em geral, podem e devem ser protegidos e fomentados pelo direito".[48] A segunda "é que o interesse ou carência seja tão fundamental que a necessidade de seu respeito, sua proteção ou seu fomento se deixe fundamentar pelo direito, quando sua violação ou não-satisfação significa ou a morte ou sofrimento grave ou toca no núcleo essencial da autonomia."[49]

Observa-se que, ao atender interesses coletivos, o Estado deve respeitar ao máximo a liberdade e esfera do poder privado. Conforme leciona Robert Alexy, a ponderação de princípios conta com a adequação, a necessidade e a proporcionalidade em sentido estrito.[50] Nesse sentido, Humberto Ávila define a necessidade como "a verificação da existência de meios que sejam alternativos àquele inicialmente escolhido pelo Poder Legislativo ou Poder

[45] Locke defende que todos nascem com direitos fundamentais, e estes devem ser blindados contra o mero uso da força, sendo necessário alguém de fora da esfera da disputa para decidir quem possui titularidade sobre o objeto discutido, sendo assim criado o Estado. Para decidir quem tem o melhor direito, isso pode ser decidido tanto por meio da jurisdição através da figura do juiz, tanto através de leis através dos legisladores. LOCKE, J. **Ensaio acerca do entendimento humano**. São Paulo: Nova Cultural, 1999.

[46] ALEXY, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros, 5. ed., 2006, p. 51.

[47] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. Porto Alegre: Livraria do Advogado, 11. ed., 2012, p. 152.

[48] ALEXY, Robert. **Direitos fundamentais no Estado constitucional Democrático**. Revista de Direito Administrativo, Ed. Renovar, Rio de Janeiro, 217:55-66, jul./set. 1999, p. 58 e ss.

[49] Ibid., p. 61.

[50] ALEXY, Robert. Op. cit., p. 60.

Executivo, e que possam promover igualmente o fim sem restringir, na mesma intensidade, os direitos fundamentais afetados."[51]

Denota-se que um meio eleito para a concretização de um fim deve ser adequado para tanto, ou seja, capaz de promovê-lo. Tal exame não se atém à esfera abstrata da norma, mas analisa também a realidade, pois, tratando de fim extrínseco, este se consolida no mundo dos fatos. Tal aspecto é um dos modos de otimizar a consolidação dos valores e ideais, haja vista que, ao permitir uma maleabilidade na aplicação da norma ao caso concreto, em razão do princípio da proporcionalidade, o ordenamento torna-se mais moldável ao contexto histórico, cultura e modificações sociais.[52]

Ademais, a ideia de que o **princípio fundamental da dignidade da pessoa humana funciona como fonte de direitos materialmente fundamentais não expressos na Constituição** se alia à sua posição de critério para reconhecer a fundamentalidade de um direito expresso em outro capítulo da Constituição ou em um tratado internacional. Portanto, o princípio fundamental da **dignidade da pessoa humana** funciona como um **critério para a identificação de direitos fundamentais**.[53]

Nesse sentido, os direitos ao respeito pela vida privada e à proteção de dados estão intimamente relacionados, são direitos distintos e autônomos. Eles também foram descritos como o direito "clássico" à proteção da privacidade, e como um direito mais "moderno", o direito à proteção de dados. Embora o primeiro seja entendido como um direito negativo, e o segundo como um direito positivo,[54] ambos se esforçam para proteger valores semelhantes, ou seja, a autonomia e a dignidade humana dos indivíduos, concedendo-lhes uma esfera pessoal na qual eles podem desenvolver livremente suas personalidades, pensar e moldar suas opiniões.[55]

Destaca-se, portanto, a vigência do princípio da dignidade da pessoa humana, positivado como cláusula pétrea no art. 1º, II da Carta Magna, e no art. XIV, parágrafo 3º do Decreto nº 3.810/2001,[56] o MLAT, como matriz geradora dos direitos fundamentais que devem ser

---

[51] ÁVILA, Humberto. **Teoria dos princípios: da definição à aplicação dos princípios jurídicos**. São Paulo: Malheiros, 13.ed., 2012, p. 192.
[52] SARMENTO, Daniel. **A ponderação de interesses na Constituição Federal**. Rio de Janeiro: Lúmen Juris, 2003, p. 87.
[53] CUNHA JÚNIOR, Dirley da. **Curso de Direito Constitucional**. Salvador: Editora Juspodivm,2011, pp. 538-539.
[54] Schertel, Laura. Privacidade, Proteção de Dados e Defesa do Consumidor. Linhas Gerais de um Novo Direito Fundamental. São Paulo: Saraiva, 2014.
[55] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Facial recognition technology: fundamental rights considerations in the context of law enforcement**, FRA Blog, 2019. Disponível em: <https://fra.europa.eu/en/publication/2019/facial-recognition>. Acesso em: 04 de dezembro de 2019.
[56] Artigo XIV - Busca e Apreensão

protegidos em um caso concreto. Deste modo, entende-se que, para a requisição de dados, deverá ser efetuada a proteção de interesses de indivíduos quanto a transferências dos seus dados garantindo um equilíbrio entre a segurança pública, a privacidade e a proteção de dados pessoais.

Tendo em vista que os direitos fundamentais são mandatos de otimização, ou seja, o legislador, além de respeitar os princípios fundamentais, deve procurar concretizar os direitos fundamentais por meio de leis, podendo configurar como omissão legislativa, **defende-se que esta c. Corte analise os direitos da privacidade e proteção de dados pessoais sob o prisma do direito fundamental à dignidade da pessoa humana, utilizando dos princípios da necessidade e proporcionalidade, à luz das normas pátrias e do direito comparado** que serão demonstrados a seguir.

4. Parâmetros para requisição de dados em investigações - necessidade e proporcionalidade

O Marco Civil da Internet estabelece, em seu art. 11, que seja aplicada a legislação brasileira às pessoas jurídicas com sede no exterior em ações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, desde que ofertem serviço aos consumidores brasileiros ou pelo menos um integrante do mesmo grupo econômico possua sede no Brasil, indo ao encontro do artigo 9, caput, e § 2°, da Lei de Introdução às Normas do Direito Brasileiro.

Além disso, o Código de Processo Penal, em seu art. 156, I,[57] ordena que o juiz observe os princípios da adequação, da necessidade e da proporcionalidade ao ordenar produção de provas. O mesmo vale para a apreciação de pedidos de medidas cautelares de produção de provas, positivado no seu art. 282, I e II.[58]

O Estado tem a obrigação de provar que suas atividades de vigilância das comunicações são necessárias para alcançar um objetivo legítimo. Dessa forma, a necessidade faz um juízo

---

(...)
3. A Autoridade Central do Estado Requerido poderá requerer que o Estado Requerente aceite termos e condições julgados necessários à proteção de interesses de terceiros quando da transferência de um bem.

[57] Art. 156. A prova da alegação incumbirá a quem a fizer, sendo, porém, facultado ao juiz de ofício:

I – ordenar, mesmo antes de iniciada a ação penal, a produção antecipada de provas consideradas urgentes e relevantes, observando a necessidade, adequação e proporcionalidade da medida;

[58] Art. 282. As medidas cautelares previstas neste Título deverão ser aplicadas observando-se a:
I - necessidade para aplicação da lei penal, para a investigação ou a instrução criminal e, nos casos expressamente previstos, para evitar a prática de infrações penais;
II - adequação da medida à gravidade do crime, circunstâncias do fato e condições pessoais do indiciado ou acusado.

comparativo, exige que, quando o meio escolhido restringe umdireito fundamental, sejam buscados meios alternativos que não gerem colisões entre o objetivo legítimo (*in casu*, segurança pública) e o direito afetado (*in casu*, o direito à privacidade).

No contexto legislativo estadunidense, não há uma legislação uniforme sobre proteção de dados pessoais tal como na Europa. Uma série de leis federais e estaduais incidem sobre a requisição de dados em um contexto de investigação.

Ao passo que as leis estaduais variam, é comum ter as políticas relativas à privacidade escritas e delineadas para conhecimento geral. Várias leis restringem a coleta de dados provenientes de comunicações pessoais, as quais incluem e-mails pessoais e profissionais, redes sociais e ligações telefônicas.

Como visto acima, no caso dos Estados Unidos, o CLOUD Act modificou o procedimento para o governo dos Estados Unidos coletar dados armazenados no exterior estabelecendo efeitos extraterritoriais de teor agressivo. Ao abrir mão do MLAT para regular essa coleta, a norma estadunidense tem potencial de interferir na soberania de outras jurisdições mais protetivas, como os regimes de proteção de dados de legislações europeias, sem garantir padrões similares de salvaguarda. Desta forma, é recomendável que esta Corte Suprema se afaste de posicionamento similar, pela ausência de respeito aos princípios de proteção de dados, bem como pela possibilidade de gerar conflitos diplomáticos.

Ainda quanto ao ordenamento jurídico dos EUA, o organismo responsável por regular e implementar as regras referentes à proteção de dados é a Federal Trade Commission (FTC). No entanto, a maior parte das normas é elaborada pelos Estados Federados, o que gera incongruência em relação aos dispositivos. Por exemplo, a lei da Califórnia incorporou diversos elementos encontrados na GDPR. Um dos elementos principais é a obrigação das empresas em responderem prontamente aos questionamentos dos consumidores relacionados a como os dados pessoais estão sendo utilizados, vendidos ou revelados.[59] Essas distinções interestaduais acabam por gerar uma enorme insegurança jurídica aos jurisdicionados: empresas ficam em dúvida quanto a qual modelo regulatório seguir, enquanto indivíduos correm o risco de terem seus direitos fundamentais violados.

Já na legislação europeia, o direito à privacidade é protegido em dois ordenamentos internacionais distintos. No Conselho da Europa, formado por 47 Estados-Membros, este

[59]BROOKS, Ryan. **Data Privacy Laws by State: The U.S. Approach to Privacy Protection**. Netwrix Blog, 2019. Disponível em: <https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/>. Acesso em: 01 de dezembro de 2019.

direito é protegido pelo art. 8 da Convenção Europeia de Direitos Humanos (CEDH).[60] Na União Europeia (UE), formado até então por 28 Estados-Membro, protege-se a privacidade no artigo 7 da Carta de Direitos Fundamentais da UE (Carta da UE).[61]

De acordo com art. 8 (2) da CEDH e art. 52 (1) da Carta da UE, o direito à privacidade só pode ser legitimamente restringido pelo governo sob certas condições, que são bastante semelhantes em cada uma dessas convenções.

Na CEDH, afirma-se que pode ocorrer interferência se: (i) esta estiver "de acordo com a lei "; (ii) for para a busca de um "interesse legítimo" (como segurança nacional, segurança pública ou para a prevenção de desordem ou crime), e; (iii) for "necessário" em uma sociedade democrática.

Quanto à Carta da UE, as condições para limitações exigem que a interferência: (i) seja "fornecida por lei"; (ii) respeite a "essência" desses direitos e liberdades; (iii) esteja sujeita ao "princípio da proporcionalidade" e; (iv) "seja necessária para atingir objetivos de interesse geral reconhecidos pela União ou a necessidade de proteger os direitos e liberdades de terceiros".

Para os fins do que importa a essa análise, assumimos que os requisitos de conformidade legal e interesse legítimo já estejam preenchidos. A interferência deverá obedecer os parâmetros do MLAT (Decreto 3.810/2001) e do Marco Civil da Internet (Lei 12.965/2014) e o interesse legítimo é o de prevenção de desordem ou crime. Nos parágrafos seguintes analisaremos as demais condições, que podem ser resumidas nos princípios da necessidade e da proporcionalidade.

a) Princípio da necessidade na interferência à privacidade

O princípio da **necessidade** busca identificar quais são as medidas essenciais, a fonte de prova na requisição de dados deve ser imprescindível ao prosseguimento da investigação e a consecução do arcabouço probatório, bem como delinear o período ou abrangência dos dados a serem coletados em íntima correlação ao aos elementos concretos do caso investigado.[62]

---

[60]CORTE EUROPEIA DE DIREITOS HUMANOS. **Convenção Europeia dos Direitos do Homem**. Council of Europe Publisher, 1950. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 03 de dezembro de 2019.

[61] COMISSÃO EUROPEIA. **Carta dos direitos fundamentais da União Europeia**. Jornal Oficial das Comunidades Europeias, 2000. Disponível em: <https://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 02 de dezembro de 2019.

[62] Neste sentido, ver também AZEREDO, João Fábio A. **Sigilo das Comunicações Eletrônicas diante do Marco Civil da Internet**. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). Direito & Internet III. Tomo II. São Paulo: Quartier Latin, , 2015, p. 227.

Uma vez que a vigilância de comunicações é um ato altamente intrusivo e que interfere com os direitos à privacidade e com a liberdade de expressão e opinião, ameaçando os fundamentos de uma sociedade democrática, a vigilância proporcional vai tipicamente requerer uma autorização prévia de uma autoridade judicial competente, conforme a legislação vigente.

Para que uma interferência seja considerada legítima, atender aos dois requisitos anteriores não é suficiente. Por exemplo, no contexto europeu, tanto a CEDH como a Carta da UE exigem uma avaliação da necessidade da interferência, cujo grau deve ser avaliado em relação a quão necessária ela é para lograr alcançar determinado objetivo. Portanto, não é suficiente que a medida de interferência seja "útil", "razoável" ou "oportuna", mas a autoridade pública também deve estabelecer claramente a imperiosa necessidade imperiosa de impor a limitação, o que significa que o uso do poder pelo Estado deve limitar-se à extensão mínima necessária.[63]

No Conselho da Europa, o Tribunal Europeu dos Direitos Humanos (TEDH) é bastante rigoroso quanto ao nível de interferência em contextos de vigilância, tendo em vista que as tecnologias para invadir meios de comunicação estão se tornando mais invasivas. Em *Kennedy*, o Tribunal considerou que poderes para vigiar os cidadãos deveriam apenas ser tolerados na medida em que **sejam estritamente necessários para salvaguardar as instituições democráticas**.[64] Necessidade estrita significa que **garantias adequadas e eficazes contra abusos devem existir.** Esta interpretação está relacionada ao desenvolvimento do conjunto de salvaguardas de *Weber*[65] e *Zakharov*.[66]

Ademais, em *Szabó & Vissy*,[67] o TEDH declarou que a estrita necessidade, quando aplicada a medidas de vigilância tem duplo alcance: necessidade geral, para a salvaguarda das instituições democráticas; e necessidade particular, para a obtenção de inteligência vital em uma operação individual. Se estes dois critérios não forem cumpridos, a medida estará sujeita a abusos pelas autoridades devido às poderosas tecnologias existentes a sua disposição.

Quanto à UE, o Tribunal de Justiça da União Europeia (TJUE) também avaliou o teste da necessidade no contexto de vigilância. Para este tribunal, a necessidade envolve a análise de medidas alternativas: "quando há uma escolha entre vários medidas, deve se utilizar aquela que menos interfira no direito fundamental em questão".[68] O conceito de instrumento menos

---

[63] VAN DER SLOOT, Bart. **Where Is the Harm in A Privacy Violation? Calculating The Damages Afforded in Privacy Cases by The European Court of Human Rights**. 8 JIPITEC , p. 322, 2017. Disponível em: <https://www.jipitec.eu/issues/jipitec-8-4-2017/4641>. Acesso em: 01 de dezembro de 2019.
[64] *Kennedy v. the United Kingdom* App no 26839/05 (ECtHR, 18 May 2010).
[65] *Weber and Saravia v. Germany* App no 54934/00 (ECtHR, 29 Jun 2006).
[66] *Roman Zakharov v. Russia* App no 47143/06 (ECtHR, 04 Dec 2015).
[67] *Szabó & Vissy v. Hungary* App. No. 37138/14 (ECtHR, 12 Jan. 2016).
[68] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. Op. cit., p. 75.

invasivo é geralmente considerado conjuntamente com a avaliação do teste de proporcionalidade, discutido a seguir.

b) Princípio da proporcionalidade na interferência à privacidade

O princípio da proporcionalidade se reflete em duas nuances. A primeira é que a interferência deve utilizar sempre o instrumento menos invasivo, o que é reconhecido por alguns doutrinadores como o **princípio da subsidiariedade**.[69] Em segundo lugar, a medida deve ser aplicada como ***ultima ratio***: todos os outros meios disponíveis para a investigação criminal devem ser exaustivamente testados antes que se recorra à obtenção de dados de conteúdo privado, como os armazenados e/ou transitados em plataformas de comunicação. Se as demais alternativas forem ineficientes ou onerosas, isso deve ser comprovado, não bastando a simples alegação.

Trazendo o exemplo europeu para fins de analogia, embora este princípio esteja explicitamente declarado no artigo 52(1) da Carta da UE, ele não pode ser encontrado diretamente no art. 8 (2) da CEDH. Contudo, o TEDH reconhece que o princípio da proporcionalidade deve ser aplicado na interpretação de casos sobre vigilância estatal. Assim, para que a interferência seja necessária em uma sociedade democrática, não basta ser relevante e suficiente, mas deve também ser proporcional aos objetivos legítimos perseguidos.[70]

Assim, Além disso, desde *Klass*,[71] uma salvaguarda que foi revelada como essencial para a correta aplicação do teste de proporcionalidade segundo o requisito de necessidade democrática é a **existência de um regime de supervisão** (*oversight*). Embora este papel esteja hoje sendo cumprida pelo Poder Judiciário, a numerosidade de casos similares existentes exige a supervisão contínua por uma autoridade reguladora. O LAPIN entende que esta deverá ser a **Autoridade Nacional de Proteção de Dados**, criada pelo artigo 55-A da Lei nº 13.709/2018 (LGPD), que **precisa ser dotada de independência para poder exercer sua tarefa de supervisão livre de influências políticas ou econômicas de entes públicos e privados**.

No caso do TJUE, o princípio da proporcionalidade é acessado em duas etapas.[72] Primeiro, ao avaliar se as limitações do direito à privacidade pode ser permitido, deve ser verificado se eles respeitam o conteúdo essencial desse direito. Em *Schrems*, o Tribunal da UE considerou que legislação que permita às autoridades públicas o acesso ao conteúdo de comunicação

[69] VAN DER SLOOT, Bart. Op. cit., p. 7.
[70] CORTE EUROPEIA DE DIREITOS HUMANOS. **Guide On Article 8 Of The European Convention On Human Rights**. European Commission Publisher ,2018.
[71] *Klass and Others v Germany* App no 5029/71 (6 Sep 1978).
[72] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. Op. cit., p. 67.

eletrônicas de forma genérica, comprometem a essência do direito garantido pela Artigo 7 da Carta.[73] Segundo, ao avaliar se as limitações podem ou não ser justificadas, deve ser verificado se a medida não impõe um ônus desproporcional e excessivo aos indivíduos afetados pela interferência.[74]

c) A tradução dos princípios da necessidade e proporcionalidade em salvaguardas legais

A jurisprudência das cortes europeias quanto a casos de interferência do direito à privacidade em contextos de vigilância resultou no desenvolvimento de salvaguardas legais, isto é, elementos que devem estar previstos em legislações sobre o tema para garantir o equilíbrio necessário entre o interesse legítimo das autoridades de investigação e o direito à privacidade.

Neste contexto, o TEDH desenvolveu um esquema para determinar a **"qualidade da lei"** (*quality of law*), nas legislações nacionais sobre mecanismos de vigilância. Primeiro, foi apresentado em *Weber e Saravia*[75] uma lista de salvaguardas mínimas que devem ser estabelecidas para evitar abusos de indivíduos. Esta lista se relaciona principalmente a aspectos substantivos e processuais das medidas de vigilância. Essas salvaguardas foram estendidas em *Zakharov*, para incluir regras relativas à acessibilidade dos mecanismos legais e de supervisão.[76] Na Tabela 1, a lista de salvaguardas discutidas em cada caso é apresentada. A análise mais detalhada de cada salvaguarda está disponível na bibliografia deste memorial.[77]

Tabela 1: Salvaguardas mínimas para proteção do direito à privacidade em legislações sobre vigilância, de acordo com a TEDH

***Weber* (2006)**	***Zakharov* (2015)**
	Acessibilidade da Lei
Natureza das ofensas	**Escopo** das medidas de segurança
Categoria dos indivíduos-alvo	
Duração das medidas de vigilância	**Duração** das medidas de segurança

[73] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*. EU:C:2015:650 para 94.
[74] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. Op. cit., p. 76.
[75] *Weber and Saravia v. Germany* (2006) para 95.
[76] *Roman Zakharov v. Russia* (2015) para 23.
[77] MORAES, T. G. **A Spark of Light in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures**. Dissertação (Master Thesis in the Law and Technology LLM Program), 2019.

Procedimentos para o e**xame, uso e armazenamento** de dados	**Procedimentos** a serem seguidos para o **armazenamento, acesso, exame, uso, comunicação e destruição** dos dados interceptados
Precauções para **comunicação** de dados com terceiros	
Circunstâncias em que registros devem ser apagados ou **destruídos**	
	Autorização da vigilância (*oversight ex-ante*)
	Supervisão da implementação da vigilância (*oversight* "durante")
	Notificação e **remédios legais disponíveis** (*oversight ex-post*)

Fonte: MORAES, T.[78]

Quanto ao TJUE, salvaguardas similares foram desenvolvidas na análise de legislações de retenção de dados. Em *Digital Rights Ireland*,[79] a natureza das ofensas e as categorias de pessoas visadas foram consideradas. Também foi declarado que condições substantivas e procedimentais deveriam estar em vigor. Por fim, destacou-se a importância da **supervisão prévia realizada por um tribunal ou por um órgão administrativo independente** quando autoridades investigativas desejarem analisar os dados retidos.

As mesmas salvaguardas foram reafirmadas em *Tele2 Sverige e Watson*,[80] quando o tribunal reforçou que o regime de autorização deve ser seguida de uma notificação às pessoas afetadas, logo que essa notificação não seja mais suscetível de comprometer as investigações realizadas por essas autoridades. O Tribunal da UE também abordou que os dados devem ser retidos em um nível particularmente alto de proteção e segurança por meio de medidas técnicas e organizacionais apropriadas (*privacy by design*),[81] que estão relacionados com as salvaguardas procedimentais em *Zakharov*.

Embora o exemplo europeu tenha sido destacado neste memorial, tendo em vista a robustez de seus regimes de privacidade e proteção de dados, ambos aplicáveis a contextos de segurança pública, o LAPIN entende que **salvaguardas próprias devem ser desenvolvidas**

[78] Ibid, p. 31.
[79] Joined Cases C‑293/12 and C‑594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*. EU:C:2014:238.
[80] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*. EU:C:2016:970.
[81] Ibid, para 122.

por esta c. Corte, uma vez que a análise deverá ser feita tomando por consideração a realidade socioeconômica brasileira e a Constituição Democrática da República Federativa do Brasil, de 1988.

5. Conclusão

Tendo em vista os pontos descritos nesta contribuição, o Laboratório de Políticas Públicas e Internet resume seus argumentos em quatro sugestões não-excludentes a serem adotadas por este Tribunal no julgamento da Ação Declaratória de Constitucionalidade n. 51:

1. **Na ausência de instrumento mais adequado** para a requisição de dados em territórios internacionais sob a jurisdição de outro Estado, **seja aplicado o Tratado Mútuo de Assistência Legal**, ou MLAT, no acrônimo em inglês;
2. Sejam abarcados os **princípios e direitos ligados à proteção de dados presentes na Lei Geral de Proteção de Dados**, Lei 13.709/2018, que embora não se aplique a contextos de segurança pública, deve servir como **baliza até que legislação específica seja criada**, bem como os art. 156 e 282, do Código de Processo Penal, como parâmetros para a fundamentação de decisões de órgãos investigativos que pretendam o acesso a dados pessoais de residentes no Brasil, tomando por consideração as **Teorias da Privacidade Contextual** e da **Expectativa Razoável da Privacidade**, bem como os **princípios da necessidade e proporcionalidade**;
3. Seja **sugerida ao Congresso Nacional a adoção de legislação adequada** ao contexto de tratamento internacional de dados pessoais na segurança pública, de modo a garantir maior segurança jurídica para envolvidos em casos de persecução penal que envolvam o tratamento de dados pessoais pelo Estado brasileiro.
4. Sejam analisados os **direitos da privacidade e proteção de dados pessoais** sob o prisma do direito fundamental à **dignidade da pessoa humana**, utilizando dos **princípios da necessidade e proporcionalidade**, à luz das normas pátrias e do direito comparado sobre o tema.

Brasília,
06 de dezembro de 2019.