VOTO

1. Considerações iniciais. 2. Da audiência pública. 3. Legitimidade ativa *ad causam* . 4. Mérito. 5. A virtualização da vida privada em nossos dias. 6. Breve histórico dos bloqueios de aplicações de Internet no Brasil. 7. Das ordens de bloqueio do *WhatsApp* . 8. Considerações sobre o direito às liberdades de expressão e de comunicação (art. 5º, IX, da CF). 9. Considerações sobre o direito à privacidade (art. 5º, X, da Constituição da República). 10. Considerações sobre o sigilo das comunicações privadas (art. 5º, XII, da Constituição da República). 11. Do dever de guarda de metadados. 12. Da Lei Geral de Telecomunicações (Lei nº 9.472/1997). 13. Influxos do *standard* normativo da Convenção de Budapeste sobre o Cibercrime. 14. Análise da constitucionalidade dos preceitos impugnados. 15. A questão da criptografia. 16. Das sanções previstas no art. 12, III e IV, da Lei nº 12.965/2014. 17. Conclusão.

A Ministra Presidente Rosa Weber (Relatora): N a sessão de julgamento do Plenário realizada em 27.5.2020, apresentei minha justificativa de voto no presente feito. Desde então, tive oportunidade de amadurecer o meu entendimento sobre a matéria nele discutida, à luz dos acontecimentos da história recente do País e do mundo. Por esta razão, peço vênia para apresentar justificativa de voto reformulada, com a incorporação de acréscimos e ajustes que reputo necessários ao fiel cumprimento da Constituição da República, e que dizem com o ponto exposto no **item 16** deste voto.

Na ocasião, julguei (i) improcedente o pedido de declaração de inconstitucionalidade do art. 12, III e IV, da Lei nº 12.965/2014; (ii) procedente o pedido de interpretação conforme a Constituição do art. 10, § 2º, da Lei nº 12.965/2014, a fim de assentar exegese segundo a qual " *o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer,*

respeitado o disposto nos incisos II e III do art. 7º, e para fins de investigação criminal ou instrução processual penal"; (iii) improcedente o pedido sucessivo de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei nº 12.965/2014, à compreensão de que não abrangido em sua hipótese de incidência o conteúdo que dele se pretende excluir; e (iv) parcialmente procedente o pedido sucessivo de interpretação conforme a Constituição do art. 12, III e IV, da Lei nº 12.965/2014 apenas para (a) assentar que autorizada a imposição das penalidades de suspensão temporária das atividades e de proibição de exercício das atividades, aos provedores de conexão e de aplicações de internet, nos casos de descumprimento da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, (b) ficando afastada qualquer exegese que – isoladamente ou em combinação com o art. 7º, II e III, da Lei nº 12.965/2014 – estenda a sua hipótese de incidência de modo a abarcar o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação.

Faço, na linha do que fundamentarei na sequência, retificação quanto ao item **(iv)** da conclusão, nele mantido o juízo de procedência parcial, com os acréscimos destacados em **negrito.**

Renovo, hoje, meus cumprimentos, saudando todos os que ocuparam a tribuna, naquela assentada, com profícuas sustentações orais. E saúdo de modo especial os participantes da audiência pública realizada no âmbito deste feito, em conjunto com a **ADPF 403** , sob a relatoria do Ministro Edson Fachin, agradecendo pelas inestimáveis contribuições recebidas, decididamente fundamentais à adequada prestação jurisdicional em tema complexo dessa natureza, a envolver inclusive aspectos técnicos de difícil compreensão para os que não são da área.

1. Considerações iniciais

Como relatado, discute-se na presente ação de fiscalização abstrata a higidez constitucional de dois artigos da **Lei nº 12.965, de 23 de abril de 2014, o chamado Marco Civil da Internet, mais precisamente o art. 10, em seu § 2º, e o art. 12, em seus incisos III e IV.**

Tais dispositivos têm sido invocados para justificar decisões judiciais determinando a suspensão temporária de serviços que permitem a troca de mensagens entre usuários da Internet como sanção pelo descumprimento, por parte da empresa responsável pelo aplicativo, de ordem judicial de disponibilização do conteúdo das comunicações.

A **Lei nº 12.965/2014** , é sabido, estabelece princípios, garantias, direitos e deveres para o **uso da Internet no Brasil** , instituindo assim o chamado **Marco Civil da Internet no Brasil** , amplamente celebrado, inclusivo no âmbito internacional, por situar nosso país em posição de vanguarda no tocante à proteção dos direitos e à previsão de deveres para os usuários da rede mundial de computadores.

O Marco Civil da Internet, como observaram diversos *amici curiae* e expositores da audiência pública, é fruto de intensos debates e estudos, com ampla participação da sociedade civil desde a sua concepção até a aprovação do seu decreto regulamentador, o **Decreto nº 8.771/2016** .

Ao disciplinar o uso da Internet no Brasil, o Marco Civil da Internet se propõe a harmonizar princípios como a garantia da liberdade de expressão e de comunicação, a proteção da privacidade e dos dados pessoais e a responsabilização dos agentes de acordo com suas atividades.

De inegável relevância para a consolidação do Estado Democrático de Direito em nosso país, bem como para o dimensionamento e a concretização dos direitos fundamentais consagrados na Constituição de 1988, as questões ora enfrentadas dizem respeito a valores fundacionais da ordem jurídica pátria, conforme consagra o próprio preâmbulo da Carta Política **: liberdade e segurança, desenvolvimento e justiça** .

2. Da audiência pública

Faço questão de enfatizar a importância da audiência pública realizada para o devido equacionamento, neste Supremo Tribunal Federal, de questão complexa e de tamanha relevância. O diálogo entre esta Casa e diferentes setores da sociedade, atuando como co-intérpretes da Constituição, qualifica e legitima a jurisdição constitucional, beneficiando os jurisdicionados como um todo, além de cumprir ditame da Constituição brasileira ao ressaltar o **caráter democrático do Estado de Direito** por ela instituído.

Em casos de **relevância institucional** , como o presente, compreendo que a realização de audiências públicas constitui um dos pilares centrais do efetivo **acesso à justiça** . Como já observou o Juiz da Suprema Corte da Argentina, Ricardo Lorenzetti, " *a justiça progride, se expande e chega à sociedade quando todos têm a mesma oportunidade de chegar e dizer a sua verdade. Então, o primeiro pressuposto é que todos tenham sua voz no Tribunal, seu dia no Tribunal*".

Além disso, os subsídios contidos em conhecimentos técnicos, estudos rigorosos e na experiência de especialistas, acadêmicos e profissionais de diferentes áreas densificam a jurisdição constitucional do ponto de vista substantivo, com o esclarecimento de aspectos técnicos – porém juridicamente relevantes – relativos à operacionalização dos registros de conexão e de acesso a aplicações de internet e ao processamento das operações de coleta, armazenamento, tratamento e guarda de registros, de dados pessoais e de comunicações privadas por provedores de conexão e provedores de aplicações de internet.

A consideração da diversidade de olhares e pontos de vista sobre o tema, da multiplicidade de compreensões sobre as questões aqui enfrentadas, é essencial à elaboração das perguntas corretas e, consequentemente, chegar-se a consensos possíveis e respostas satisfatórias.

Entendo que a justa aplicação do Direito não prescinde da adequada compreensão dos **fatos** que se pretende disciplinar, bem como das suas implicações sociais. Em outras palavras, **a integridade do direito supõe coerência na sua aplicação à realidade.** Somente assim a decisão judicial tem condições de se ancorar na **melhor interpretação possível do direito objetivo** : a Constituição, as leis, a tradição jurídica, a prática institucional e os valores de uma sociedade. A interpretação judicial da lei, na lição de Dworkin, " *deve refletir não apenas suas convicções sobre justiça (...) – embora estas também tenham um papel a desempenhar –, mas também suas convicções sobre os ideais de integridade e equidade políticas e de devido processo legal, na medida em que estes se aplicam especificamente à legislação em uma democracia*".

3. Legitimidade ativa *ad causam*

A legitimidade *ad causam* do autor, partido político com representação no Congresso Nacional, tem assento nos **arts. 103, VIII, da Constituição da República** e **2º, VIII, da Lei nº 9.868/1999** .

Atendidos, ainda, os pressupostos formais de admissibilidade, admito a ação direta e passo ao exame do **mérito.**

4. Mérito

O que se busca, em última análise, é o **reconhecimento da inconstitucionalidade das sanções correspondentes à suspensão temporária das atividades e à proibição do seu exercício impostas a empresa responsável por plataforma de comunicação via Internet pelo descumprimento de ordem judicial de disponibilização do conteúdo de mensagens privadas de usuários.**

Eis o teor dos **arts. 10, § 2º, e 12, III e IV, da Lei nº 12.965/2014** (dispositivos impugnados em **destaque**):

> "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> (...)
>
> **§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.**
>
> "
>
> "Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> **III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou**
>
> **IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.**
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua

filial, sucursal, escritório ou estabelecimento situado no País." (destaquei)

Para o devido equacionamento da controvérsia, imprescindível examinar os preceitos questionados em conjunto com os **arts. 7º, II e III, e 11 da Lei nº 12.965/2014** , aos quais fazem eles **remissão** . Transcrevo-os:

> *" **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;"** (destaquei)*
>
> *" **Art. 11** . Em qualquer operação de **coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações** por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os **direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros** .*
>
> ***§ 1º** O disposto no caput aplica-se aos **dados coletados** em território nacional e ao **conteúdo das comunicações** , desde que pelo menos um dos terminais esteja localizado no Brasil.*
>
> ***§ 2º** O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.*
>
> ***§ 3º** Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.*
>
> ***§ 4º** Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo."*

Os preceitos normativos impugnados na presente ação direta, como já apontei, têm sido invocados para fundamentar decisões judiciais em que ordenada a suspensão das atividades de serviços de troca de mensagens privadas, aí residindo o cerne da questão constitucional ora em exame.

5. A virtualização da vida privada em nossos dias

Nos tempos atuais, pergunta-se com mais frequência ao interlocutor " *o número de WhatsApp* " - ou, na linguagem popular, " *o zap* " do que " *o número do telefone* ".

No século XXI, parte significativa da vida privada de grande número de brasileiros descortina-se por meio dos respectivos celulares. Mais do que estações para fazer e receber chamadas, ou meros espelhos negros quando inativos dentro dos bolsos e bolsas, os telefones celulares, uma vez ativados em nossas mãos, convertem-se em janelas luminosas para a nossa intimidade.

Uma estante inteira de álbuns de fotografia da família se comprime em um único aplicativo. Em outro, permanecem registradas inclusive as últimas refeições. A porta giratória da agência bancária cedeu lugar à senha digitada na tela ou à impressão digital coletada detrás dela. No mesmo dispositivo, a porta de entrada para nosso diário, nossas leituras e músicas preferidas. As mensagens que respondemos e as que ainda nem visualizamos. Os textos lidos e os textos por ler. As conversas que tivemos, os planos futuros e os desejos íntimos, compartilhados com amigos na crença de que ninguém mais está a ouvi-los, lê-los ou vê-los. Os objetos antes guardados nas gavetas dos escritórios e prateleiras das salas de estar – nessa condição protegidos de invasão arbitrária – hoje converteram-se em impulsos eletromagnéticos que transitam, por cabos ou ondas, entre os circuitos eletrônicos dos celulares e sistemas de armazenamento chamado de **nuvem,** em metáfora que não deixa de conter uma certa poesia.

Os aparelhos de telefone móvel guardam muito mais da vida privada e intimidade de seus proprietários do que as portas e paredes, gavetas e armários da residência de cada um deles, e a inviolabilidade do **domicílio** não temos dificuldade alguma em reconhecer.

Ao mesmo tempo, como advertem BEZERRA e AGNOLETTO, em sua obra Combate ao crime cibernético: doutrina e prática, nesse " *novo cenário em que vivemos, apresentam-se várias formas de delito, quer seja usando a internet como ferramenta ou sendo a própria finalidade do crime em si* ."

6. Breve histórico dos bloqueios de aplicações de Internet no Brasil

O Marco Civil da Internet propõe-se a fixar orientações e diretrizes para o equacionamento, sempre à luz da Constituição, de controvérsias que começaram a acontecer bem antes dele.

Um dos primeiros casos de bloqueios judiciais de grande repercussão no Brasil ocorreu em 2007, a partir da divulgação de vídeo contendo cenas de intimidade de uma famosa apresentadora de televisão e modelo, capturadas em ambiente público, sem autorização, no site *YouTube* .

Já entre 2015 e 2016, em um intervalo de apenas **oito meses** , o conhecido serviço de mensagens instantâneas e chamadas de voz *WhatsApp* teve suas atividades suspensas três vezes no Brasil – por alguns dias ou algumas horas –, em virtude de decisões judiciais. Em nenhum desses casos, o **provedor da aplicação ou sua empresa controladora** era **réu** por violação das obrigações decorrentes do Marco Civil ou qualquer outra obrigação prevista pela legislação brasileira. **Em dezembro de 2015, por ordem de um juiz do Estado de São Paulo, em fevereiro de 2016, por um juiz do Estado de Alagoas, e em julho de 2016, por ordem de uma juíza do Estado do Rio de Janeiro.**

Houve, ainda, uma ordem de bloqueio em fevereiro de 2015, da Justiça do **Piauí, e outra em maio de 2016, por um Juiz de Sergipe,** ambas cassadas antes da implementação. O juiz subscritor dessa última ordem é o mesmo que, em março de 2016, chegara a ordenar a prisão de diretor do *Facebook* no Brasil, por suposto descumprimento de decisão judicial.

Casos como esses têm feito o Estado brasileiro figurar, ao lado de Estados que não compartilham das mesmas tradições e valores democráticos caros à nossa sociedade, em listas de países pouco comprometidos com a preservação das liberdades individuais na Internet. Cito alguns exemplos.

Em 2016, durante o que foi reportado como uma tentativa de golpe militar na Turquia, *Facebook* , *YouTube* e *Twitter* ficaram inoperantes naquele país.

No mesmo ano, o *Facebook* foi temporariamente banido de Bangladesh, à alegação de que a medida era necessária para manutenção da ordem pública, após a Suprema Corte ter confirmado a condenação à pena de morte de dois homens acusados de crimes de guerra praticados durante o conflito que levou o país a se tornar independente do Paquistão.

Bloqueios, suspensões e banimentos temporários também ocorreram no Egito, durante os protestos de 2011. Na Índia, por alguns dias, durante protestos na região do Punjab em 2011 e por seis meses na Cachemira entre

2016-2017. A lista de países que acompanham o Brasil nesse histórico de práticas inclui ainda Paquistão, Tajiquistão, Sudão, Sri Lanka, Malásia, Irã e China.

7. Das ordens de bloqueio do *WhatsApp*

As **ordens judiciais de bloqueio partem da premissa de que houve o descumprimento anterior de uma primeira ordem judicial determinando o fornecimento do conteúdo das comunicações** . As circunstâncias que importam, aqui, são: **(i) a legalidade e a constitucionalidade da ordem de disponibilização do conteúdo das mensagens** e **(ii) a possibilidade material do cumprimento da ordem.**

Como resultado das ordens de suspensão dos serviços do WhatsApp, serviços similares, como *Viber* e *Telegram* , observaram um rápido aumento vertical na sua base de usuários. O *Telegram* , por exemplo, reportou aumento de mais de um milhão de usuários nos dois dias seguintes à suspensão das atividades do seu principal concorrente.

Os bloqueios comprometem o exercício, por milhões de brasileiros, das liberdades fundamentais de expressão e de comunicação asseguradas pelo texto constitucional. Não à toa, causaram verdadeira comoção social, além de terem perturbado de relações familiares a transações comerciais, de reuniões de negócios a notificações de atos processuais do próprio Poder Judiciário.

É importante dizer, desde logo, como ficará demonstrado, que **a apontada lesão à Constituição, diante das ordens judiciais de bloqueio de aplicativos de mensagens, não guarda relação direta com a vigência do Marco Civil da Internet brasileira, mas com a sua invocação indevida para a prática de atos que não são por ele, Marco Civil, amparados** . **A interpretação acaso equivocada da lei, no entanto, em absoluto conduz à sua inconstitucionalidade, inquinando de vício, isto sim, o ato assim praticado, passível de correção pelas vias próprias do devido processo legal.**

8. Considerações sobre o direito às liberdades de expressão e de comunicação (art. 5º, IX, da CF)

Integra o pleno exercício das liberdades de expressão e de comunicação a capacidade das pessoas de escolherem livremente as informações que pretendem compartilhar, as ideias que pretendem discutir, o estilo de

linguagem empregado e o meio de comunicação. O conhecimento de que a comunicação é monitorada por terceiros interfere em todos esses elementos componentes da liberdade de informação: os cidadãos podem mudar o modo de se expressar ou até mesmo absterem-se de falar sobre certos assuntos, no que a doutrina designa por efeito inibitório (*chilling effect*) sobre a liberdade de expressão. Nesse sentido,

> "A comunicação desinibida é também uma precondição do desenvolvimento pessoal autônomo. Seres humanos desenvolvem suas personalidades comunicando-se com os demais."

As consequências da ausência dessa precondição em uma sociedade vão desde a desconfiança em relação às instituições sociais, à apatia generalizada e a debilitação da vida intelectual, fazendo de um ambiente em que as atividades de comunicação ocorrem de modo inibido ou tímido, por si só, uma grave restrição à liberdade de expressão.

Sob enfoque diverso, considerando que *software* é linguagem, e como tal, protegido pela liberdade de expressão, indaga-se se compelir o desenvolvimento compulsório de uma aplicação para se implementar a vulnerabilidade desejada, a determinação para a escrita compulsória de um programa de computador não configuraria, ela mesma, uma violação do direito à liberdade de expressão do desenvolvedor?

De toda sorte, transformar o Brasil em um país avesso à liberdade de expressão não é o melhor caminho para combater os usos irresponsáveis das ferramentas de comunicação.

9. Considerações sobre o direito à privacidade (art. 5º, X, da Constituição da República)

É certo que a Constituição da República qualifica como **invioláveis** , na condição de direitos fundamentais da personalidade, a **intimidade** , a **vida privada** , a **honra** e a **imagem** das pessoas, conferindo-lhes especial proteção, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (**art. 5º, X**). *In verbis* :

> "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

Tal como a liberdade de manifestação do pensamento – e seus desdobramentos como a liberdade de expressão intelectual, artística e científica e a liberdade de imprensa –, o assim chamado direito à privacidade (*right to privacy*) – e os seus consectários direito à intimidade, à honra e à imagem – também emana do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.

Apesar da muita tinta despendida a respeito, o conceito de privacidade permanece, nas palavras de Richard Posner, elusivo (vago, impreciso) e mal definido. No clássico artigo *The Right to Privacy,* escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, sugere-se **a relação de tal estado de coisas com o fato de as mudanças políticas, sociais e econômicas demandarem incessantemente o reconhecimento de novos direitos, impondo, de tempos em tempos, a redefinição da exata natureza e extensão da proteção à privacidade do indivíduo** .

Na quadra atual, inegável que a privacidade, enquanto **direito a ser deixado em paz** , na expressão cunhada pelos magistrados da Suprema Corte americana, merece proteção adequada e efetiva do ordenamento jurídico. **Cumpre indagar, porém, o escopo e a extensão desse direito específico.**

Privacidade não se confunde com isolamento. Já em 1624 anotava John Donne, o poeta, com precisão científica, que " *nenhum homem é uma ilha, completo em si mesmo; todo homem é um pedaço do continente, uma parte do todo* " (tradução livre).

Proteção da privacidade em absoluto diz com direito a passar a vida sem ser contrariado, sem sentir desconforto social, sem ser ofendido .

Em uma abordagem contemporânea e integradora, pode-se dizer, (com COHEN, Julie, em tradução livre) que o direito à privacidade visa a proteger " *a subjetividade emergente, dinâmica, dos esforços de atores comerciais e governamentais para tornar indivíduos e comunidades fixos, transparentes e predizíveis. Ela protege as práticas (…) através das quais a capacidade de auto determinação se desenvolve* ".

Assim compreendida a privacidade, a conclusão inarredável é a de que, tanto quanto a ampla liberdade de expressão, **a proteção da privacidade também é uma característica estrutural indispensável das sociedades democráticas** .

E isso porque **tanto o reconhecimento de uma esfera de privacidade imune à ingerência quanto a garantia de salvo-conduto à palavra proferida surgiram, na história do constitucionalismo moderno, como fatores de limitação do poder das autoridades constituídas sobre os cidadãos.**

Se aos cidadãos não for assegurada uma esfera de intimidade privada, livre de ingerência externa, um lugar onde o pensamento independente e novo possa ser gestado com segurança, de que servirá a liberdade de expressão?

O direito à privacidade tem como objeto, na quase poética expressão de Warren e Brandeis, " *a privacidade da vida privada* ". O escopo da proteção são os assuntos pessoais, em relação aos quais não se vislumbra interesse público legítimo na sua revelação, e que o indivíduo prefere manter privados. " *É a invasão injustificada da privacidade individual que deve ser repreendida e, tanto quanto possível, prevenida* ".

Vale observar, ainda, que os maiores desafios contemporâneos à proteção da privacidade nada têm a ver com a imposição de restrições à liberdade de manifestação, enquanto relacionados, isto sim, aos imperativos da segurança nacional e da eficiência do Estado, à proliferação de sistemas de vigilância e à emergência das mídias sociais, juntamente com a manipulação de dados pessoais em redes computacionais por inúmeros, e frequentemente desconhecidos, agentes públicos e privados.

Nesse contexto, pertinente, ainda, a contribuição de Alan Westing à doutrina jurídica da privacidade no mundo contemporâneo, ao caracterizar a estrutura desse direito como controle sobre os usos da informação pessoal. Nesse sentido, a privacidade, afirma, " *é a pretensão de indivíduos, grupos ou instituições de determinarem para si quando, como e em que extensão a informação sobre eles será comunicada a outros* ".

Tal concepção do direito à privacidade está alinhada com o reconhecimento do seu papel social na própria preservação da personalidade e no desenvolvimento da autonomia individual. A existência de uma esfera de privacidade permite, por exemplo, que determinados conflitos pessoais ou erros da juventude, desde que não tenham

consequência significativa para a sociedade, não tenham projeção exacerbada sobre as possibilidades de vida de um indivíduo. A privacidade produz um ambiente seguro para que pensamentos, ideias e opiniões sejam compartilhados em círculos limitados e testados antes de serem publicamente expostos. Permite, dito de outro modo, o espaço de liberdade onde se processa a experimentação necessária ao progresso social.

A facilidade com que a privacidade será protegida ou exposta transforma-se à medida em que evoluem as tecnologias da informação e da comunicação.

Se, de um lado, sucedem-se ou alternam-se tecnologias de comunicação – carta, telégrafo, telefone, telefone móvel, redes sociais, aplicativos de mensagens – de outro, adaptam-se e apuram-se as tecnologias voltadas à vigilância – interceptação, raio-x, acesso furtivo a sistemas, desencriptação etc.

As últimas três décadas, em particular, têm testemunhado uma espécie de "corrida armamentista" entre tecnologias que facilitam a vigilância e tecnologias de proteção da privacidade, em que o desenvolvimento de uma impulsiona acaba impulsionando a evolução da contraparte.

De um lado, agentes estatais da área de segurança pública alegam que o desenvolvimento de tecnologias de proteção da privacidade cada vez mais eficientes tem minado as suas capacidades de prevenir, investigar e reprimir crimes, deixando-os "no escuro". Do outro lado do debate, o cenário atual é descrito como sendo, ao contrário, o de uma "Era de ouro da vigilância.

Nessas condições, não podem a hermenêutica constitucional e o desenvolvimento legislativo ficar alheios a essas mudanças no tempo, tendo em vista a manutenção do **equilíbrio entre proteção da privacidade e os limites da atuação do Estado** . É que a Constituição, assim como o estado da técnica, institui um conjunto de restrições à atuação do Estado. Como analisa o professor Lawrence Lessig, em ensaio seminal acerca das implicações do desenvolvimento das tecnologias de comunicação em rede para a interpretação constitucional, é a combinação de **constrangimentos tecnológicos** e **constrangimentos legais** que define, em um dado momento, as restrições efetivamente enfrentadas pelo Estado, caso este deseje intervir em determinado aspecto do domínio privado de um cidadão.

Longe de ter seu significado usurpado, a Constituição escrita no mundo analógico há de ser **traduzida** para o mundo digital, de modo a preservar,

neste, **os interesses, os direitos e as liberdades que originalmente preservava** . Desse modo, o sentido das palavras da Constituição, o alcance da proteção constitucional, busca-se, é preservado em face da mudança do contexto.

No voto – então vencido – proferido em *Olmstead v. United States* (1928), o Justice Louis Brandeis, da Suprema Corte dos EUA, ressalta que um princípio vital deve ser capaz de aplicação mais ampla do que somente à conduta particular que lhe deu origem. Na peça, que já identificava, no direito à privacidade das comunicações, a conformação constitucional que somente veio a prevalecer na jurisprudência daquela Corte quarenta anos depois, diz ele:

> "Isso é particularmente verdadeiro das constituições. Elas não são promulgações efêmeras, projetadas para dar conta de ocasiões passageiras. Elas são, para usar as palavras do Juiz Marshall 'projetadas para se aproximarem da imortalidade o tanto quanto as instituições humanas forem capazes'. O futuro está sob seu cuidado e tutela (...). Na aplicação de uma constituição, portanto, não podemos contemplar apenas o que tem sido, mas o que pode vir a ser. Sob qualquer outra premissa, a aplicação de uma constituição, de fato, seria mais fácil, como também seria deficiente em eficácia e poder. Seus princípios gerais teriam pouco valor e seriam convertidos, por precedentes, em fórmulas impotentes e sem vida. Direitos declarados em palavras, perdidos na realidade."

A cada estágio do desenvolvimento tecnológico, em que se torna materialmente possível a imposição de níveis de controle cada vez maiores sobre diferentes aspectos das vidas das pessoas, renova-se a questão a ser respondida pelas Cortes quanto a "permitir que esses espaços sejam preenchidos com incremento do poder estatal, ou com o incremento das proteções à privacidade individual". Com efeito,

> "quando as tecnologias daquele mundo mudam, nos defrontamos com uma escolha. Podemos imaginar a eficiência tendo permissão para governar nesse novo espaço, ao deixarmos as liberdades protegidas pela imperfeição irem embora; ou nós podemos imaginar a recriação de esperas de liberdade para substituírem aquelas criadas por imperfeições na tecnologia. Essas são nossas escolhas democráticas e são escolhas reais."

Já no contexto do debate mais recente em torno da adoção do Marco Civil da Internet no Brasil e seu significado para a proteção dos direitos fundamentais dos usuários da rede, Paulo Rená da Silva Santarém, em dissertação sobre o tema, pontua que:

> "(...) hoje o Brasil e o mundo precisam responder duas importantes perguntas. Primeiro, quais são as exigências que a sociedade e as comunicações colocam para os horizontes políticos no início do séc. XXI? E, segundo, quais as exigências que a política e a democracia da sociedade do séc. XXI colocam para as nova tecnologias de informação e comunicação?
>
> A formulação conjunta dessas perguntas, como um par interdependente, vincula-se ao duplo entendimento de que, de um lado, o fenômeno da convergência de mídias que vivemos hoje em dia não consiste apenas em um fenômeno tecnológico, mas social; e que os efeitos da mudança da tecnologia irão in-terferir na forma como enxergamos a nossa presença no mundo, inclusive a nossa presença como cidadãos. Questionar a relação de mão dupla entre a política e a tecnologia, sem essa intertex-tualidade, pode apenas levar a respostas que, para ambas as perguntas, sejam construídas de formas tão simples quanto inúteis."

10. Considerações sobre o sigilo das comunicações privadas (art. 5º, XII, da Constituição da República)

Sem que os institutos se confundam, a garantia do **sigilo das comunicações privadas** está intimamente relacionada à **proteção da privacidade** .

Ainda em 1967, no paradigmático julgamento do caso ***Katz v. United States*** , a Suprema Corte dos EUA superou a sua jurisprudência anterior para assentar que a escuta e a gravação de comunicações telefônicas equivalem aos procedimentos de **busca e apreensão** e, como tais, sujeitam-se aos limites traçados pela Quarta Emenda à Constituição daquele país, que essencialmente assegura o direito à inviolabilidade da intimidade, da vida privada e do domicílio contra certas modalidades de ações estatais arbitrárias.

A proteção constitucional contra a invasão estatal arbitrária passou a se estender, na redefinição empreendida pela Corte sob a liderança do Chief Justice Earl Warren, a qualquer " *expectativa razoável de privacidade* ". Transcrevo:

> "A atividade do Estado pelo qual foram ouvidas e registradas eletronicamente as palavras do peticionário violou a privacidade na qual ele justificadamente se fiava ao utilizar a cabine telefônica, e constitui, portanto, uma 'busca e apreensão' na acepção da Quarta Emenda. O fato de o dispositivo eletrônico empregado para atingir tal objetivo não ter atravessado a parede da cabine não tem nenhuma relevância constitucional."

Em 2018, no julgamento de ***Carpenter . United States*** , aquela Corte decidiu que a mesma cláusula da Constituição também protege o **sigilo dos registros referentes às informações de localização de telefones móveis** , mantidos pelas operadoras do serviço, condicionada a sua disponibilização à existência de ordem judicial de busca e apreensão proferida no curso de procedimento criminal.

O histórico dos registros de localização de telefones móveis, constatou-se, permite que o Estado instaure uma " *vigilância quase perfeita* " e que " *viaje de volta no tempo para refazer o itinerário de uma pessoa* ", levando a preocupações relacionadas à privacidade ainda maiores do que aquelas apresentadas pelo monitoramento por meio da tecnologia **GPS** (*Global Positioning System* ou Sistema de Posicionamento Global).

A Constituição brasileira, a fim de instrumentalizar tais direitos, prevê, no **art. 5º, XII,** a **inviolabilidade do " *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 penal*** ".

O **art. 5º, XII, da CF** protege, cumpre salientar, a **comunicação** dos dados, o evento pelo qual dados ou informações são transmitidos ou recebidos do ponto A ao ponto B. Já a proteção do sigilo de dados armazenados tem amparo no **art. 5º, X, da CF** , como decorrência do direito à privacidade.

Essa distinção é especialmente relevante para a devida compreensão da diferença entre as hipóteses dos **incisos II e III do art. 7º, bem como os §§ 1º e 2º do art. 10 da Lei nº 12.965/2014.**

E nessa linha, pode-se adiantar que, ao enfeixar a disponibilização do conteúdo das comunicações privadas – no que se refere às informações em fluxo – com a exigência de ordem judicial, nas hipóteses e na forma da lei, o **art. 10, § 2º, da Lei nº 12.965/2014** veicula hipótese de relativização do sigilo das comunicações compatível, a princípio, com os limites do direito fundamental da personalidade correspondente à proteção do sigilo de dados e de comunicações, consagrado no citado **art. 5º, XII, da CF.**

A jurisprudência desta Suprema Corte tem reconhecido que a os limites constitucionais do sigilo alcança as comunicações telemáticas de dados. Neste sentido os seguintes precedentes:

> "Recurso ordinário em *habeas corpus* . Constitucional. Processual penal. (...) **Interceptação telemática** e prorrogações. Mencionada incompatibilidade do parágrafo único do art. 1º da Lei nº 9.296/96 com o art. 5º, inciso XII, da Constituição Federal. Inconstitucionalidade não verificada. Inexistência no ordenamento jurídico constitucional vigente de garantias individuais de ordem absoluta. Doutrina e precedentes. **Exceção constitucional ao sigilo que alcança as comunicações de dados telemáticos** , visto que cláusula tutelar da inviolabilidade não pode constituir instrumento de salvaguarda de práticas ilícitas (HC nº 70.814/SP, Primeira Turma, Relator o Ministro Celso de Mello, DJ de 24/6/94). Recurso ordinário não provido. (...) O Supremo Tribunal Federal já decidiu pela licitude da "interceptação telefônica, determinada em decisão judicial fundamentada, quando necessária, como único meio de prova, à apuração de fato delituoso" (Inq nº 2.424/RJ, Pleno, Relator o Ministro Cezar Peluso, DJe de 26/3 /10). (...) Em face da concepção constitucional moderna de que inexistem garantias individuais de ordem absoluta, mormente com escopo de salvaguardar práticas ilícitas (v.g. HC nº 70.814/SP), **a exceção constitucional ao sigilo alcança as comunicações de dados telemáticos, não havendo que se cogitar de incompatibilidade do parágrafo único do art. 1º da Lei nº 9.296/96 com o art. 5º, inciso XII, da Constituição Federal** . Precedente e doutrina. 12. Recurso ordinário ao qual se nega provimento." (**RHC 132115** , Relator Ministro Dias Toffoli, **Segunda Turma** , julgamento em 06.02.2018, DJe 19.10.2018)
>
> "RECURSO ORDINÁRIO EM *HABEAS CORPUS* . APURAÇÃO DE CRIME DE FALSIDADE DOCUMENTAL. BUSCA E

APREENSÃO. VALIDADE. DILIGÊNCIA REALIZADA EM ÓRGÃO PÚBLICO. ARRECADAÇÃO DE COMPUTADORES SOBRESSALENTES À ORDEM JUDICIAL. ENTREGA VOLUNTÁRIA DAS MÁQUINAS PELA AUTORIDADE RESPONSÁVEL. CLÁUSULA DE RESERVA DE JURISDIÇÃO OBSERVADA. EXAME PERICIAL CONDICIONADO À POSTERIOR AUTORIZAÇÃO JUDICIAL. PRESERVAÇÃO DO DIREITO À INTIMIDADE. ACESSO AOS DADOS REGISTRADOS EM DISPOSITIVO ELETRÔNICO. SUPOSTA VIOLAÇÃO AO SIGILO DE CORRESPONDÊNCIA ELETRÔNICA. INOCORRÊNCIA. INDEFERIMENTO DE DILIGÊNCIAS EM PROCEDIMENTO CRIMINAL. CERCEAMENTO DE DEFESA. NÃO VERIFICAÇÃO. CONTRADITÓRIO E AMPLA DEFESA PRÓPRIOS DA FASE JUDICIAL. RECURSO DESPROVIDO. (...) 2. Conquanto verificada a entrega voluntária ao agente policial, o exame pericial nos equipamentos apreendidos, condicionado à autorização específica da autoridade judicial responsável pela supervisão do caderno investigativo, resguarda a regularidade da apreensão e o direito à privacidade do repositório de dados e de informações neles contidos. **3. Descabe invocar a garantia constitucional do sigilo das comunicações de dados quando o acesso não alcança a troca de dados, restringindo-se apenas às informações armazenadas nos dispositivos eletrônicos. A orientação jurisprudencial do STF assinala que "A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270)" (RE 418.416, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, DJ 19.12.2006).** 4. Em se tratando de instrumento destinado à formação da *opinio delicti* do órgão acusatório, o procedimento administrativo de investigação criminal não demanda a amplitude das garantias constitucionais da ampla defesa e do contraditório, próprias da fase judicial. Eventual prejuízo advindo do indeferimento de diligências no curso das apurações (nomeação de assistente técnico e formulação de quesitos) é passível de questionamento na ação penal decorrente do respectivo inquérito policial. 5. Recurso ordinário em habeas corpus desprovido. (**RHC 132062** , Relator Ministro Marco Aurélio, Relator p/ acórdão: Ministro Edson Fachin, Primeira Turma, julgamento em 22.11.2016, DJe 24.10.2017)"

" **SIGILO DE DADOS – AFASTAMENTO** . Conforme disposto no **inciso XII do artigo 5º da Constituição Federal, a regra é a privacidade quanto à correspondência, às comunicações telegráficas, aos dados e às comunicações, ficando a exceção – a quebra do sigilo – submetida ao crivo de órgão equidistante – o Judiciário – e, mesmo assim, para efeito de investigação criminal ou instrução processual penal** ." (**RE**

389808 , Relator Ministro Marco Aurélio, Tribunal Pleno, julgamento em 15.12.2010, DJe 10.5.2011)

Para que dúvida não pairasse quanto ao alcance das garantias constitucionais, no que se refere ao ambiente digital, o **art. 3º, II, da Lei nº 12.965/2014** reafirmou a **proteção da privacidade** como princípio norteador da disciplina do uso da internet no Brasil. Os seus **arts. 7º e 8º** consagram o papel essencial **do acesso à internet** para o **pleno exercício da cidadania** , assegurando, entre outros direitos, a **inviolabilidade e o sigilo do fluxo de comunicações** do usuário, salvo por ordem judicial, na forma da lei , bem como a **inviolabilidade e o sigilo** das suas **comunicações privadas armazenadas** , salvo por ordem judicial .

O **art. 5º, XII, da CF,** a seu turno, não dá margem a exegese outra que não a de que a lei somente pode autorizar a suspensão do sigilo de comunicações privadas **para fins de investigação criminal ou instrução processual penal** . Trata-se de limite ao alcance da atividade legislativa, adstrita que está aos contornos traçados na Lei Maior. Ainda que a legislação não estampe no próprio texto a limitação do seu alcance, é dever do intérprete atentar para a regência constitucional ao aplicar a lei no caso concreto.

Entendo, nessa linha de raciocínio, que a adequada exegese dos **arts. 7º, II e III, e 10, § 2º, do Marco Civil da Internet** , à luz do **art. 5º, XII, da Constituição da República** , conduz à conclusão inequívoca de que, à maneira das comunicações telefônicas, a inviolabilidade do sigilo das comunicações realizadas pela internet somente pode ser excepcionada, por ordem judicial, **no âmbito da persecução penal** . Na expressa dicção da Constituição, "*para fins de investigação criminal ou instrução processual penal*".

11. Do dever de guarda de metadados

Impõe-se o registro de que a obrigação de guarda de metadados, de que trata o **art. 15 do Marco Civil da Internet** , não se estende a conteúdo. O referido preceito é expresso ao determinar, aos provedores de aplicações de internet, a guarda, sob sigilo, dos **registros de acesso (metadados)** . Eis o seu teor:

"Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma

organizada, profissionalmente e com fins econômicos deverá manter os respectivos **registros de acesso a aplicações de internet** , sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no *caput* a guardarem **registros de acesso a aplicações de internet** , desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os **registros de acesso a aplicações de internet** sejam guardados, inclusive por prazo superior ao previsto no *caput* , observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo."

Tal obrigação, à evidência, não se estende ao **conteúdo** das comunicações. Caso assim fosse, equivaleria a determinar que companhias telefônicas armazenassem as gravações de todas as chamadas realizadas por seus usuários, por igual período, para que ficassem à disposição em caso de eventual mandado judicial para sua disponibilização.

12. Da Lei Geral de Telecomunicações (Lei nº 9.472/1997)

A organização dos serviços de telecomunicações, no Brasil, é objeto da **Lei nº 9.472/1997 (Lei Geral das Telecomunicações)** . Seu **art. 60** define como serviço de telecomunicações o " *conjunto de atividades que possibilita a oferta de telecomunicação* ", sendo esta descrita, por sua vez, como " *a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza* " (**art. 60, § 1º, da LGT**).

Os equipamentos, aparelhos, dispositivos, terminais e demais meios necessários à realização da telecomunicação (computadores pessoais, *notebooks* , *tablets* , telefones celulares etc) são legalmente designados como estações de telecomunicações (**art. 60, § 2º, da LGT**).

Atividades como a desempenhada pelo aplicativo *WhatsApp* são consideradas, conforme a disciplina legislativa, **serviços de valor adicionado**

, na medida em que acrescentam, a um serviço de telecomunicações que lhe dá suporte e com qual não se confundem, novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações.

Os **provedores de serviços de valor adicionado são usuários** da infraestrutura das redes e dos serviços de telecomunicações que lhes dão suporte, com os direitos e deveres inerentes a essa condição (**art. 61, § 1º**). Nessa condição, o uso das redes de serviços de telecomunicações, para a prestação dos serviços de valor adicionado lhes é assegurado pela lei (**art. 61, § 2º**).

Enquanto **serviços de valor adicionado** , na dicção da Lei Geral das Telecomunicações, as **aplicações de internet** de que trata a **Lei nº 12.965 /2014 (Marco Civil da Internet)** , não se enquadram, elas mesmas, como serviços públicos de telecomunicações.

Como pontuou, na qualidade de *amicus curiae* , a ASSESPRO NACIONAL, ao atuarem no tecnológico e especialíssimo ambiente informatizado da Internet, para viabilizar a mais ampla comunicação entre as pessoas, os provedores de aplicações de Internet desenvolvem, sob o manto da livre iniciativa (**art. 170, *caput* , da CF**) atividade protegida pelos direitos fundamentais à manifestação do pensamento (**art. 5º, IV, da CF**) ao acesso à informação (**art. 5º, XIV, da CF**) e à liberdade da expressão da atividade intelectual, científica e de comunicação, independente de censura ou licença (**art. 5º, IX, da CF**).

13. Influxos do *standard* normativo da Convenção de Budapeste sobre o Cibercrime

Em julho de 2019, teve início o processo de adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético, que passou a vigorar no país a partir da sua promulgação pelo Decreto nº 11.491, de 12 de abril de 2023 (DOU de 13.4.2023) Se, ao Estado brasileiro, mesmo antes da adesão formal, já era facultado participar das reuniões relativas à Convenção e seus protocolos, na condição de observador, uma vez completado o procedimento de adesão, o Brasil está vinculado à sua observância, sendo inafastável, no contexto do presente esforço exegético, o equacionamento dos influxos desse *standard* normativo sobre o tema de fundo aqui vertido.

Adotada em 23 de novembro de 2001 no âmbito do Conselho da Europa e aberta à adesão de Estados não-membros dessa organização, a **Convenção**

de Budapeste sobre o Cibercrime , em vigor desde 1º de julho de 2004, reconhece legítima, no seu **Artigo 18º** , a adoção, pelos Estados-partes, de medidas legislativas e outras necessárias para habilitar suas autoridades competentes a ordenarem, a um fornecedor de serviços que os preste no seu território, que comunique dados na sua posse ou sob o seu controle, relativos a seus usuários, **que não sejam dados relativos ao tráfego ou ao conteúdo** , e que permitam determinar:

> **a)** O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;
>
> **b)** A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;
>
> **c)** Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

No que se refere ao dados correspondentes ao **conteúdo de comunicações** , o emprego legítimo de medidas para obrigar um fornecedor a recolher ou registrar esse conteúdo ou viabilizar que seja recolhido ou registrado pelas autoridades competentes é objeto do **Artigo 21º da Convenção** . O preceito exige **(i)** que se aponte no direito interno, um prévio leque de **infrações definidas como especialmente graves** , a ponto de justificar a natureza da medida; **(ii)** que não se exija mais do que a capacidade técnica do fornecedor pode oferecer; e **(iii)** que a medida tenha como objeto o conteúdo de comunicações **específicas** .

Em ambas as hipóteses (tanto o procedimento do Artigo 18 quanto o procedimento do Artigo 21 da Convenção), a legitimidade da adoção das medidas encetadas está subordinada, ainda, às disposições dos seus **Artigos 14 e 15** , que sujeitam o exercício de tais poderes **(i)** ao âmbito de **investigação criminal ou instrução processual penal** ; **(ii)** à observância das **condições** e **salvaguardas** estabelecidas pela legislação nacional, que deve assegurar proteção **adequada dos direitos humanos e das liberdades** ; e **(iii)** à observância do **princípio da proporcionalidade** .

14. Análise da constitucionalidade dos preceitos impugnados

Assentado esse pano de fundo jurídico e conceitual, concluo que o **art. 10, § 2º, da Lei nº 12.965/2014** confere suporte normativo para comando

judicial de disponibilização do conteúdo de comunicações privadas travadas por meio de aplicações de mensagens apenas no âmbito de investigação criminal ou da instrução processual penal.

Ao permitir a disponibilização do conteúdo de comunicações privadas – em fluxo ou armazenadas – somente por ordem judicial, nas hipóteses e na forma que a lei estabelecer, o **art. 10, § 2º, da Lei nº 12.965/2014** transita dentro do campo semântico demarcado pelo **art. 5º, XII, da Constituição da República** , segundo o qual o sigilo das comunicações telegráficas, de dados e das comunicações telefônicas pode ser levantado, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Tratando-se de norma restritiva de direito fundamental da personalidade, sua aplicação legítima depende de sua conformidade com o **art. 5º, XII, da Constituição** : ordem judicial dada no âmbito de investigação criminal ou instrução processual penal.

Questiona-se, na sequência, a licitude do uso, nas comunicações privadas, de tecnologias de proteção do sigilo e da segurança das comunicações, notadamente das tecnologias **criptográficas** que tornem materialmente inviável o cumprimento, pela plataforma, de eventual comando judicial de disponibilização do conteúdo de comunicações privadas havidas por seu intermédio. Sob outro enfoque, há que perquirir se pode o Estado obrigar os particulares que oferecem plataformas ou serviços de comunicação privada a adotarem mecanismos que assegurem o acesso ao conteúdo das conversas, caso seja licitamente determinada a sua disponibilização, nos moldes do **art. 10, § 2º, da Lei nº 12.965/2014** ? E ainda, se pode ser apenada a não observância de determinação nesse sentido?

Entendo que a resposta no ponto é negativa. O poder de o Estado determinar a disponibilização do conteúdo de mensagens no âmbito de investigação criminal ou da instrução processual penal não conduz à conclusão de que ilegal o oferecimento de serviço que adote tecnologia por força da qual inacessível, esse conteúdo, ao próprio provedor da plataforma. Uma vez desenvolvida e adotada por ele, um particular, tecnologia voltada a garantir a segurança e a privacidade de comunicações, e oferecida essa tecnologia, como valor agregado, a outros particulares que contratam seus serviços, não pode o Estado compeli-lo a oferecer um serviço menos seguro e vulnerável, sob o pretexto de que pode vir,

eventualmente, a utilizar essa vulnerabilidade artificial, para cumprir ordem judicial a respeito. Isso significaria tornar ilegal a criptografia, ou pelo menos alguns de seus usos.

15. A questão da criptografia

Embora a ciência da criptografia seja tão antiga quanto a escrita, o desenvolvimento e disseminação de tecnologias criptográficas na contemporaneidade é o que torna as comunicações e as transações online mais seguras e, em consequência, a sociedade também fica mais segura.

Outrora monopólio de governos, a invenção da criptografia de chave pública tornou viável o uso da tecnologia por particulares, e possível o comércio eletrônico. Ela é essencial para a segurança das transações eletrônicas que viabilizam a própria existência de operações comerciais e financeiras na Internet.

Lembro-me do conto "A Carta Roubada", de Edgar Allan Poe, em que o conteúdo de um documento de natureza pessoal é mantido em segredo, em meio à realização de buscas no aposento onde repousava, sem maiores esforços para encobri-lo. De modo similar, o emprego da criptografia de chave pública confere segurança e privacidade às comunicações efetuadas por meio de redes abertas ao acesso de todos.

Seria um inadmissível contrassenso, e mesmo retrocesso, tornar ilegal ou limitar dessa maneira o uso de criptografia. Relatório do *National Research Council* (Conselho Nacional de Pesquisa) dos EUA apontava, já em 1996, que os "*esforços para controlar a criptografia seriam ineficazes, e seus custos excederiam qualquer benefício imaginável*".

Além disso, a difusão da criptografia também tem garantido a segurança da comunicação de grupos de direitos humanos e indivíduos que se mobilizam contra regimes opressivos ao redor do mundo.

Em certa medida, a liberdade fundamental que assegura ao indivíduo o direito de fechar o portão de casa com um cadeado, elevar a altura do muro ou pendurar uma cortina na janela, autoriza cogitar uma espécie de direito fundamental à encriptação, ou pelo menos que o uso da criptografia consiste em uma ferramenta indispensável, nos dias de hoje, para assegurar o direito à privacidade.

Volto à pergunta: pode o Estado compelir fabricantes de dispositivos eletrônicos, provedores de aplicações digitais ou autores de *software* a implementar, nos produtos que desenvolvem, mecanismos para desabilitar ou contornar tecnologias de encriptação neles incorporadas?

A ideia, que não é nova, de forçar a implementação de " *back doors* " (portas dos fundos) em *softwares* de criptografia, para franquear acesso furtivo a autoridades públicas, ainda que limitada a situações excepcionais, vem sendo abandonada em todo o mundo. Medidas dessa natureza teriam como consequência, invariavelmente, tornar as tecnologias de comunicação menos seguras para todos os seus usuários, além de violar frontalmente a proteção da liberdade de expressão e a proteção do sigilo das informações. Seria, além disso, potencialmente inócua, porque os usuários que se utilizam de aplicações para o cometimento de crimes migrariam para aplicativos fora do alcance das autoridades.

Consagrada uma liberdade na Constituição, a chave hermenêutica para o seu devido dimensionamento, em face de transformações tecnológicas que alteram o modo como essa liberdade é exercida, há de buscar, tanto quanto possível, a sua máxima preservação. O Estado não pode ambicionar que a migração para uma plataforma diversa da anteriormente regulada signifique uma oportunidade para afrouxamento de garantias e liberdades. Ora,

> "Tomadas as liberdades substantivas dos indivíduos como experiências empíricas de fruição de direitos, como oportunidades efetivas de moldar o próprio destino e ajudar uns aos outros, ou, ainda, como expansão das capacidades das pessoas de levar o tipo de vida que elas valorizam, é possível afirmar que o advento de novos patamares tecnológicos está diretamente relacionado ao surgimento de novas liberdades e, consequentemente, por demandas no sentido da sua concretização."

As expectativas razoáveis dos titulares dos direitos constitucionais devem ser mantidas. Qual é o sentido de uma Constituição que, no ano de 2020, protege o sigilo das comunicações telegráficas, mas não protege o sigilo das comunicações realizadas por aplicações de internet ou qualquer outro meio pelo qual as pessoas de fato se comunicam hoje? A Constituição não é um simulacro, não pode ser lida como se fosse um museu de direitos.

Em 2016, acolhendo pedido apresentado pelo FBI (*Federal Bureau of Investigation*), um tribunal federal dos EUA ordenou à empresa Apple que implementasse mecanismo pelo qual pudesse ser acessado o conteúdo armazenado em um dispositivo informático por ela fabricado – um iPhone utilizado por um dos atiradores do massacre de San Bernardino, ocorrido no final do ano anterior, 2015. Tratava-se, em síntese, de substituir a ferramenta de *software* de segurança e proteção da privacidade instalada no aparelho por uma nova versão, vulnerável a acesso de terceiros, a ser desenvolvida. Deliberadamente enfraquecer a segurança de um produto cuja função é proporcionar privacidade às comunicações do seu usuário.

O caso, porém, foi abandonado pelo órgão investigador após ter obtido sucesso em acessar as informações contidas no celular com a assistência de ferramentas desenvolvidas por um terceiro.

Na ocasião, Zeid Raad Al Hussein, Alto-Comissário das Nações Unidas para os Direitos Humanos de 2014 a 2018, afirmou que o caso arriscava abrir uma Caixa de Pandora que poderia ter implicações extremamente perigosas sobre ativistas de direitos humanos, jornalistas, denunciantes e dissidentes políticos, sendo um "presente para regimes autoritários" e criminosos.

A criptografia, como recurso tecnológico, tem-se revestido de especial relevo na implementação de direitos humanos. Com efeito, no mundo atual, é importante componente da proteção dos direitos à privacidade e à liberdade de expressão (**artigos 17 e 19 do Pacto Internacional sobre Direitos Civis e Políticos, no âmbito das Nações Unidas**):

> **Artigo 17**
>
> "(...) ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência"
>
> **Artigo 19**
>
> "Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro meio de sua escolha."

Em estudo publicado em 2015, **Chaves para promoção de Sociedades do Conhecimento inclusivas** , a UNESCO (Organização das Nações Unidas

para a Educação, a Ciência e a Cultura) concluiu que uma Internet segura deve ser construída sobre quatro pilares que se complementam: **acesso a informação e conhecimento, liberdade de expressão, privacidade e ética** .

Sob essa ótica, a proteção de dados e a proteção da privacidade são fatores críticos para a preservação não só da liberdade de expressão, como da própria segurança do usuários das redes de informação e comunicação:

> "(...) a manipulação de práticas de segurança, como a introdução de "portas dos fundos" no *software* , para permitir acesso legítimo ao governo, pode deixar os usuários da Internet vulneráveis a outras ameaças ilegítimas. Os invasores podem entrar pelas mesmas portas, tornando os sistemas menos seguros. Desse modo, embora a vigilância estatal seja vista como justificada em muitos aspectos, as abordagens da questão têm levantado preocupações de que o remédio pode prejudicar os direitos e liberdades democráticos que ele deveria servir para proteger."

O *trade-off* aqui, portanto, não se dá entre segurança pública e privacidade, pois a pretensão que ameaça a privacidade, ainda que fundada no combate a uma ameaça imediata à segurança, vulnera no longo prazo, também a segurança das redes e seus usuários como um todo, expondo-os a maiores riscos de ciberataques, fraudes, roubos de identidade, invasão da intimidade extorsão etc.

A mesma tecnologia que tornaria mais fácil às autoridades de segurança pública acessarem conteúdo armazenado pode – e, existindo, será – utilizada por criminosos para terem acesso a informações privadas de futuras vítimas.

O referido estudo reconhece, ainda, o papel desempenhado pela criptografia na criação de condições materiais para o exercício dos direitos relacionados à proteção da privacidade e da liberdade de expressão:

> "Na medida em que nossos dados possam ser considerados representativos de nós mesmos, a criptografia tem um papel a desempenhar na proteção de quem somos e na prevenção de abuso de conteúdo do usuário. Também permite uma proteção significativamente maior da privacidade e do anonimato em trânsito, garantindo que o conteúdo (e às vezes também os metadados) das comunicações sejam vistos apenas pelo destinatário pretendido."

Para David Kaye , **Relator Especial das Nações Unidas sobre a promoção e a proteção do direito à liberdade de opinião e de expressão** , a criptografia,

> "fornece aos indivíduos um meio de proteger sua privacidade, capacitando-os a navegar, ler, desenvolver e compartilhar opiniões e informações sem interferência e permitir que jornalistas, organizações da sociedade civil, membros de grupos étnicos ou religiosos, os perseguidos por causa de sua orientação sexual ou identidade de gênero, ativistas, acadêmicos, artistas e outros exerçam os direitos à liberdade de opinião e de expressão."

Adotada em 1997 pela **Organização para a Cooperação e Desenvolvimento Econômico - OCDE** , a Recomendação Relativa às Diretrizes para Política de Criptografia, sem deixar de reconhecer o risco de uso da tecnologia para atividades ilegais, proclama o princípio segundo o qual " *o direito fundamental dos indivíduos à privacidade, incluindo o sigilo das comunicações e a proteção dos dados pessoais, deve ser respeitado nas políticas nacionais de criptografia e na implementação e uso de métodos criptográficos.* "

Trata-se, pois, de tecnologia que atua no sentido da realização material da garantia de preservação do sigilo das comunicações consagrada no **art. 5º, XII, da CF** . Entendimento diverso significaria submeter a regra, que é a proteção do sigilo das comunicações, à exceção, que é o acesso do Estado ao conteúdo da comunicação privada no curso da persecução criminal.

Pretensões no sentido de forçar a adoção de mecanismos tecnológicos que permitam o acesso estatal à comunicação privada, ainda que em caráter excepcional, equivalem a restringir o mercado de cadeados residenciais àqueles que também puderem ser abertos por uma chave especial mantida em posse da polícia.

Sendo viável o cumprimento da ordem judicial, por óbvio deve ela ser atendida, seja pelo provedor do serviço que recebe o comando de disponibilização, seja por agentes do Estado incumbidos de efetivar o acesso. O provedor que, podendo, não cumpre a determinação, incorre em descumprimento de ordem judicial, podendo ser impelido ao cumprimento, inclusive com a imposição de *astreintes* .

16. Das sanções previstas no art. 12, III e IV, da Lei nº 12.965/2014

O último questionamento que se põe consiste em saber se o art. 12, III e IV, da Lei nº 12.965/2014 autoriza sejam impostas a suspensão temporária e a proibição do exercício das atividades a provedor responsável pela guarda de registros de conexão e de acesso a aplicações de internet, dados pessoais e do conteúdo de comunicações privadas, em caso de descumprimento de ordem judicial de disponibilização do conteúdo de comunicações privadas.

Embora tenha anteriormente concluído pela **resposta negativa,** o amadurecimento da minha compreensão sobre o tema e a leitura mais detida e sistemática dos **arts. 7º, II e III, 10, 11 12, III e IV, 13, 15 e 22 da Lei nº 12.965/2014** conduzem-me, no presente momento, a resposta diversa. É que o **art. 12, III e IV, da Lei nº 12.965/2014** autoriza seja imposta a suspensão temporária ou a proibição do exercício das atividades que envolvem a " *operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações* " (atos previstos no art. 11). E o *caput* do art. 12 é expresso ao enunciar que tais sanções podem ser cominadas em caso de descumprimento, pelo provedor de conexão ou de aplicações de internet responsável pela guarda de registros de conexão e de acesso, de dados pessoais e do conteúdo de comunicações privadas, dos deveres fixados nos arts. 10 e 11, quais sejam:

(a) violação do dever de preservar a intimidade, a vida privada, a honra e a imagem dos usuários do serviço;

(b) disponibilização do conteúdo de comunicações privadas a qualquer terceiro, público ou privado, sem ordem judicial que tenha sido proferida no âmbito de investigação criminal ou de instrução processual penal, em hipótese e na forma permitida pela lei;

(c) falha em informar, de forma clara, as medidas e os procedimentos de segurança e de sigilo adotados para a guarda dos registros;

(d) descumprimento da legislação brasileira, em particular **os direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e dos registros** , nas operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações, quando pelo menos um desses atos ocorra em território nacional;

(e) descumprimento do dever de prestar informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao **respeito à privacidade e ao sigilo das comunicações;**

(f) descumprimento de ordem judicial para disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata a lei, no âmbito de investigação criminal ou de instrução processual penal;

(g) descumprimento de ordem judicial para disponibilização do conteúdo de comunicações privadas específicas, no âmbito de investigação criminal ou de instrução processual penal, nas hipóteses e na forma de lei que estabeleça prévio leque de infrações definidas como especialmente graves, a ponto de justificar a natureza da medida.

O **art. 12, III e IV, da Lei nº 12.965/2014** permite a suspensão ou proibição, repito, das atividades que envolvem a " *operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações"* para salvaguardar a integridades desses elementos em face de provedor que venha a vulnerá-los. **Trata-se de uma norma protetiva não só dos direitos dos usuários, mas dos direitos de terceiros que podem vir a ser afetados pelas atividades ali disciplinadas.**

Não se descura, como já afirmei, que a *mens legis* das sanções previstas no **art. 12 da Lei nº 12.965/2014** é voltada à proteção da privacidade, e não o contrário, apenando a violação da privacidade e de outros direitos dos usuários fora dos estritos limites legais.

Nada obstante, também não ignorou, o legislador, a necessidade de balancear o escopo da proteção, em face dos demais valores e bens jurídicos assegurados, observados dos limites delineados pelo **art. 5º, XII, da Constituição da República** , **o que enseja a alteração da minha conclusão anterior, no ponto.** Passo a admitir que autorizada a imposição das penalidades previstas no art. 12, III e IV, da Lei nº 12.965/2014 inclusive em face do descumprimento de ordem judicial para disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata a lei, no âmbito de investigação criminal ou de instrução processual penal; e do descumprimento de ordem judicial para disponibilização do conteúdo de comunicações privadas específicas, no âmbito de investigação criminal ou de instrução processual penal, nas hipóteses e na forma de lei que estabeleça prévio leque de infrações definidas como especialmente graves, a ponto de justificar a natureza da medida.

Em síntese, o **art. 12 da Lei nº 12.965/2014** , ao sancionar as **infrações às normas** previstas nos seus **arts. 10 e 11** , alcança **as violações aos deveres de guarda, tal como ali dimensionados, tanto quanto as violações aos comandos de disponibilização nas hipóteses ali previstas.**

À falta de previsão legal, ainda, não há justificativa para que as penalidades previstas nos **incisos do art. 12 da Lei nº 12.965/2014** sejam impostas, necessariamente, de forma progressiva. A imposição da penalidade deve ser sopesada caso a caso e deve, por óbvio, ser proporcional à infração.

17. Conclusão

(i) julgo improcedente o pedido de declaração de inconstitucionalidade do art. 12, III e IV, da Lei nº 12.965/2014;

(ii) julgo procedente o pedido de interpretação conforme a Constituição do art. 10, § 2º, da Lei nº 12.965/2014, a fim de assentar, à luz do art. 5º, XII, da Constituição, exegese segundo a qual "*o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º, e para fins de investigação criminal ou instrução processual penal*";

(iii) julgo improcedente o pedido sucessivo de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei nº 12.965/2014, à compreensão de que não abrangido em sua hipótese de incidência o conteúdo que dele se pretende excluir;

(iv) julgo parcialmente procedente o pedido sucessivo de interpretação conforme a Constituição do art. 12, III e IV, da Lei nº 12.965/2014 apenas para **(a)** assentar que autorizada a imposição das penalidades de suspensão temporária das atividades e de proibição de exercício das atividades, aos provedores de conexão e de aplicações de internet, nos casos de descumprimento da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, **inclusive em face do descumprimento, no âmbito de investigação criminal ou de instrução processual penal, de *(a.1)* ordem judicial para disponibilização de registro de conexão e de acesso a aplicações de internet e dados pessoais, ou *(a.2)* ordem judicial para disponibilização do conteúdo de comunicações privadas específicas, quando materialmente possível o seu cumprimento, nas hipóteses e na forma de lei que estabeleça prévio leque de infrações definidas como especialmente graves, a ponto de justificar a natureza da medida; (b)** ficando afastada, todavia, qualquer exegese que – isoladamente ou em combinação com o **art. 7º, II e III, da Lei nº 12.965/2014** – estenda a sua

hipótese de incidência de modo a abarcar o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação.

É como voto.