MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA

EXCELENTÍSSIMO SENHOR MINISTRO PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL

PETIÇÃO INICIAL AJCONST/PGR Nº 1335730/2023

A **PROCURADORA-GERAL DA REPÚBLICA**, com fundamento nos arts. 102, I, "a" e "p", 103, VI e § 2º, e 129, IV, da Constituição Federal; no art. 46, parágrafo único, I, da Lei Complementar 75, de 20.5.1993 (Lei Orgânica do Ministério Público da União); e na Lei 9.868, de 10.11.1999, vem propor

AÇÃO DIRETA DE INCONSTITUCIONALIDADE POR OMISSÃO COM PEDIDO DE MEDIDA CAUTELAR

contra a ausência de atuação normativa do Congresso Nacional, representada pela omissão parcial na regulação do uso, por órgãos e agentes públicos, de **programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal** – *smartphones*, *tablets* e dispositivos eletrônicos similares – a fim de dar efetividade aos mandamentos constitucionais de proteção estatal da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados, estatuídos no art. 5º, X e XII, da Constituição Federal.

I. CABIMENTO DA AÇÃO

Cabimento da ação direta de inconstitucionalidade por omissão pressupõe a existência de disposição do texto constitucional cuja efetividade dependa de adoção de medida por parte do Poder Legislativo ou de órgão da administração pública.

Omissão legislativa que dá ensejo à propositura desse instrumento de controle concentrado tanto pode ser total – caracterizada pela existência de lacuna normativa sobre a matéria – quanto parcial – no caso de, apesar de existente norma infraconstitucional, essa não satisfaça plenamente o preceito constitucional, porque insuficiente para concretizar os direitos tutelados.

Acerca da omissão suscetível de impugnação por meio de ADO, afirma Luiz Guilherme Marinoni:

> *(…) omissão inconstitucional, objeto da ação direta de inconstitucionalidade, é, em princípio, normativa. É a falta da edição de norma – cuja incumbência é, em regra, do Legislativo, mas que também pode ser do Executivo e até mesmo do Judiciário – que abre oportunidade à propositura da ação. Neste sentido, pode ser objeto da ação a ausência de ato de caráter geral, abstrato e obrigatório.*
> *Assim, a ação não permite questionar apenas a ausência de atos normativos primários, mas também a falta de atos normativos secundários, como os regulamentos, de competência do Executivo, e, eventualmente, até mesmo a inexistência de atos normativos cabíveis ao Judiciário.*

> *No caso em que a lei não contém os elementos que lhe dão condição de aplicabilidade, a falta de regulamento é empecilho evidente para a efetividade da norma constitucional. Porém, a falta de ato de caráter não normativo, inclusive por poder ser enquadrado na previsão do art. 103, § 2º, da CF, que remete à ciência para a "adoção de providências necessárias", igualmente pode ser objeto de omissão inconstitucional e da correspondente ação direta.*
> *Pense-se, por exemplo, na falta de organização do Judiciário ou na insuficiência de estruturação da saúde pública. É possível falar, nessas hipóteses, de falta de tutela fático-concreta aos direitos fundamentais, que, como é óbvio, não sofrem apenas com a carência de tutela normativa, mas também com a ausência de tutela fática de natureza administrativa.*
> *Portanto, a omissão inconstitucional, objeto da ação, não decorre, necessariamente, de previsão de legislar contida em norma constitucional, mas pode advir da falta ou da insuficiência de norma, ou de prestação fático-administrativa, para proteger ou viabilizar a realização de um direito fundamental. Evidencia-se, neste momento, que o legislador não tem dever apenas quando a norma constitucional expressamente lhe impõe a edição de lei, mas também quando um direito fundamental carece, em vista da sua natureza e estrutura, de norma infraconstitucional, especialmente para lhe outorgar tutela de proteção.*[1]

Em obra doutrinária, assinala o Ministro Gilmar Mendes que o controle abstrato da omissão inconstitucional é essencial para a preservação da força normativa da Constituição e volta-se, precipuamente, à "*defesa da ordem fundamental contra condutas com ela incompatíveis*", tendo por objeto a "*mera inconstitucionalidade morosa dos órgãos competentes para a concretização da norma*

1 MARINONI, Luiz Guilherme. O Sistema Constitucional Brasileiro. In: SARLET, Ingo Wolfgang; ____; MITIDIERO, Daniel. *Curso de direito constitucional*. 3. ed. São Paulo: Revista dos Tribunais, 2014, p. 1.241-1.242.

constitucional", abarcando tal controle "*não só a atividade legislativa, mas também a atividade tipicamente administrativa que pudesse, de alguma maneira, afetar a efetividade de norma constitucional*".[2]

Sobre a chamada *inertia deliberandi* – é dizer, a mora do parlamento em concluir o processo legislativo e promulgar leis –, observa ainda:

> *(…) a concretização da ordem fundamental estabelecida na Constituição de 1988 carece, nas linhas essenciais, de lei. Compete às instâncias políticas e, precipuamente, ao legislador, a tarefa de construção do Estado constitucional. Como a Constituição não basta em si mesma, têm os órgãos legislativos o poder e o dever de emprestar conformação à realidade social. A omissão legislativa constitui, portanto, objeto fundamental da ação direta de inconstitucionalidade em apreço.*
> *Esta pode ter como objeto todo o ato complexo que forma o processo legislativo, nas suas diferentes fases. Destinatário principal da ordem a ser emanada pelo órgão judiciário é o Poder Legislativo. (…)*
> *Questão que ainda está a merecer melhor exame diz respeito à* inertia deliberandi *(discussão e votação) no âmbito das Casas Legislativas. Enquanto a sanção e o veto estão disciplinados, de forma relativamente precisa, no texto constitucional, inclusive no que concerne a prazos (art. 66), a deliberação não mereceu do constituinte, no tocante a esse aspecto, uma disciplina mais minuciosa. (…)*
> Quid juris, *então, se os órgãos legislativos não deliberarem dentro de um prazo razoável sobre projeto de lei em tramitação? Ter-se-ia aqui uma omissão passível de vir a ser considerada morosa no processo de controle abstrato da omissão?*
> *(…) peculiaridades da atividade parlamentar, que afetam, inexoravelmente, o processo legislativo, não justificam, todavia, uma conduta ma-*

2 MENDES, Gilmar F., BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional.* 6. ed. São Paulo: Saraiva, 2011, p. 1.289-1.291.

> *nifestamente negligente ou desidiosa das Casas Legislativas, conduta esta que pode pôr em risco a própria ordem constitucional.*
> *Não temos dúvida, portanto, em admitir que também a* inertia deliberandi *das Casas Legislativas pode ser objeto da ação direta de inconstitucionalidade da omissão. Assim, pode o Supremo Tribunal Federal reconhecer a mora do legislador em deliberar sobre questão, declarando, assim, a inconstitucionalidade da omissão.*[3]

Também ao analisar a inércia legislativa, Anna Cândida da Cunha Ferraz situa-a como um dos processos informais de mutação da Constituição:

> *A inércia provoca mutação inconstitucional na Constituição quando a omissão dos poderes constituídos é intencional, provisória mas prolongada, de tal sorte que paralisa a aplicação da norma constitucional, evidentemente não desejada pelo constituinte. Configura, na verdade, uma inconstitucionalidade por omissão, figura hoje consagrada inclusive na Constituição Brasileira de 1988. Como modalidade de processo de mutação da constituição a inércia é processo pernicioso, que acarreta consequências desastrosas à vida constitucional dos Estados. De um lado porque, ao contrário dos demais processos de mutação, raramente busca adaptar a Constituição à realidade. De outro, porque arrasta consigo, quase que invariavelmente, a descrença na Constituição.*[4]

Omissão inconstitucional que enseja a propositura de ADO, assim, pode advir não somente da falta de legislação expressamente exigida por dispositivo do texto constitucional, mas também da ausência ou insuficiência

---

3 *Idem*, p. 1.293-1.294.

4 FERRAZ, Anna Cândida da Cunha. Mutação, reforma e revisão das normas constitucionais. In: CLÈVE, Clèmerson Merlin; BARROSO, Luís Roberto (orgs.). *Direito Constitucional:* teoria geral da constituição. São Paulo: Revista dos Tribunais, 2011, p. 791.

de prestação – legislativa ou fático-administrativa – que obste a concretização de regras e princípios insertos na Lei Maior.

Nesta ação direta, a inconstitucionalidade que se busca sanar diz respeito à omissão parcial do legislador nacional em dar efetividade plena e conferir proteção eficaz aos mandamentos contidos no art. 5º, X e XII, da Constituição Federal, que estabelece:

> *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
> *(…)*
> *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;*
> *(…)*
> *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; (…).*

A exceção prevista na parte final inciso XII do art. 5º da CF foi, em princípio, disciplinada pelo Congresso Nacional com a edição da Lei 9.296, de 24.7.1996, que estabeleceu os requisitos para a decretação da medida judicial de interceptação do fluxo das comunicações telefônicas e em sistemas de informática e

de telemática, no curso de investigação criminal e em instrução processual penal, de modo a assegurar o respeito aos direitos fundamentais dos investigados.

Também a tutelar a inviolabilidade das comunicações privadas em meio digital, pela rede mundial de computadores, houve a edição da Lei 12.965, de 23.4.2014 (Marco Civil da Internet – MCI), a qual trouxe como princípios a proteção da privacidade e dos dados pessoais (art. 3º, II e III), assim como a inviolabilidade da intimidade, da vida privada, do sigilo de comunicações na internet, de comunicações privadas armazenadas (art. 7º, I, II e III) e da proteção de registros de conexão e de acesso a aplicações de internet (arts. 7º, VII, 10 e 11).

Posteriormente, houve a promulgação da Lei 13.709, de 14.8.2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que estabeleceu como fundamentos da disciplina da proteção de dados o respeito à privacidade e à inviolabilidade da intimidade, da honra e da imagem (art. 2º, I e IV). Excepcionou o diploma, de seu âmbito de aplicação, o tratamento de dados pessoais para fins de segurança pública, de defesa nacional, de segurança do Estado, de investigação e de repressão a infrações penais (art. 4º, III); cuja regulação remeteu a legislação específica, a qual "*deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos em lei*" (art. 4º, § 1º).

Em que pese ao escopo visado por tais diplomas nacionais, ainda se verifica uma omissão inconstitucional parcial do legislador federal, no que se refere à concretização e à proteção suficiente e efetiva dos bens jurídicos tutelados pelo art. 5º, X e XII, da Constituição Federal.

É que, a partir dos mais recentes avanços tecnológicos, houve uma proliferação global de ferramentas de intrusão virtual, utilizadas no âmbito de **serviços de inteligência e de órgãos de repressão estatais,** para a vigilância remota, secreta e invasiva de dispositivos móveis de comunicação digital, sob o pretexto do combate ao terrorismo e ao crime organizado.

Tais ferramentas tecnológicas são aptas a interceptar comunicações telefônicas e telemáticas, a partir da "infecção" de dispositivos eletrônicos por um programa espião *(spyware*) e, com isso, possibilitar aos intrusos monitorar conversas, escutar o som ambiente pelo microfone do dispositivo; captar imagens por meio das câmeras frontal e traseira; determinar a localização em tempo real, por meio do sistema de GPS; capturar as imagens da tela e acompanhar em tempo real tudo o que é digitado (*keylogger*) ou visualizado pelo usuário, funcionalidades que podem vir a ser obtidas sem qualquer intervenção do usuário-vítima ("*zero click*").

Os graves impactos a direitos fundamentais advindos da utilização desregulada e ilegítima desses recursos por parte do poder público foram destacados em relatório elaborado pelo Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos, o qual aponta a ocorrência não só de violações à garantia do sigilo de dados e de comunicações, como também às garantias da intimidade, da vida privada e do devido processo legal, e ainda à liberdade de expressão, de manifestação do pensamento e de imprensa:

> *(…) Embora supostamente sejam empregadas para combater o terrorismo e o crime, essas ferramentas de programas espiões têm sido frequentemente usadas por razões ilegítimas, inclusive para reprimir opiniões críticas ou dissidentes, e aqueles que as expressam, incluindo jornalistas, figuras políticas da oposição e defensores dos direitos humanos.*
> *7. Os recursos das ferramentas e serviços de spyware oferecidos no mercado global são espantosos. O Pegasus, por exemplo, uma vez instalado, concede acesso completo e irrestrito a todos os sensores e informações dos dispositivos infectados, transformando efetivamente a maioria dos smartphones em dispositivos de vigilância 24 horas, acessando câmera e microfone, dados de geolocalização, e-mails, mensagens, fotos e vídeos, assim como todas as aplicações. Permite ao intruso obter um quadro detalhado da vida das suas vítimas, os seus pensamentos, preferências, atividades profissionais, pensamento político, saúde, situação financeira e vida social e íntima. Enquanto muitas ferramentas de hackeamento exigem alguma ação por parte da vítima, como clicar em um link ou abrir um anexo de uma mensagem, o Pegasus é instalado de forma furtiva, por meio do chamado "ataque de zero clique". O software torna quase impossível que as vítimas evitem a infecção depois de terem sido alvejadas.*
> *(…)*

9. O hackeamento de dispositivos de comunicação pessoal constitui uma grave interferência no direito à privacidade e pode estar relacionado a violações de uma série de outros direitos. Dado que a intrusão nos dispositivos de comunicação digital permite o acesso a rascunhos e históricos de busca e navegação, pode também permitir aprofundamentos sobre os processos de pensamento dos indivíduos sujeitos ao hackeamento, bem como suas visões e crenças políticas e religiosas, interferindo assim nas liberdades de opinião e de pensamento. As operações de hackeamento podem ser experiências profundamente traumáticas, afetando a saúde mental das vítimas e de suas famílias. Há relatos de que o hackeamento teria levado à prisão e detenção de defensores dos direitos humanos e políticos, alguns dos quais teriam sido submetidos a tortura. O hackeamento direcionado também tem sido associado a execuções extrajudiciais.

10. Além disso, atacar jornalistas e meios de comunicação com ferramentas de hackeamento prejudica gravemente a liberdade da mídia, principalmente porque as fontes de informação podem temer a detecção e as repercussões. A mera existência de programas de hackeamento pode ter efeitos inibitórios sobre a liberdade de expressão, sobre o trabalho da mídia e sobre o debate e participação públicos, potencialmente desgastando a governança democrática. Nas palavras da Suprema Corte da Índia, em sua recente decisão sobre o uso do programa de computador Pegasus, o efeito inibitório da vigilância seria um "ataque ao papel vital de fiscalização pública da imprensa".

11. O hackeamento também pode ter um impacto negativo nos direitos ao devido processo legal e ao julgamento justo. Obter acesso a um dispositivo pode permitir que um invasor não apenas observe o conteúdo desse dispositivo e suas interações com outros dispositivos, mas também manipule o dispositivo, inclusive pela alteração, exclusão ou adição de arquivos. Assim, é possível forjar provas para incriminar ou chantagear indivíduos tidos como alvo.[5]

5 NAÇÕES UNIDAS (2022). *O direito à privacidade na era digital: Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos*. Trad. DUTRA, Luíza, SANTARÉM, Paulo Renã da Silva. Genebra: ONU, 4.8.2022. Publicação original em:

Reportagens divulgadas pelos principais portais de comunicação internacionais revelaram, nos últimos anos, a aquisição desses softwares – em especial, a ferramenta *Pegasus*, desenvolvida pela empresa *NSO Group* – por regimes autoritários ao redor do mundo, para o fim de espionar jornalistas, defensores e ativistas de direitos humanos, adversários políticos e, até mesmo, chefes de Estado.[6]

Diante desse contexto, e sem desconsiderar o importante quadro de proteção a direitos fundamentais estabelecido por meio das Leis 9.296/1996, 12.965/2014 e 13.709/2018, constata-se ainda a **insuficiência** do ordenamento jurídico pátrio em conferir proteção adequada à garantia da inviolabilidade

---

https://digitallibrary.un.org/record/3985679?ln=en; acesso em 6.11.2023.

6 Entre os casos mais graves divulgados de utilização política do software *Pegasus* e de ferramentas *spyware,* tem-se o assassinato do jornalista saudita Jamal Khashoggi em 2018 (https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/?itid=lk_inline_manual_20), o assassinato do jornalista Cecilio Pineda Birto no México em 2017, bem como a espionagem de ativistas de direitos humanos, jornalistas e políticos de oposição naquele país (https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexiconso-client-cecilio-pineda-birto; https://noticias.uol.com.br/ultimas-noticias/efe/2021/07/20/governo-de-pena-nieto-espionou-lopezobrador-jornalistas-e-ativistas.htm), a espionagem de membros do sistema judicial e de políticos na Polônia (https://www.terra.com.br/noticias/em-watergate-polones-oposicao-foi-espionada-com-software-pegasus,5a7c22ef97cc5da07e9493a212c49f19fqg57yw8.html), a invasão do telefone do ex-presidente da França Emmanuel Macron e de outros chefes de Estado (https://www.dw.com/pt-br/macron-e-outros-l%C3%Adderes-foram-alvos-do-sistema-pegasus/a-58571315), a.espionagem de rivais políticos em Israel (https://internacional.estadao.com.br/noticias/geral,policia-israelense-usou-o-spyware-pegasus-paraespionar- rivais-de-netanyahu,70003954369), para citar alguns.

da vida privada, da intimidade e do sigilo de comunicações e dados pessoais em aparelhos digitais de comunicação pessoal, tais como *smartphones*, *tablets* e dispositivos eletrônicos similares, diante das novas ferramentas e sistemas de infiltração e de intrusão virtual remota, utilizados por órgãos e agentes públicos no curso de investigações e em atividades de inteligência.

Configura-se, assim, omissão parcial em tornar plenamente efetivos os mandamentos do art. 5º, X e XII, da Constituição Federal.

A ação direta de inconstitucionalidade por omissão é, portanto, o instrumento processual adequado para exortar o Poder Legislativo a adotar "*providências necessárias*" (art. 103, § 2º, da CF) direcionadas a sanar a omissão inconstitucional sob testilha e estabelecer, enquanto não suprida a mora, balizas e diretrizes provisórias para o uso das aludidas ferramentas, de modo a assegurar o respeito às garantias previstas nos referidos comandos do texto constitucional.

II. FUNDAMENTAÇÃO

A Constituição Federal de 1988 inseriu no rol dos direitos e das garantias fundamentais a inviolabilidade da intimidade e da vida privada das pessoas (art. 5º, X) e consolidou a garantia de proteção a diferentes espécies de comunicação pessoal, escrita ou oral (art. 5º, XII), tutelando "*em primeira linha, o processo comunicativo intersubjetivo, no sentido da reserva das comunicações*

pessoais em face do conhecimento pelo Estado ou por terceiros, independentemente da maior ou menor importância do conteúdo da comunicação".[7] Pretendeu os preceitos constitucionais evitar a interferência de terceiros no processo comunicativo estabelecido entre os interlocutores.

No sistema constitucional brasileiro, não há direitos ou garantias que se revistam de caráter absoluto, visto que razões de relevante interesse público ou exigências oriundas de outras liberdades públicas legitimam, ainda que excepcionalmente, por parte dos órgãos e entidades estatais, a adoção de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos da Constituição.

A Lei Maior permite que incidam sobre as liberdades públicas, em face do regime jurídico a que estão sujeitas, limitações de ordem jurídica, destinadas a assegurar a coexistência harmoniosa das liberdades. Assim, os direitos e garantias fundamentais são passíveis de limitação ou restrição.

Ao tratar da possibilidade de quebra judicial da inviolabilidade da privacidade, Ingo W. Sarlet ressalta que a restrição desse direito há de ocorrer no caso concreto a fim de resguardar outros direitos fundamentais:

---

7 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional.* 2 ed. São Paulo: Revista dos Tribunais, 2013, pp. 424-425.

> *Assim como os demais direitos pessoais, também o direito à privacidade não se revela ilimitado e imune a intervenções restritivas. Todavia, ao não prever, para a privacidade e intimidade, uma expressa reserva legal, além de afirmar que se cuida de direitos invioláveis, há que se reconhecer que a Constituição Federal atribuiu a tais direitos um elevado grau de proteção, de tal sorte que uma restrição apenas se justifica quando necessária a assegurar a proteção de outros direitos fundamentais ou bens constitucionais relevantes (no caso, portanto, de uma restrição implicitamente autorizada pela Constituição Federal), de modo que é em geral na esfera dos conflitos com outros direitos que se pode, em cada caso, avaliar a legitimidade constitucional da restrição.*[8]

Para André de Carvalho Ramos, a era digital agudiza a importância do direito à privacidade, bem como a necessidade de se ter a correta ponderação com os direitos tensionados, como, por exemplo, o direito difuso à segurança pública de toda a sociedade. Para o citado autor:

> *O desenvolvimento tecnológico das últimas décadas gerou uma mudança de paradigma na coleta, transmissão e armazenamento de informação tendendo a abranger, de modo mais ou menos sutil, todas as facetas da vida em sociedade. Esse imenso acervo de informação sobre um indivíduo já é utilizado maciçamente pelas empresas privadas dos mais diversos setores: desde gigantes da internet, empresas multinacionais de bens e serviços até o pequeno comerciante que contrata um serviço para oferta focada em potenciais clientes, cujos dados foram coletados por rede social de uso "gratuito". Do ponto de vista do indivíduo, é praticamente um truísmo reconhecer que suas interações armazenadas no mundo digital fornecem mais informações sobre sua pessoa que eventual violação do seu domicílio físico No plano da segurança pública e da persecução criminal, o Estado também utiliza*

8 SARLET, Ingo W.; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional*. 7 ed. São Paulo: Saraiva Educação, 2018, pp. 471-472.

> *essas informações para fins de promover (i) o direito à segurança; (ii) o direito à verdade e o (iii) direito à justiça.*[9]

Não menos certo, por outro lado, é que o afastamento do sigilo de dados não consubstancia autorização para que o poder público investigue arbitrariamente registros privados à procura de supostas ilegalidades, não se podendo operar de forma a conferir legitimidade de busca generalizada por parte do Estado. Nesse sentido, já decidiu o Supremo Tribunal Federal:

> *COMISSÃO PARLAMENTAR DE INQUÉRITO – QUEBRA DE SIGILO – AUSÊNCIA DE INDICAÇÃO CONCRETA DE CAUSA PROVÁVEL – NULIDADE DA DELIBERAÇÃO PARLAMENTAR – MANDADO DE SEGURANÇA CONCEDIDO. A QUEBRA DE SIGILO NÃO PODE SER UTILIZADA COMO INSTRUMENTO DE DEVASSA INDISCRIMINADA, SOB PENA DE OFENSA À GARANTIA CONSTITUCIONAL DA INTIMIDADE.*
> *– A quebra de sigilo, para legitimar-se em face do sistema jurídico-constitucional brasileiro, necessita apoiar-se em decisão revestida de fundamentação adequada, que encontre apoio concreto em suporte fático idôneo, sob pena de invalidade do ato estatal que a decreta. A ruptura da esfera de intimidade de qualquer pessoa – quando ausente a hipótese configuradora de causa provável – revela-se incompatível com o modelo consagrado na Constituição da República, pois a quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo Poder Público ou por seus agentes. Não fosse assim, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada, que daria ao Estado – não obstante a ausência de quaisquer indícios concretos – o poder de vasculhar registros sigilosos alheios, em ordem a viabilizar, mediante a ilícita utilização do procedimento de devassa*

9 CARVALHO RAMOS, André de. *Curso de direitos humanos.* 10ª ed., São Paulo: Saraiva, 2023, pp. 860-861.

> *indiscriminada (que nem mesmo o Judiciário pode ordenar), o acesso a dado supostamente impregnado de relevo jurídico-probatório, em função dos elementos informativos que viessem a ser eventualmente descobertos.*
> (MS 23.851/DF, Rel. Min. Celso de Mello, *DJ* de 21.6.2002.)

Em sede de agravo regimental no Inquérito 2.245/MG, entendeu a Corte que o pedido de quebra de sigilo deve conter identificação precisa e fundamentada quanto aos sujeitos cujas informações são requisitadas:

> *AGRAVO REGIMENTAL. INQUÉRITO. QUEBRA DE SIGILO BANCÁRIO. REMESSA DE LISTAGEM QUE IDENTIFIQUE TODAS AS PESSOAS QUE FIZERAM USO DA CONTA DE NÃO RESIDENTE TITULARIZADA PELA AGRAVANTE PARA FINS DE REMESSA DE VALORES AO EXTERIOR. LISTAGEM GENÉRICA: IMPOSSIBILIDADE. POSSIBILIDADE QUANTO ÀS PESSOAS DEVIDAMENTE IDENTIFICADAS NO INQUÉRITO. AGRAVO PROVIDO PARCIALMENTE.*
> *1. Requisição de remessa ao Supremo Tribunal Federal de lista pela qual se identifiquem todas as pessoas que fizeram uso da conta de não residente para fins de remessa de valores ao exterior: impossibilidade.*
> *2. Configura-se ilegítima a quebra de sigilo bancário de listagem genérica, com nomes de pessoas não relacionados diretamente com as investigações (art. 5º, inc. X, da Constituição da República).*
> *3. Ressalva da possibilidade de o Ministério Público Federal formular pedido específico, sobre pessoas identificadas, definindo e justificando com exatidão a sua pretensão.*
> *4. Agravo provido parcialmente.*
> (INQ 2.245-AgR/MG, Rel. Min. Cármen Lúcia, *DJe* de 9.11.2007.)

Ao explicitar o significado da expressão *"dados"* constante do art. 5º, XII, da CF, Tércio Sampaio Ferraz Júnior esclarece que *"o objeto protegido no*

direito a inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação".[10] Nas palavras do autor:

> *Em primeiro lugar, a expressão "dados" manifesta uma certa impropriedade (Celso Bastos & Ives Gandra, p. 73). Os citados autores reconhecem que por "dados" não se entende o objeto de comunicação, mas uma modalidade tecnológica de comunicação. Clara, nesse sentido, a observação de Manoel Gonçalves Ferreira Filho (p. 38): "Sigilo de dados. O direito anterior não fazia referência a essa hipótese. Ela veio a ser prevista, sem dúvida, em decorrência do desenvolvimento da informática. Os dados aqui são os dados informáticos (v. incs. XIV e LXXII)". A interpretação faz sentido.* ***O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade****. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas". Note-se, para a caracterização dos blocos, que a conjunção e une correspondência com telegrafia, segue-se uma vírgula e depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos.* ***Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefonia. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não estará havendo quebra de sigilo. Mas se alguém entra nesta transmissão, como um tercei-***

10 FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Disponível em: < http://www.revistas.usp.br/rfdusp/article/view/67231/69841 >. Acesso em: 12 nov. 2023.

> ***ro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados***." (grifos acrescidos)

Nessa linha, a jurisprudência da Suprema Corte havia se firmado no sentido de que a proteção garantida no art. 5º, XII, da Constituição Federal assegura inviolabilidade da comunicação de dados, mas não dos dados em si mesmos, ainda quando armazenados em computador:

> *(…) Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. 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/SC, Rel. Min. Sepúlveda Pertence, Plenário, *DJ* de 19.12.2006.)

Em linha convergente, assentara já a Segunda Turma do STF que a cláusula constitucional do art. 5º, XII, da Constituição não protege os registros telefônicos de aparelhos celulares apreendidos, não havendo de estender o sigilo das comunicações telefônicas ao depósito registral de ligações feitas (HC 91.867/PA, Rel. Min. Gilmar Mendes, Segunda Turma, *DJe* de 20.9.2012).

Contudo, em 2020, foi ressaltado pelo Min. Relator Gilmar Mendes que as novas circunstâncias fáticas e jurídicas relativas ao poder de armazenamento e o acesso à internet (evolução fática), bem como a proteção contemporânea aos dados pessoais (evolução jurídica) exigem que a proteção da intimidade (art. 5º, X) seja incrementada, em verdadeira mutação constitucional, no sentido de que seja indispensável (i) ordem judicial ou (ii) anuência do titular (STF, H.C 168.052/SP, Rel. Min. Gilmar Mendes, j. em sessão virtual de 9 a 19 de outubro de 2020).

Consta do voto do Min. Relator Gilmar Mendes tema vinculado à presente ação, que vem a ser justamente a necessidade de se evitar a existência de um "<u>Estado espião</u>":

> *Esses avanços tecnológicos são importantes e devem ser utilizados para a segurança pública dos cidadãos e a elucidação de delitos . Contudo, deve-se ter cautela, limites e controles para não transformar o Estado policial em um Estado espião e onipresente, conforme descrito por George Orwell em seu livro "1984".*[11]

Como visto, há inegáveis avanços da tecnologia móvel digital, sobretudo no que diz respeito aos aparelhos de telefonia celular. A grande maioria dos telefones móveis está, hoje, constantemente conectada à internet e dispõe de mecanismos de armazenamento de dados que, muitas vezes, acabam

11 STF, H.C 168.052/SP, Rel. Min. Gilmar Mendes, j. em sessão virtual de 9 a 19 de outubro de 2020

por revelar mais sobre a intimidade e a personalidade do proprietário do que a comunicação verbal.

O tema assume, portanto, inegável importância, estando submetido ao Supremo Tribunal Federal no ARE 1.042.075/RJ (Tema 977, Rel. Min. Dias Toffoli, pendente de julgamento), que aprecia o alcance da tutela do art. 5º, X e XII, da CF relativamente ao acesso, pela autoridade policial, sem autorização judicial, a registros e informações contidas em telefones celulares que se refiram à conduta delitiva e/ou permitam a identificação do agente do crime.

O voto proferido pelo Ministro Gilmar Mendes naquele processo bem retratou a profunda mudança das circunstâncias fáticas em torno dessa temática, em decorrência do desenvolvimento das mais novas tecnologias de comunicação e de tráfego de dados por *smartphones*, contexto que tem pautado a evolução normativa em tema de proteção da intimidade e da vida privada. Veja-se:

> *(…) a legislação infraconstitucional avançou para possibilitar a proteção dos dados armazenados em comunicações privadas, os quais só podem ser acessados mediante prévia decisão judicial – matéria submetida à reserva de jurisdição.*
> *Entendo que o avanço nesse importante tema da proteção do direito à intimidade e à vida privada deve ser considerado na interpretação do alcance das normas do art. 5º, X e XII, CF.*

> *Mais importante que a alteração do contexto jurídico,* ***a impactante transformação das circunstâncias fáticas joga novas luzes sobre o tema****. Nesse sentido, houve um incrível desenvolvimento dos mecanismos de comunicação e armazenamento de dados pessoais em smartphones e telefones celulares na última década.*
> *Nos dias atuais, esses aparelhos são capazes de registrar as mais variadas informações sobre os seus usuários, como a sua precisa localização por sistema GPS ou estações de rádio base, as chamadas realizadas e recebidas, os registros da agenda telefônica, os dados bancários dos usuários, informações armazenadas em nuvem, os* sites *e endereços eletrônicos acessados, lista de e-mail, mensagens por aplicativos de telefone, fotos e vídeos pessoais, entre outros.*
> *Além disso, a conexão de todos esses aparelhos à rede mundial de computadores faz com que estejamos todos integralmente conectados, o tempo todo, fornecendo dados e informações para órgãos públicos e privados. Conforme noticiado pelos meios de comunicação, os celulares são a principal forma de acesso dos brasileiros e cidadãos do país à* internet*. Esse motivo, por si só, já seria suficiente para concluir pela incidência das normas acima descritas no que toca à proteção dos dados, fluxos de dados e demais informações contidas nesses dispositivos.* – grifos no original.

No referido voto, destacou o Ministro Gilmar Mendes os impactos negativos provocados por ferramentas de intrusão virtual remota em aparelhos celulares à garantia da inviolabilidade da intimidade e da vida privada. Concluiu, então, pela necessidade de extrair nova exegese do art. 5º, X e XII, da CF, que vincule à prévia decisão judicial o acesso a dados e informações contidos em aparelhos celulares, exigindo-se a demonstração da necessidade, adequação e proporcionalidade do acesso, à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo dos dados e das comunicações:

(…) Há, nos dias atuais, a possibilidade de inserção de softwares espiões em aparelhos celulares (MENDES, Carlos Hélder. Tecnoinvestigação. *Entre a proteção de dados e a infiltração por software. JusPodivm, 2020; CAPRIOLI, Francesco. Il "captatore informatico" come strumento di ricerca della prova in Italia.* Revista Brasileira de Direito Processual Penal*, v. 3, n. 2, 2017).*

A partir do telefone, pode-se verificar se determinada pessoa esteve ou não em determinado local, qual percurso ela percorreu e que sites *acessou no caminho. Câmeras de reconhecimento facial integradas à internet possibilitam o reconhecimento instantâneo de suspeitos. Algorítimos podem ser usados para prever e evitar crimes (GUIMARÃES, Rodrigo C. A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal.* Revista Brasileira de Direito Processual Penal*, v. 5, n. 3, 2019; PEDRINA, Gustavo M. Consequências e perspectivas da aplicação de inteligência artificial a casos penais.* Revista Brasileira de Direito Processual Penal*, v. 5, n. 3, 2019).*

Esses avanços tecnológicos são importantes e devem ser utilizados para a segurança pública dos cidadãos e a elucidação de delitos *(SOARES, Gustavo T.* Investigação criminal e inovações técnicas e tecnológicas*. D' Plácido, 2016). Contudo,* ***deve-se ter cautela, limites e controles para não transformar o Estado policial em um Estado espião e onipresente****, conforme descrito por George Orwell em seu livro 1984.*

(…) ***entendo ser possível o acesso aos dados contidos em aparelhos celulares****, uma vez que não há uma norma absoluta de proibição da visualização do seu conteúdo, conforme se poderia extrair a partir de uma interpretação literal da norma contida no art. 5º, XII, da Constituição da República.*

Não obstante, a proteção à intimidade e à vida privada, contida no art. 5º, X, da CF/88, e a exigência da observância ao princípio da proporcionalidade nas intervenções estatais nesses direitos impõem a revisão de meu posicionamento anterior, para que ***o acesso seja condicionado à prévia decisão judicial****. (GLOECKNER, Ricardo J.; EILBERG, Daniela D. Busca e apreensão de dados em telefones celulares: novos*

> *desafios diante dos avanços tecnológicos.* Revista Brasileira de Ciências Criminais*, v. 27, n. 156, p. 353-393, jun. 2019).*

Em linha convergente com essa nova compreensão proposta para o art. 5º, X e XII, da Constituição, busca a presente ação o reconhecimento de uma omissão parcial do Congresso Nacional, no que se refere à edição de norma regulamentadora do uso, por órgãos e agentes públicos, de programas de intrusão virtual e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – *smartphones*, *tablets* e dispositivos eletrônicos similares – para dar efetividade aos mandamentos constitucionais de proteção estatal da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados.

Mais uma vez, reporta-se às informações coletadas no antes referido relatório do Gabinete do Alto Comissariado das Nações Unidas para Direitos Humanos, que expõe a potencialidade lesiva das ferramentas de espionagem remota atualmente existentes no mercado, cuja utilização tem se tornado cada vez mais comum por parte de órgãos governamentais no âmbito de investigações e de inteligência, à míngua de regulamentação mínima por parte do Estado:

> *6. O programa espião Pegasus é o exemplo mais proeminente em um cenário crescente de programas espiões comercializados por empresas para governos em todo o mundo. De acordo com pesquisadores, pelo menos 65 governos adquiriram ferramentas comerciais de vigilância*

de spyware. A NSO informou que conta com 60 agências governamentais em 45 países entre seus clientes. Poucos dias antes das revelações do Pegasus, o Citizen Lab e a Microsoft lançaram um relatório que detalhava como outro programa de computador, o Candiru, havia sido usado por governos para atingir defensores de direitos humanos, dissidentes, jornalistas, ativistas e políticos. Em novembro de 2021, a empresa de rede social Meta anunciou ter desativado sete entidades que tinham como alvo pessoas através da Internet em mais de 100 países. A empresa também alertou cerca de 50.000 pessoas que acreditava terem sido alvo de tais atividades. Relatou-se que mais de 500 empresas desenvolvem, comercializam e vendem essas ferramentas de vigilância para governos.

(…)

15. Reagindo às revelações sobre o uso do programa de computador Pegasus, várias instituições regionais e nacionais, incluindo o Conselho da Europa, a Comissão Interamericana de Direitos Humanos, o Parlamento Europeu e a Suprema Corte da Índia, expressaram preocupação com a proliferação de programas espiões e iniciaram audiências e investigações. Investigações criminais e ações civis também estão em andamento.

16. A orientação sobre os requisitos mínimos e as proteções necessárias para qualquer uso governamental de programas espiões pode se basear em um extenso corpo existente de análises de direitos humanos relacionadas à vigilância. Os impactos adversos de longo alcance do hackeamento exigem uma abordagem particularmente cautelosa de seu uso, limitando-o às circunstâncias mais excepcionais, em estrita observância aos requisitos do direito internacional dos direitos humanos.

17. No entanto, ***muitas jurisdições não estabeleceram essas proteções legais essenciais e não possuem leis claras, precisas e publicamente disponíveis que regulem as operações de hackeamento****. Enquanto alguns Estados promulgaram estruturas legais que cumpririam com a lei internacional de direitos humanos, outros* ***contam com leis excessivamente amplas ou desatualizadas, promulgadas antes do advento das tecnologias modernas****.*

18. Como as revelações sobre o programa de computador Pegasus e relatórios relacionados mostraram, hackeamento por vários atores estatais muitas vezes parecem perseguir objetivos que não são legítimos sob a lei internacional de direitos humanos. Embora, em certas circunstâncias, medidas de vigilância intrusivas possam ser permitidas de acordo com os artigos 17 e 19 do Pacto Internacional sobre Direitos Civis e Políticos com base na proteção da segurança nacional ou da ordem pública, o hackeamento nunca pode ser justificado por razões políticas ou comerciais, o que é frequentemente o caso quando os defensores dos direitos humanos ou jornalistas são tidos como alvos.
19. Mesmo que objetivos legítimos estejam sendo perseguidos, como objetivos de segurança nacional ou a proteção dos direitos de terceiros, ***a avaliação de necessidade e proporcionalidade do uso de programas espiões limita severamente os cenários em que programas espiões seriam permitidos****. Há fortes argumentos de que ferramentas como o Pegasus, que permitem* ***intromissões irrestritas na vida das pessoas e podem até mesmo atingir seus pensamentos íntimos, poderiam afetar a essência do direito à privacidade e interferir nos direitos absolutos à liberdade de pensamento e opinião****. Dados os impactos adversos substanciais do uso de programas espiões e seu alcance muito além de qualquer alvo pretendido, seu* ***uso deve ser limitado aos casos em que serviriam para prevenir ou investigar um crime grave específico ou ato que represente uma grave ameaça à segurança nacional****. Seu uso deve ser* ***estritamente direcionado a uma investigação da pessoa ou pessoas suspeitas de cometer ou ter cometido tais atos****. Este deve ser o último recurso, ou seja, todas as medidas menos intrusivas devem ter sido esgotadas ou ter se mostrado inúteis, e devem ser estritamente limitadas em escopo e duração. Somente dados relevantes devem ser acessados e coletados. As medidas também devem estar sujeitas a uma supervisão independente rigorosa; a aprovação prévia por um órgão judicial é essencial. Além disso, controles de exportação robustos e transparentes que considerem explicitamente os riscos de direitos humanos podem ser uma ferramenta*

> *poderosa para prevenir violações e abusos de direitos. O ACNUDH reitera seu recente apelo, bem como os de especialistas e grupos de direitos humanos, por uma moratória sobre a venda, transferência e uso de ferramentas de hackeamento até que um regime de salvaguardas baseado em direitos humanos esteja em vigência.*

Visando à apuração *in concreto* de responsabilidades – o que não é objeto desta ação direta de inconstitucionalidade por omissão (espécie do controle abstrato de constitucionalide) – há notícia de Inquérito Civil Público (ICP) em curso no qual se apuram negociações entre empresa de tecnologia estrangeira e órgão público brasileiro para possível aquisição de extensa gama de produtos e serviços capazes de invadir aparelhos telefônicos, rastrear pessoas, simular antenas de celulares, fazer pesquisas e coleta de dados na *deep web*, entre outras funcionalidades.[12]

Entre os softwares e ferramentas supostamente negociados, estariam o *Pegasus*, capaz de infectar aparelho celular e tomar seu controle sem o conhecimento ou, mesmo, nenhuma interação por parte do usuário, bastando, para a infecção do equipamento, que o operador da ferramenta saiba algum dado identificador relacionado ao alvo (número de telefone, e-mail, nome de usuário em rede social); a ferramenta *Pixcell*, que tem a capacidade de obter toda a comunicação do celular alvo, a partir da simulação de uma estação rádio base;

12 Confira-se: https://g1.globo.com/politica/blog/camila-bomfim/post/2023/11/01/mpf-passa-a-investigar-suspeita-de-segundo-sistema-ilegal-de-espionagem-da-abin.ghtml. Acesso: 12.11.2023.

o software *Hermes*, voltado à coleta de dados de pessoas de interesse, de forma indetectável, na rede aberta e na *deep web*; a ferramenta *Landmark*, que permite localizar qualquer pessoa em tempo real, bastando o fornecimento do número de acesso telefônico; o programa *Storm*, voltado à extração de dados mantidos em nuvens sem deixar rastros, entre outras ferramentas similares.

Não há dúvida de que tais instrumentos podem ser muito eficazes no combate à criminalidade e ao terrorismo no mundo contemporâneo, sobretudo se aplicados de forma legal e com a observância estrita dos ditames constitucionais, sendo a sua utilização precedida da necessária autorização judicial para a obtenção dos dados pessoais dos investigados, e submetida a diretrizes, condicionantes e procedimentos previstos no microssistema de proteção de dados, além de controle jurisdicional intenso.

O ponto central da controvérsia que a presente ação cinge-se ao uso secreto e abusivo desses softwares e ferramentas, sem autorização judicial, tampouco limites ou salvaguardas, de forma contrária à tutela do interesse público e aos deveres de proteção dos direitos fundamentais, que se impõem em um Estado de direito.

Compreende-se, por conseguinte, que a não regulamentação do uso de ferramentas digitais de monitoramento secreto e invasivo, e de programas

de intrusão virtual remota de aparelhos eletrônicos de comunicação pessoal – como é o caso do programa espião *Pegasus* citado no relatório da ONU –, para além de configurar omissão parcial em dar efetividade aos mandamentos contidos no art. 5º, X e XII, da Constituição Federal, ofende o princípio da proporcionalidade em sua acepção positiva, da qual deriva a vedação à proteção insuficiente a bens jurídicos constitucionalmente tutelados, a impor ao Estado e, no particular, ao Poder Legislativo, o dever de tutelar de maneira adequada e eficaz os direitos fundamentais.

Sobre tal princípio, discorreu o Ministro Roberto Barroso em voto no RE 878.694/MG, salientando que "*o Estado também viola a Constituição (…) quando não atua de modo adequado e satisfatório para proteger bens jurídicos relevantes*":

> *O princípio da proporcionalidade, tal como é hoje compreendido, não possui apenas uma dimensão negativa, relativa à vedação do excesso, que atua como limite às restrições de direitos fundamentais que se mostrem inadequadas, desnecessárias ou desproporcionais em sentido estrito. Ele abrange, ainda, uma dimensão positiva, referente à vedação à proteção estatal insuficiente de direitos e princípios constitucionalmente tutelados. A ideia nesse caso é a de que o Estado também viola a Constituição quando deixa de agir ou quando não atua de modo adequado e satisfatório para proteger bens jurídicos relevantes. Tal princípio tem sido aplicado pela jurisprudência desta Corte em diversas ocasiões para afastar a incidência de normas que impliquem a tutela deficiente de preceitos constitucionais.*
> (RE 878.694/MG, Rel. Min. Roberto Barroso, *DJe* de 6.2.2018.)

O Ministro Gilmar Mendes, com base na doutrina e jurisprudência constitucional alemãs, também tratou da proibição da proteção deficiente dos direitos fundamentais no julgamento do HC 102.087/MG, em que foi relator para o acórdão. Veja-se:

> *Assim, na dogmática alemã, é conhecida a diferenciação entre o princípio da proporcionalidade como proibição de excesso (*Übermassverbot*) e como proibição de proteção deficiente (*Untermassverbot*). No primeiro caso, o princípio da proporcionalidade funciona como parâmetro de aferição da constitucionalidade das intervenções nos direitos fundamentais como proibições de intervenção.* ***No segundo, a consideração dos direitos fundamentais como imperativos de tutela*** *(…)* ***imprime ao princípio da proporcionalidade uma estrutura diferenciada. O ato não será adequado caso não proteja o direito fundamental de maneira ótima****; não será necessário na hipótese de existirem medidas alternativas que favoreçam ainda mais a realização do direito fundamental; e violará o subprincípio da proporcionalidade em sentido estrito se o grau de satisfação do fim legislativo for inferior ao grau em que não se realiza o direito fundamental de proteção.*
> (HC 102.087/MG, Red. p/ acórdão Min. Gilmar Mendes, 2ª Turma, *DJe* 159, de 14.8.2012) – Grifo nosso.

No plano do Direito Internacional dos Direitos Humanos, André de Carvalho Ramos adverte que "*Por outro lado, a jurisprudência internacional dos direitos humanos aplica também o princípio da proibição deficiente (dimensão positiva*

da proporcionalidade), considerando que a ausência de proteção a direitos humanos ou mesmo sua deficiência representa um agir desproporcional por parte do Estado".[13]

Ao não estabelecer a disciplina regulamentadora da utilização, por órgãos e agentes públicos, de programas para intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – *smartphones*, *tablets* e dispositivos eletrônicos similares – o legislador nacional incide em omissão contrária à exigência imposta no art. 5º, X e XII, da CF, provocando **redução arbitrária e injustificada do nível de proteção das garantias fundamentais** previstas naquelas normas constitucionais, com ofensa ao princípio da proporcionalidade, derivado do postulado do devido processo legal (art. 5º, LIV, da CF), em sua dimensão substantiva.

Encontra-se, de todo modo, configurada a omissão inconstitucional do Congresso Nacional em tornar efetivos os mandamentos constitucionais de proteção estatal da inviolabilidade da intimidade, da vida privada e do sigilo das comunicações telefônicas e de dados, previstos respectivamente nos incisos X e XII do art. 5º da Constituição Federal.

No que concerne à fixação de prazo para adoção de providências necessárias à edição de lei, desde o julgamento da ADI 2.061/DF, entendia a

13 CARVALHO RAMOS, André de. *Teoria Geral dos Direitos Humanos na Ordem Internacional.* São Paulo: Saraivajur, 2019, p. 248.

Corte que os 30 dias previstos no art. 103, § 2º, da Constituição somente se aplicavam a atribuições administrativas do Chefe do Executivo:

> *AÇÃO DIRETA DE INCONSTITUCIONALIDADE POR OMISSÃO. ART. 37, X, DA CONSTITUIÇÃO FEDERAL (REDAÇÃO DA EC Nº 19, DE 4 DE JUNHO DE 1998).*
> *Norma constitucional que impõe ao Presidente da República o dever de desencadear o processo de elaboração da lei anual de revisão geral da remuneração dos servidores da União, prevista no dispositivo constitucional em destaque, na qualidade de titular exclusivo da competência para iniciativa da espécie, na forma prevista no art. 61, § 1º, II, a, da CF. Mora que, no caso, se tem por verificada, quanto à observância do preceito constitucional, desde junho/1999, quando transcorridos os primeiros doze meses da data da edição da referida EC nº 19/98. Não se compreende, a providência, nas atribuições de natureza administrativa do Chefe do Poder Executivo, não havendo cogitar, por isso, da aplicação, no caso, da norma do art. 103, § 2º,* in fine, *que prevê a fixação de prazo para o mister. Procedência parcial da ação.*
> (ADI 2.061/DF, Rel. Min. Ilmar Galvão, *DJ* de 29.6.2001)

Ocorre, por outro lado, que "*a Constituição não pode se submeter à vontade dos Poderes constituídos nem ao império dos fatos e das circunstâncias. A supremacia de que ela se reveste – enquanto for respeitada – constituirá a garantia mais efetiva de que os direitos e liberdades não serão jamais ofendidos*" (ADI-MC 293/DF, Rel. Min. Celso de Mello, *DJ* de 16.4.1993).

Com base nessa compreensão, a jurisprudência posterior do STF tem flexibilizado o entendimento de que a decisão em ADO deva se limitar a

constatar a inconstitucionalidade da omissão, passando a admitir fixação de prazo para providências necessárias ao cumprimento dos deveres impostos pela norma mais importante do país, a Constituição Federal. Nesse sentido, colhe-se trecho da ementa da mencionada ADI 3.682/MT:

> *(…) A omissão legislativa em relação à regulamentação do art. 18, § 4º, da Constituição, acabou dando ensejo à conformação e à consolidação de estados de inconstitucionalidade que não podem ser ignorados pelo legislador na elaboração da lei complementar federal.*
> *4. Ação julgada procedente para declarar o estado de mora em que se encontra o Congresso Nacional, a fim de que, **em prazo razoável de 18 (dezoito) meses**, adote ele todas as providências legislativas necessárias ao cumprimento do dever constitucional imposto pelo art. 18, § 4º, da Constituição, devendo ser contempladas as situações imperfeitas decorrentes do estado de inconstitucionalidade gerado pela omissão. Não se trata de impor um prazo para a atuação legislativa do Congresso Nacional, mas apenas da fixação de um **parâmetro temporal razoável**, tendo em vista o prazo de 24 meses determinado pelo Tribunal nas ADI nºs 2.240, 3.316, 3.489 e 3.689 para que as leis estaduais que criam municípios ou alteram seus limites territoriais continuem vigendo, até que a lei complementar federal seja promulgada contemplando as realidades desses municípios.* (Grifos nossos.)

Dada a obrigatoriedade imposta ao Estado de dar proteção eficiente e adequada aos bens jurídicos tutelados pelo art. 5º, X e XII, da CF, e tendo em vista a omissão inconstitucional demonstrada nesta ação, é cabível estabelecer prazo razoável ao Congresso Nacional para que delibere e conclua o processo legislativo, aprovando a norma disciplinadora da utilização, por órgãos e

agentes públicos, de programas de intrusão virtual remota e ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – *smartphones*, *tablets* e dispositivos eletrônicos similares – a fim de dar efetividade aos mandamentos constitucionais referidos.

Referido prazo não se confunde com o do art. 103, § 2º, da Lei Maior e do art. 12-H, § 1º, da Lei 9.868/1999, mas respeita as garantias constitucionais mencionadas.

Por outro lado, tendo em vista o risco potencial de lesão ampla e indiscriminada a direitos fundamentais, até que se veja efetivamente suprida a omissão legislativa inconstitucional ora apontada, com a promulgação de lei nacional disciplinadora do uso das aludidas ferramentas de monitoramento e de intrusão remota em aparelhos de comunicação, é recomendável a adoção de solução normativa provisória por essa Suprema Corte.

Sabe-se que, em princípio, não cabe ao Supremo Tribunal Federal, que não tem função de legislador positivo, definir qual a resposta normativa a se aplicar ao caso, com vistas a sanar a omissão inconstitucional.

Contudo, na via do mandado de injunção, por meio do qual também se impugna lacuna legislativa, a jurisprudência da Suprema Corte desenvolveu-

se no sentido de admitir a possibilidade de estabelecer solução normativa provisória às omissões legislativas levadas ao seu conhecimento.

No julgamento do paradigmático MI 708/DF, o Relator Ministro Gilmar Mendes evidencia essa evolução em seu voto (*DJe* 206, de 30.10.2008):

> *(…) As decisões proferidas nos Mandados de Injunção nºs 283 (Relator: Sepúlveda Pertence), 232 (Relator: Moreira Alves) e 284 (Relator: Celso de Mello) sinalizam uma nova compreensão do instituto e a admissão de uma solução "normativa" para a decisão judicial.*
> *Assim, no caso relativo à omissão legislativa quanto aos critérios de indenização devida aos anistiados (art. 8º do ADCT), o Tribunal entendeu que, em face da omissão, os eventuais afetados poderiam dirigir-se diretamente ao juiz competente que haveria de fixar o montante na forma do direito comum (Cf., nesse sentido, MI nº 562-DF, Rel. Min. Ellen Gracie, DJ 20.6.2003; e MI nº 543-DF, Rel. Min. Octavio Galloti, DJ 24.5.2002). Em outro precedente relevante, considerou-se que a falta de lei não impedia que a entidade beneficente gozasse da imunidade constitucional expressamente reconhecida (Cf. MI nº 679, Rel. Min. Celso de Mello, DJ 17.12.2002).*
> *As decisões referidas indicam que o Supremo Tribunal Federal aceitou a possibilidade de uma regulação provisória pelo próprio Judiciário, uma espécie de sentença aditiva, se se utilizar a denominação do direito italiano.*

Naquele caso específico, decidiu-se pela aplicação aos servidores públicos da Lei 7.783, de 28.6.1989, que dispõe sobre o exercício do direito de greve na iniciativa privada. A Corte, inclusive, conferiu efeito *erga omnes* à decisão normativa.

A mesma saída foi utilizada em julgamento posterior, no qual se discutiu a mora legislativa na regulamentação do direito social ao aviso prévio dos trabalhadores, previsto no inciso XXI do art. 7º da Constituição:

> *Mandado de injunção.*
> *2. Aviso prévio proporcional ao tempo de serviço. Art. 7º, XXI, da Constituição Federal.*
> *3. Ausência de regulamentação.*
> *4. Ação julgada procedente.*
> *5. Indicação de adiamento com vistas a consolidar proposta conciliatória de concretização do direito ao aviso prévio proporcional.*
> *6. Retomado o julgamento.*
> *7. Advento da Lei 12.506/2011, que regulamentou o direito ao aviso prévio proporcional.*
> *8. Aplicação judicial de parâmetros idênticos aos da referida legislação.*
> *9. Autorização para que os ministros apliquem monocraticamente esse entendimento aos mandados de injunção pendentes de julgamento, desde que impetrados antes do advento da lei regulamentadora.*
> *10. Mandado de injunção julgado procedente.*
> (MI 943/DF, Rel. Min. Gilmar Mendes, *DJe* 81, 2.5.2013.)

Nessa mesma direção, admitiu o Supremo Tribunal Federal ser possível a adoção de solução normativa definida judicialmente em sede de jurisdição constitucional (ADO 25/DF, Rel. Min. Gilmar Mendes, *DJe* de 18.8.2017).

Diante do grave quadro exposto, afigura-se recomendável buscar, na legislação nacional atualmente vigente, uma moldura normativa a ser, em caráter provisório, aplicada à utilização, por parte de órgãos e agentes públicos,

de programas de intrusão virtual remota e ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – *smartphones*, *tablets* e dispositivos eletrônicos similares – com o escopo de dar efetividade aos mandamentos constitucionais de proteção estatal da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados, estatuídos no art. 5º, X e XII, da Constituição Federal, até que o Congresso Nacional supra a mora inconstitucional apontada.

Deve-se impor um mínimo de salvaguardas a respeito de quem está promovendo a investigação e da legalidade desta, o que passa pelo registro, por exemplo, da autorização judicial do uso da ferramenta, do nome da autoridade pública que ingressa no sistema, da data e hora do acesso, para citar algumas das formalidades imprescindíveis ao controle da atividade que tem o potencial de lesar gravemente a privacidade dos cidadãos.

Trata-se de exigências formais de controle básico que se espera para a instauração e tramitação de qualquer procedimento estatal que possibilite acessar informações protegidas por sigilo, ou a partir do qual se possam obter dados passíveis de levar os indivíduos e pessoas jurídicas a sofrerem sanções pela prática de atos ilícitos (sejam efeitos na esfera criminal, cível, eleitoral ou administrativa).

Sem tais controles, sem o registro de quem acessa os dados, do fim para o qual acessa e da autorização judicial respectiva, permite-se a condução de procedimentos estatais secretos, completamente à margem do Estado de direito e sem qualquer limite, legitimando-se a espionagem e a investigação secreta por agentes não identificados e/ou incompetentes, sem possibilidade de responsabilização posterior dos usuários e investigadores por eventuais abusos ou excessos de poder (portanto sem responsividade ou *accountability*).

Assim, a imposição de limites, balizas e controles para a utilização das citadas ferramentas é fundamental, haja vista que, diferentemente de interceptações telefônicas ou telemáticas, onde a concessionária de telefonia e o provedor de e-mails intervêm no fornecimento dos dados, mediante a apresentação de ordem judicial, nos instrumentos de espionagem intrusiva remota os órgãos estatais possuem controle absoluto do momento em que os dados serão invadidos, prescindindo de terceiros.

Ao disciplinar a interceptação de comunicações telefônicas, estatui a Lei 9.296/1996 que a medida dependerá de autorização judicial (art. 1º, *caput*), estendendo as suas diretrizes à interceptação do fluxo de informações em sistemas informáticos e telemáticos (art. 1º, parágrafo único).

Adiante, os arts. 2º e 3º do diploma federal estabelece exigências mínimas que também podem nortear o balizamento provisório a ser fixado pela Corte para remediar a omissão normativa questionada nesta ação direta, concernente à utilização das ferramentas de invasão remota:

> *Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:*
> *I – não houver indícios razoáveis da autoria ou participação em infração penal;*
> *II – a prova puder ser feita por outros meios disponíveis;*
> *III – o fato investigado constituir infração penal punida, no máximo, com pena de detenção.*
> *Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.*
> *Art. 3° A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:*
> *I – da autoridade policial, na investigação criminal;*
> *II – do representante do Ministério Público, na investigação criminal e na instrução processual penal.*

O art. 8º-A da Lei 9.296/1996, inserido pela Lei 13.964/2019, regula a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, com aplicação subsidiária das regras da interceptação telefônica e telemática. Na regulação específica, exige-se a descrição circunstanciada do local e da forma de instalação do dispositivo de captação ambiental, com demonstração de que a prova ou informação que se pretende obter não pode ser produzida por

outros meios de prova, não podendo a captação durar mais de 15 (quinze) dias, renovável mediante novo controle judicial:

> *Art. 8º-A. Para investigação ou instrução criminal, poderá ser autorizada pelo juiz, a requerimento da autoridade policial ou do Ministério Público, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, quando: (Incluído pela Lei nº 13.964, de 2019)*
> *I – a prova não puder ser feita por outros meios disponíveis e igualmente eficazes; e (Incluído pela Lei nº 13.964, de 2019)*
> *II – houver elementos probatórios razoáveis de autoria e participação em infrações criminais cujas penas máximas sejam superiores a 4 (quatro) anos ou em infrações penais conexas. (Incluído pela Lei nº 13.964, de 2019)*
> *§ 1º O requerimento deverá descrever circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental. (Incluído pela Lei nº 13.964, de 2019)*
> *§ 2º A instalação do dispositivo de captação ambiental poderá ser realizada, quando necessária, por meio de operação policial disfarçada ou no período noturno, exceto na casa, nos termos do inciso XI do caput do art. 5º da Constituição Federal. (Incluído pela Lei nº 13.964, de 2019) (Vigência)*
> *§ 3º A captação ambiental não poderá exceder o prazo de 15 (quinze) dias, renovável por decisão judicial por iguais períodos, se comprovada a indispensabilidade do meio de prova e quando presente atividade criminal permanente, habitual ou continuada. (Incluído pela Lei nº 13.964, de 2019)*
> *§ 4º A captação ambiental feita por um dos interlocutores sem o prévio conhecimento da autoridade policial ou do Ministério Público poderá ser utilizada, em matéria de defesa, quando demonstrada a integridade da gravação. (Incluído pela Lei nº 13.964, de 2019) (Vigência)*
> *§ 5º Aplicam-se subsidiariamente à captação ambiental as regras previstas na legislação específica para a interceptação telefônica e telemática. (Incluído pela Lei nº 13.964, de 2019)*

A legislação em exame também disciplina o descarte de provas, em parâmetros que devem ser estendidos a quaisquer atividades estatais de natureza investigativa, de inteligência, fiscalizatória ou de controle. Com efeito, mesmo nos casos em que a medida invasiva puder ser utilizada licitamente, a interceptação ou captação de dados pode obter informações de terceiros, ou mesmo dos próprios alvos ou investigados, mas que não tragam nenhum benefício às investigações e sequer sejam úteis às atividades de inteligência, fiscalização e controle, tais como dados pessoais, fotos íntimas, informações médicas e profissionais irrelevantes para as autoridades estatais, cuja revelação possa gerar danos materiais e morais a pessoas naturais e jurídicas. Nesses casos, preservam-se apenas parcialmente as informações obtidas com as ferramentas investigativas, descartando-se o que é inútil e desnecessário, sempre com supervisão dos órgãos de controle:

> *Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.*
> *Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.*

Também pode-se extrair balizas relevantes a partir do MCI. No ponto, os arts. 22 e 23 da Lei 12.965/2014 estabelecem requisitos mínimos para

a requisição judicial de afastamento do sigilo dos registros de conexão ou de acesso a aplicações de internet, são eles: (**i**) demonstração dos indícios fundados da ocorrência do ilícito, (**ii**) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou de instrução probatória e (**iii**) delimitação do período ao qual se referem os registros, cabendo ao juiz adotar "*providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro*":

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

Nos termos do MCI, pode a autoridade investigante, com o escopo de formar conjunto probatório em processos criminais, requerer o acesso aos

dados telemáticos, devendo demonstrar, para tanto, a existência de fundados indícios da ocorrência do crime, justificando de forma motivada a utilidade dos registros solicitados, com delimitação, ao máximo, do respectivo período ao qual se referem.

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

> *Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
> *§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.*
> *§ 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.*
> *§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.*

> *§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.*

O tipo de informação a ser disponibilizada direciona à autoridade requisitante um ônus agravado de fundamentação, o qual está implícito no referido art. 10 e decorre também da leitura sistemática do microssistema protetivo de dados e comunicações e de seus princípios reitores, dentro de um contexto em que envolvidos os direitos fundamentais e a preferência por meios investigativos que gerem menos riscos a terceiros não envolvidos no ilícito.

Disso decorre que todo tratamento de dados há de ser regido pelos preceitos da adequação e da necessidade, o que significa ser compatível com as finalidades informadas ao titular e se limitar ao mínimo necessário para alcançá-las, abrangendo os dados pertinentes, proporcionais e não excessivos (art. 6º, II e III, da LGPD).

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

Em consequência, **cumpre à autoridade requerente se desincumbir de uma obrigação de fundamentação agravada**, a fim de circunscrever a medida aos casos em que há efetiva necessidade e adequação, de modo a prevenir danos a terceiros e preservar sua segurança, sem que isso obste o cumprimento dos deveres constitucional e convencional de investigar e punir.

É imprescindível, no ponto, que se estabeleça um controle acerca de quais agentes públicos usam as ferramentas, com registro do dia e hora de acesso (controle de "*log*"), e de quais agentes consultam e analisam o resultado das diligências (informações, dados e comunicações protegidas por sigilo). Ainda, que se estabeleçam regras claras sobre o descarte de informações e dados irrelevantes de investigados e de terceiros, que não tenham utilidade para a investigação que fundamentou o uso da ferramenta; e rotinas de fiscalização consolidadas, por parte de órgãos legitimados, para prevenir e detectar eventuais abusos na utilização dos softwares.

Assim, de forma complementar às normas de proteção expostas, também as normas de organização e de procedimento se associam como mecanismos de salvaguarda do direito à intimidade e à vida privada. Essas obrigações específicas se conjugam a outros deveres e obrigações gerais incidentes sobre a atuação do Estado, previstos nas diversas áreas do ordenamento jurídico, para proporcionar o conjunto de salvaguardas necessárias à proteção dos direitos fundamentais.

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

Nesse sentido, o art. 23 do MCI prevê caber ao juiz, ao decidir o pedido, tomar providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo atribuir segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

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

Para além, no microssistema protetivo dos dados e comunicações, há igualmente as previsões da LGPD atinentes aos princípios da segurança, da prevenção, da responsabilização e da prestação de contas (Lei 13.709/2018, art. 6º, VII, VIII e X).

Apesar da inaplicabilidade da LGPD às atividades de investigação e repressão de infrações penais (art. 4º, III, *d*), sua principiologia é referência

para a contextualização das garantias envolvidas no manejo de dados. Nesse sentido, o tratamento de dados pela autoridade pública há de atender a finalidade que as justifica, na busca do interesse público (art. 23), havendo, ainda, de garantir a inocorrência de danos em virtude desse tratamento (art. 6º, VII, VIII e X).

O Supremo Tribunal Federal já afirmou a constitucionalidade do compartilhamento de dados sigilosos com órgãos de controle e fiscalização, para tutelar o interesse público. Nessa hipótese, consoante decidiu, exsurgem obrigações associadas aos atores envolvidos, decorrentes dos fins específicos para os quais for autorizado o afastamento do sigilo.[14] Como explicitado em tese fixada na ocasião, o compartilhamento dos dados se faz conjugado a uma série de obrigações associadas específicas – a formalidade das comunicações, com garantia do sigilo, a certificação do destinatário e o estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.[15]

---

14 O fornecimento dos dados em questão difere-se de uma quebra de sigilo, consistindo, na verdade, em transferência temporária de informações, com deveres de guarda pelos órgãos envolvidos. Nesse sentido, ao apreciar o Tema 990 de repercussão geral, o STF, afirmou a constitucionalidade do compartilhamento de dados bancários e fiscais dos contribuintes com órgãos de investigação criminal, tendo presentes os postulados constitucionais da intimidade e do sigilo de dados, assinalando a possibilidade de se relativizar os sigilos, desde que de forma proporcional e razoável, e com a finalidade de defesa da probidade e do combate à corrupção, bem como de outros valores constitucionais caros à sociedade brasileira (RE 1.055.941/SP, Rel. Min. Dias Toffoli, *DJe* de 4.12.2019).

15 Foram fixadas as seguintes teses: *"1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil – em que se define o lançamento do tributo – com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informa-*

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

Por outro lado, houve nos últimos anos o desenvolvimento de técnicas de criptografia avançadas, como a criptografia de ponta a ponta, garantindo a segurança na troca de dados entre duas partes sem interferências externas. No entanto, essa tecnologia também possibilitou que organizações criminosas (inclusive terroristas) utilizassem aplicativos de mensagens, como Signal, Wickr, Confide, Telegram e Whatsapp, para comunicações discretas e livres de vigilância governamental. Esse cenário facilitou a prática de diversos crimes.

Por sua vez, as ferramentas tradicionais de investigação disponíveis para o estado brasileiro mostram-se ineficientes para interceptar comunicações realizadas por esses aplicativos. Atualmente, a estratégia mais viável é a apreensão e análise posterior de dispositivos, que, embora útil,

---

ções em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; 2. O compartilhamento pela UIF e pela RFB referido no item anterior deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios."

não recupera o conteúdo de ligações ou mensagens autodestrutivas – uma funcionalidade cada vez mais comum.

Essa limitação resulta em mais uma proteção deficiente dos direitos garantidos pela Constituição Federal (conforme doutrina nacional vista acima), já que as autoridades de persecução penal carecem de meios eficazes para investigar crimes complexos cometidos por organizações criminosas.

Internacionalmente, já existem soluções comerciais capazes de superar as barreiras da criptografia de ponta a ponta, facilitando a interceptação de dados pelas autoridades. Contudo, **a ausência de normas claras sobre o uso e controle dessas tecnologias** gera insegurança jurídica para sua utilização, pois seu uso poderia – *ad terrorem* – levar à responsabilização funcional dos agentes públicos.

Desse panorama, entende-se que, ao menos, existirem diretrizes e condicionantes relevantes na legislação brasileira de proteção de dados pessoais a serem observadas, incumbindo a esta Suprema Corte consolidar e explicitar, nesta ação direta, as balizas sistêmicas que afastem arbitrariedades no uso, por órgãos e agentes públicos em atividades de inteligência ou investigação criminal, de programas de intrusão virtual remota e/ou de

ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal, como *smartphones*, *tablets* e dispositivos eletrônicos similares.

Assim, a partir das disposições do quadro legislativo até aqui exposto, pode-se extrair algumas balizas e condicionamentos a serem fixados pela Corte, em caráter provisório aos órgãos e agentes públicos usuários dos referidos instrumentos investigativos e desde que obtida autorização judicial. Por isso, requer-se liminarmente :

(**i**) **que seja ordenado** às Forças Armadas, agentes públicos de inteligência, forças policiais civis e militares de todas as esferas (no plano federal e estadual), **órgãos de inteligência e/ou investigação criminal** que se abstenham de utilizar qualquer das ferramentas tecnológicas de invasão e monitoramento de que trata esta ação direta, sem autorização judicial e sem as balizas abaixo mencionadas a título exemplificativo;

(ii) que sejam fixadas as seguintes balizas (além da autorização judicial) para a utilização das ferramentas tecnológicas de invasão e monitoramento de que trata esta ação direta:

(i**i.1**) que seja elaborado um termo de responsabilidade pelo órgão, cujas condições devem ser aceitas para liberação do acesso à ferramenta;

(**ii.2**) que seja o termo de responsabilidade submetido aos usuários, por coleta de assinatura digital ou escrita, previa ou concomitantemente ao cadastramento, exigindo-se a aceitação expressa em caixa de diálogo específica, para prosseguimento do uso do software;

(i**i.3**) que seja condicionado o uso da ferramenta à indicação do número de inquérito policial, de procedimento investigativo ou de processo judicial no curso do qual os dados estejam sendo solicitados ou requisitados, a entidade, órgão ou instituição responsável, bem assim que se faça *upload* da decisão judicial que autorizou a quebra de sigilo de dados;

(i**i.4**) que haja certificação de que qualquer transferência, remessa ou compartilhamento de dados respeite as regras de sigilo existentes, exigindo-se das autoridades que recebam o material compartilhado que assinem o termo de responsabilidade e se comprometam a manter o sigilo;

(i**i.5**) que seja determinado que qualquer cooperação ou assistência técnica e científica, em atividade de natureza policial, de inteligência, controle ou fiscalização, que seja eventualmente prestada aos Estados, Distrito Federal e Municípios, respeite as regras de sigilo existentes, exigindo-se das autoridades que se beneficiem das ferramentas que assinem o termo de responsabilidade e se comprometam a manter o sigilo;

(i**i.6**) que seja exigido, ao final de cada operação ou diligência, redação de relatório circunstanciado da utilização da ferramenta, que deverá ser armazenado por prazo não inferior a 30 anos, podendo ser mantido em sigilo do público em geral, mas não dos órgãos de controle;

(i**ii.7**) que seja desenvolvido e se disponibilize treinamento específico para seus investigadores, analistas, policiais e quaisquer outros agentes públicos que tenham que operar tais ferramentas, a fim de que o uso seja adequado à proteção dos direitos fundamentais dos alvos, investigados e de terceiros;

(i**ii.8**) que se desenvolva os sistemas eletrônicos respectivos para que sejam dotados de campos indicativos do êxito de tais ferramentas para a respectiva atividade de inteligência, controle,

fiscalização ou investigação, a fim de que haja permanente aperfeiçoamento do seu uso, possibilitando reavaliar a necessidade de prorrogar as respectivas licenças pela constatação da eficácia ou inefetividade da ferramenta na prática;

(**iv**) para utilização de ferramentas tecnológicas que consistem em *softwares* de acesso a dispositivos eletrônicos para interceptação, captação, coleta, visualização ou qualquer outra forma de acesso a dados, informações e comunicações de investigados, alvos ou pessoas em geral, contidas em aparelhos digitais de comunicação pessoal, *smartphones*, *tablets* e dispositivos eletrônicos similares:

(**iv.1**) exija das autoridades de investigação, fiscalização, controle e inteligência que obtenham, previamente à utilização da ferramenta, autorização judicial específica, da qual deve constar a identificação dos alvos investigados e demonstração do seu envolvimento em ilícitos sob investigação, descritos com clareza e precisão, ou indicação da utilidade e finalidade dos dados ou informações que se pretende obter, bem assim o período ou intervalo de tempo em que a autoridade poderá utilizar a ferramenta;

(**iv.2**) implemente mecanismo que restrinja o acesso às ferramentas investigativas a pessoas previamente cadastradas, com controle de "*log*"

e entrada condicionada à inserção de chave de "*login*" e senha, ou, alternativamente, ao uso de certificado digital (*token*) para identificação do usuário;

(**iv.3**) estabeleça sistema de registro inalterável, com identificação do usuário e senha, data e hora de acesso ao sistema, devendo tais registros ser armazenados por no mínimo 30 anos e submetidos aos órgãos de controle da atividade dos usuários ou investigadores mediante solicitação ou requisição;

(**v)** para a utilização de ferramentas tecnológicas invasivas do tipo *cell-site simulator* ("*CSS*") ou "*IMSI catcher*" (onde a sigla IMSI corresponde a "*international mobile subscriber identity*") – caso do PIXCELL – que simulam antenas de telefonia celular:r

(v.**1**) exija das autoridades de investigação, fiscalização, controle e inteligência que obtenham, previamente à utilização da ferramenta, autorização judicial específica, da qual deve constar identificação dos alvos investigados, com comprovação do seu envolvimento em ilícitos sob investigação, ou a indicação da utilidade e finalidade dos dados ou informações que se pretende obter, bem assim o

período ou intervalo de tempo e o perímetro em que a autoridade poderá instalar e utilizar a ferramenta;

(**v.2**) determine que as ferramentas sejam utilizadas apenas para identificar, localizar ou rastrear telefones celulares ou outros aparelhos de comunicação dos investigados, sem outorgar o acesso às comunicações privadas de terceiros, não relacionados com os sujeitos da investigação;

(**v.3**) que não sejam gravadas ou armazenadas conversas privadas de terceiros, cujos celulares ou dispositivos de comunicação estejam localizados nas proximidades da ferramenta de captação de dados, devendo haver o descarte imediato dos dados e comunicações respectivos, com a ressalva tão só daqueles relacionados aos alvos e investigados, que hão de ser armazenados para uso investigativo, de inteligência ou judicial.

Em síntese, em face de grave omissão inconstitucional e dos prejuízos que vem sendo provocados a direitos e garantias de especial importância para a ordem constitucional, requer-se que, até a aprovação pelo Congresso Nacional de norma legal específica quanto à referida temática, seja a lacuna normativa afastada pela indispensável autorização judicial prévia (*ex ante) e* aplicação do balizamento ora proposto, bem como de outras diretrizes a serem definidas pelo E. Tribunal, mediante a aplicação, no que couber, das

aludidas disposições da Lei de Interceptação de Comunicações Telefônicas (Lei 9.296/1996), do MCI (Lei 12.965/2014) e da LGPD (Lei 13.709/2018).

Nessa linha, torna-se essencial que o Congresso Nacional elabore normas primordialmente para **regular o uso e controle das três principais ferramentas disponíveis no mercado**: 1) *spywares*, como o Pegasus do NSO Group, que intercepta dados ao infectar um dos dispositivos envolvidos na comunicação; 2) *Imsi Catchers*, como o Pixcell (NSO Group) e o GI2 (Cognyte/Verint), que simulam estações rádio-base capturando dispositivos próximos; 3) dispositivos que **rastreiam a localização** de um alvo específico através da rede celular, como o First Mile (Cognyte/Verint) e o Landmark (NSO Group).

Por esse motivo, incumbe a essa Corte Suprema declarar a omissão parcial do Congresso Nacional em editar normatização que regulamente o uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e/ou de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – *smartphones*, *tablets* e dispositivos eletrônicos similares – fixando prazo razoável para que seja dada plena efetividade aos mandamentos contidos no art. 5º, X e XII, da CF, com definição das referidas balizas provisórias à salvaguarda dos direitos fundamentais à intimidade, à vida privada e ao sigilo das comunicações, até que seja suprida a mora legislativa inconstitucional.

III. PEDIDO CAUTELAR

Estão presentes os pressupostos para a concessão de medida cautelar. A plausibilidade jurídica do pedido (*fumus boni juris*) está suficientemente demonstrada pelos argumentos deduzidos nesta petição inicial, que encontram amparo na jurisprudência do Supremo Tribunal Federal.

Perigo na demora processual (*periculum in mora*) decorre de que a omissão legislativa atacada fragiliza o regime constitucional de proteção da intimidade, da vida privada e da inviolabilidade do sigilo das comunicações pessoais, com prejuízos contínuos e potenciais a direitos fundamentais de um número expressivo de cidadãos.

É necessária, portanto, a concessão de medida cautelar para o fim de determinar a aplicação **provisória da fixação indispensável autorização judicial prévia à utilização, por quaisquer órgão públicos (inclusive nas chamadas ações de inteligência das Forças Armadas e das forças policiais de qualquer esfera), bem como dos parâmetros e balizas fixados pelo Supremo Tribunal Federal**, até que o legislador estabeleça norma reguladora do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – *smartphones*, *tablets* e dispositivos eletrônicos similares.

Cabe reportar, aqui, aos axiomas da segurança e da prevenção, que orientam (*i*) o uso das medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; e (*ii*) a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VII e VIII, da LGPD).

Por conseguinte, além de sinal de bom direito, há premência em que essa Corte conceda a medida cautelar, para os fins expostos acima.

IV. PEDIDOS E REQUERIMENTOS

Em face do exposto, requer a PROCURADORA-GERAL DA REPÚBLICA que o Supremo Tribunal conceda medida cautelar para os fins expostos acima e nos termos do art. 12-F da Lei 9.868/1999.

Em seguida, pleiteia que se colham informações do Congresso Nacional e que se ouça a Advocacia-Geral da União, nos termos do art. 12-E, § 2º, da Lei 9.868/1999. Superadas essas fases, pede prazo para a manifestação da Procuradoria-Geral da República.

Ao final, postula que seja julgado procedente o pedido, para (*i*) declarar a inconstitucionalidade da omissão parcial do Congresso Nacional em tornar plenamente efetivos os mandamentos de proteção da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados, estatuídos no art. 5º, X e XII, da CF, por meio da regulamentação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – *smartphones*, *tablets* e dispositivos eletrônicos similares; (*ii*) fixar prazo razoável para que o Congresso Nacional supra a mora legislativa; e (*iii*) estabelecer balizas provisórias à salvaguarda dos direitos fundamentais à intimidade e à privacidade, e à inviolabilidade do sigilo das comunicações pessoais e de dados, até que seja sanada a lacuna normativa inconstitucional.

Brasília, data da assinatura digital.

Elizeta Maria de Paiva Ramos
Procuradora-Geral da República
Assinado digitalmente

AMO