EXCELENTÍSSIMO SENHOR MINISTRO

RECURSO EXTRAORDINÁRIO COM AGRAVO Nº. 1.042.075

O **Instituto Brasileiro de Ciências Criminais** (**IBCCrim**) vem, por meio de seus procuradores signatários, apresentar os presentes memoriais com o propósito de auxiliar na formação do convencimento dessa Corte em face da retomada do julgamento, com a inclusão do feito para a pauta do dia 13/12/2023.

I. A QUESTÃO EM DISCUSSÃO

Trata-se de crime cuja autoria foi verificada a partir do acesso da autoridade policial, sem determinação judicial, aos dados armazenados no aparelho celular do então investigado, conforme se lê da sentença:

> O Policial Militar Mayke da Silva, em seu depoimento de fl. 119, disse se recordar dos fatos, que a vítima foi à delegacia dizendo que havia sido roubada e que trazia um celular que seria do autor do crime, que este o teria perdido no momento do roubo. Afirma ainda que a vítima só viu um dos autores do fato, mas que pelas imagens das câmeras do banco eram dois indivíduos. Que no celular fornecido pela vítima tinham fotos do acusado e, além disso, pelo registro de ligações conseguiram o telefone fixo da namorada do acusado, e que assim, por uma consulta, conseguiu o nome dessa jovem e descobre então que esta havia visitado um indivíduo na cadeia. Que imprimiu a foto desse indivíduo e a vítima o reconheceu como sendo o autor do fato. Que então, no dia seguinte os policiais foram ao endereço do acusado, que antes de chegar na casa, o réu já foi encontrado e preso. Que a vítima reconheceu de pronto o indivíduo que fora preso. Que nas imagens a dinâmica do fato, e a atuação dos dois indivíduos é muito clara, que o réu lutou com a vítima e a agrediu quando esta caiu no chão. (fls. 158).

Aquele acusado foi condenado a 7 anos de reclusão, e o Tribunal de Justiça do Rio de Janeiro, por maioria, anulou a prova obtida pelo acesso, sem decisão judicial, aos dados contidos em seu celular. Em decorrência da teoria dos frutos da árvore envenenada, todo o conjunto probatório foi anulado, e o réu, absolvido.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

O Ministério Público, nesse recurso extraordinário, alega que o acesso aos dados em aparelho celular apreendido na prática de crime não pode ser considerada "comunicação telefônica", nestes termos:

> E aí pergunta-se: há relação entre tais informações armazenadas no celular e o sigilo das comunicações telefônicas? A resposta, saltante à vista, é negativa, já que não está o aparelho móvel, *in casu*, sendo utilizado para "comunicações telefônicas", mas sim para armazenar dados, registros e informações, devidamente apreendidos pela autoridade policial e cujo acesso prescinde de autorização judicial. E verifica-se, inclusive, ser procedimento rotineiro na praxe policial a realização de perícia de informações contidas em celulares apreendidos em práticas delitivas (fotos, registros de ligações, mensagens, contatos, etc.), não se discutindo acerca da licitude dessa prova, usualmente utilizada em processos criminais. (fls. 293/294)

O centro do recurso acusatório está na alegação de que a jurisprudência dominante nos tribunais pátrios, inclusive a desse Supremo Tribunal Federal, é de que a proteção constitucional do art. 5º, XII, é do fluxo comunicacional, não abrangendo os dados armazenados no telefone celular.

Em julgamento ocorrido em 23/11/2017, foi reconhecida a repercussão geral no presente caso. O andamento processual informado no sítio eletrônico do STF em 11/11/2020, sem alteração até a presente data, é o seguinte:

> Após o voto do Ministro Dias Toffoli (Relator), que dava provimento ao agravo e, ato contínuo, ao recurso extraordinário, de modo que, cassando-se o acórdão recorrido, se determine ao Tribunal de origem que prossiga no julgamento da apelação criminal, conforme de direito, julgando prejudicados os requerimentos constantes das petições/STF nº 38990/2018 e nº 77244/2017, e fixava a seguinte tese (tema 977 da repercussão geral): "É lícita a prova obtida pela autoridade policial, sem autorização judicial, mediante acesso a registro telefônico ou agenda de contatos de celular apreendido ato contínuo no local do crime atribuído ao acusado, não configurando esse acesso ofensa ao sigilo das comunicações, à intimidade ou à privacidade do indivíduo (CF, art. 5º, incisos X e XII)"; e dos votos dos Ministros Gilmar Mendes e Edson Fachin, que negavam provimento ao recurso interposto e propunham a fixação da seguinte tese: "O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX)", pediu vista dos autos o Ministro Alexandre de Moraes. Falou, pelo recorrido, o Dr. Pedro Paulo Lourival Carriello, Defensor

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

Público do Estado do Rio de Janeiro. Plenário, Sessão Virtual de 30.10.2020 a 10.11.2020.

Todos esses atos, portanto, são anteriores à referida EC 115/2022.

II. ACESSO A DADOS – EVOLUÇÃO EMPÍRICA, JURISPRUDENCIAL E NORMATIVA

A Constituição de 1988, em seu artigo 5º, XII, estabeleceu que "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."

Em relação à expressão "dados", a sua primeira análise pelo STF ocorreu em dezembro de 1993, por ocasião do julgamento da Ação Penal 307 (caso Collor), quando se considerou inconstitucional a apreensão de um computador e a posterior decodificação dos dados ali existentes. A compreensão do sentido do art. 5º, XII, foi assim traduzida no voto do Relator, Ministro Ilmar Galvão:

> Mas, mesmo que a apreensão material do computador, no recinto da empresa se houvesse dado em uma das situações fáticas previstas no inc. XI do art. 5º da Carta Federal, ou houvesse sido feita em cumprimento a determinação judicial, ainda assim, não estaria compreendido o conteúdo ideológico de sua memória, razão pela qual a Polícia Federal não poderia ter-se apropriado dos dados contidos naquele microcomputador, para mandar decodificá-los ao seu alvedrio, como fez, acobertados que se achavam pelo sigilo, o qual, conquanto se possa ter como corolário da inviolabilidade do próprio recinto dos escritórios da empresa acha-se especificamente contemplado no inc. XII, do mesmo artigo, ao lado da correspondência e das comunicações telegráficas e telefônicas.
>
> Aliás, nos tempos modernos, em que todos os trabalhos datilográficos das empresas é realizado por meio de digitação, a invasão da memória dos computadores implica fatalmente a quebra do sigilo não apenas de dados em geral, desde relativos a simples agenda até os relacionados a fórmulas e cálculos, mas também de toda correspondência, epistolar e telegráfica, em relação aos quais o manto constitucional é de natureza absoluta, já que não deixou espaço reservado ao trabalho normativo do legislador ordinário, como se fez com as comunicações telefônicas.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

Vencido naquela oportunidade, o Ministro Sepúlveda Pertence conseguiu posteriormente fazer prevalecer a sua posição, segundo a qual "a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não os 'dados' em si" (RE 418.416). Tal entendimento veio sendo adotado ao longo do tempo, inclusive em relação a dados encontrados em celular de investigado, como ocorreu no *HC* 91.867, julgado em 24/4/2012. Consta da ementa que "não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados."

Depois desse último julgado, alguns episódios relevantes ocorreram no âmbito internacional. Em 2014, a Suprema Corte dos Estados Unidos da América julgou o caso Riley v. Califórnia[1], em que policiais, após apreensão de um telefone celular encontrado com um suspeito, analisou fotos e vídeos a partir dos quais o associou a um tiroteio ocorrido há algumas semanas e à participação em gangues. O *Justice* Robert, em seu voto, representativo da opinião da Corte, ressaltou que os celulares modernos possuem uma imensa capacidade de armazenamento de dados, os quais, especialmente quando combinados entre si, guardam um conjunto bastante expressivo de informações sobre a pessoa, permitindo a observação de todo o seu ciclo de vida. Concluiu que, pelo impacto no direito à privacidade dos indivíduos, o acesso às informações contidas em aparelho celular só poderia se dar mediante autorização judicial específica.

Em 27 de abril de 2016, o Parlamento Europeu e o Conselho da União Europeia aprovaram a Diretiva (UE) 2016/680[2], relativa "à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detenção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados". A sua premissa central é de que "a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental". E consigna ainda que "a rápida evolução tecnológica e a globalização criaram novos

[1] Riley v. California, 134 S. Ct. 2473, 2493 (2014). Disponível em http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

[2] CELEX_32016L0680_PT_TXT PDF

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

desafios em matéria de proteção de dados pessoais". Desse modo, "a proteção eficaz dos dados pessoais na União exige não só sejam reforçados os direitos dos titulares dos dados e as obrigações de quem trata dados pessoais, mas também que haja reforço dos poderes equivalentes para controlar e assegurar a conformidade com as regras de proteção de dados nos Estados-Membros".

A Diretiva UE 2016/680 registra que "a fim de evitar um sério risco de ser contornada, a proteção das pessoas singulares deverá ser neutra em termos tecnológicos e não deverá depender das técnicas utilizadas". Assim, a proteção de dados pessoais deve ocorrer, seja o meio automatizado ou manual.

Já o Regulamento (UE) 2016/679, o Regulamento Geral sobre a Proteção de Dados na União Europeia[3], aprovado também em abril de 2016, apesar de não tratar especificamente de matéria penal, considera que a evolução tecnológica exige um quadro de proteção de dados sólido, pois é uma medida importante para "gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno".

Em 2018, o Tribunal Constitucional alemão declarou inconstitucional lei que permitia à polícia realizar, de maneira sigilosa, buscas ou investigações remotas em computadores de pessoas suspeitas de cometer crime[4].

Nesse mesmo ano, em 14 de agosto, no Brasil, é promulgada a Lei 13.709 – a Lei Geral de Proteção de Dados -, cujos princípios fundamentais são: (i) respeito à privacidade; (ii) autodeterminação informativa; (iii) liberdade de expressão, informação, comunicação e opinião; (iv) inviolabilidade da intimidade, da honra e da imagem; (v) desenvolvimento econômico e tecnológico e a inovação; (vi) livre iniciativa, livre concorrência e direito do consumidor; (vii) direitos humanos, livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º).

[3] CELEX_32016R0679_EN_TXT PDF

[4] MENKE, Fabiano. *In:* MENDES, Gilmar Ferreira. SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. *Direito, Inovação e Tecnologia,* p. 215-216

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

Essa lei, tal como estatuído em seu art. 4º, III, "d", não se aplica a "atividades de investigação e repressão de infrações penais". Todavia, o § 2º desse mesmo art. 4º dispõe que "[o] tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que 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 nesta Lei".

Antes de sua entrada em vigor (art. 65), o STF, em medida cautelar, suspendeu a eficácia de medida provisória que possibilitava o compartilhamento de dados de usuários de serviços de telefonia móvel com o Instituto Brasileiro de Geografia e Estatística – IBGE. O acórdão está assim ementado:

> EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. **2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.** 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. **Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para**

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada. (ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020. Destaque acrescido,

Também no âmbito do direito penal, a Corte começou a rever o seu entendimento, como se verifica da ementa a seguir:

Habeas corpus. (...) 2. Acesso a aparelho celular por policiais sem autorização judicial. Verificação de conversas em aplicativo WhatsApp. **Sigilo das comunicações e da proteção de dados. Direito fundamental à intimidade e à vida privada. Superação da jurisprudência firmada no HC 91.867/PA. Relevante modificação das circunstâncias fáticas e jurídicas**. **Mutação constitucional**. **Necessidade de autorização judicial**. 3. Violação ao domicílio do réu após apreensão ilegal do celular. 4. Alegação de fornecimento voluntário do acesso ao aparelho telefônico. 5. Necessidade de se estabelecer garantias para a efetivação do direito à não autoincriminação. 6. Ordem concedida para declarar a ilicitude das provas ilícitas e de todas dela derivadas. (HC 168052; Órgão julgador: Segunda Turma; Relator(a): Min. GILMAR MENDES; Julgamento: 20/10/2020; Publicação: 02/12/2020). Destaque acrescido.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

IV. A EMENDA CONSTITUCIONAL 115/2022

A EC 115/2022 inseriu no art. 5º da Constituição o inciso LXXIX, com a seguinte redação:

> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Nesse mesmo artigo 5º, a Constituição ainda prevê, em seu § 1º, que "as normas definidoras de direitos e garantias fundamentais têm aplicação imediata". Significa dizer que, por força do inciso LXXIX, acrescido pela EC 115, o direito à proteção de dados pessoais tem estatura autônoma[5], independente de outras cláusulas constitucionais que tenham com ele alguma solidariedade, como é o caso dos direitos à privacidade e à intimidade (art. 5º, X e XII).

Na famosa classificação proposta por José Afonso da Silva[6], seria uma norma de aplicabilidade imediata e eficácia contida, ou seja, norma com aptidão imediata de produzir os seus efeitos, independentemente de regulamentação, mas passível de que tais efeitos sofram restrição pelo legislador. O STF, na referida AP 307, havia aplicado essa mesma compreensão quanto ao sigilo das comunicações telefônicas, que poderia ser afastado mediante ordem judicial, "nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (art. 5º, XII). Já havia sido assentado que, enquanto não houvesse lei, o sigilo tinha caráter absoluto. Veja-se, a propósito, voto do Ministro Moreira Alves:

> Com efeito, também com relação aos dados em geral – e, consequentemente, os constantes de computador que pode armazenar as mais sigilosas informações que seu proprietário -, estão eles cobertos pela garantia do disposto no inciso XII do artigo 5º da Constituição (...)
>
> Pelos termos em que está redigido esse dispositivo, que só abre exceção para as comunicações telefônicas, é possível sustentar-se

[5] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. GenForense: Rio de Janeiro, 2020

[6] SILVA, José Afonso da. *Aplicabilidade das normas constitucionais.* 3. Ed. São Paulo: Malheiros, 1998, p. 76

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> para as comunicações telefônicas, é possível sustentar-se que as demais inviolabilidades só admitem sejam afastadas por texto constitucional expresso. Mas, ainda quando se admita que possam ser postas de lado nas hipóteses e na forma prevista na lei, o que é certo é que não há lei que disponha a respeito no concernente – que é o que importa no momento – à inviolabilidade dos dados aludidos no citado texto constitucional.

Positivado o novo direito fundamental, resta compreender o seu alcance.

O texto é claro em assegurar a proteção dos dados considerados pessoais.

Na disciplina de proteção de dados, há duas compreensões mais difundidas a respeito do que é um dado pessoal: a reducionista e a expansionista. A primeira entende que o dado é pessoal quando ele **identifica** uma pessoa natural (de forma direta). A segunda concepção entende que um dado é pessoal quando, dele, uma pessoa natural é **identificável** (de maneira direta ou indireta). A teoria expansionista abarca as inúmeras possibilidades de um dado aparentemente anônimo (a antonímia de dado pessoal) identificar uma pessoa. Um exemplo clássico é o do registro de IP. De forma direta, ele não identifica uma pessoa natural; com algumas diligências, contudo, é possível associá-lo a alguém. Por essa razão, a maioria dos países vem adotando o conceito expansionista de dado pessoal, estando essa definição também presente na Diretiva UE 2016/680. Consta de seu item 21:

> Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular **identificada ou identificável.** Para determinar se uma pessoa singular é identificável, importa considerar todos os meios que possam ser razoavelmente utilizados, quer pelo responsável pelo tratamento quer por qualquer outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta tanto a tecnologia disponível à data do tratamento dos dados como a evolução tecnológica. Os princípios de proteção de dados não deverão, pois, aplicar-se às informações anônimas, isto é, informações que não digam respeito a nenhuma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal forma anônimos que o seu titular já não possa ser identificado. (Destaque acrescido).

O direito brasileiro seguiu idêntico caminho. A Lei Geral de Proteção de Dados (13.709/18), em seu artigo 5º, I, define dado pessoal como a "informação

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

relacionada a pessoa natural identificada ou **identificável**" (destaque acrescido). O decreto regulador do Marco Civil da Internet (Decreto nº 8.771/16) assim estatui:

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
> I - dado pessoal - dado relacionado à pessoa natural identificada ou **identificável**, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; (Destaque acrescido).

O mesmo conceito foi aplicado por esse Supremo Tribunal Federal quando do julgamento da ADI 6387 (caso IBGE):

> Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados."

Nesse caso IBGE, o STF também afirmou outra dimensão essencial à proteção dos dados pessoais: o direito fundamental à autodeterminação informativa. Consta do voto do Ministro Gilmar Mendes:

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

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios.

Finalmente, no âmbito infraconstitucional, o Marco Civil da Internet prevê que a entrega de dados pessoais em investigações criminais deve ser precedida por decisão judicial, devendo o mesmo ser extensível a apreensões de aparelhos telefônicos. Em recente e derradeiro voto, na qual julgava inconstitucional a quebra coletiva e não individualizada de dados pessoas, no âmbito do RE 1301250, cujo julgamento se encontra suspenso, a Min. Rosa Weber, relatora, pontuou quais são os requisitos mínimos de uma decisão que determina a quebra de dados pessoais:

> "**Não se pode esquecer que a quebra do sigilo de dados telemáticos consubstancia restrição a direitos fundamentais. Assim, a meu juízo, referida limitação, no que diz especificamente com o afastamento do sigilo constitucional determinado por meio de decisão judicial, somente deve ser efetivada de forma pontual, episódica, caso estritamente necessária para elucidação de práticas delituosas, com a individualização do investigado e do objeto da investigação** (MORAES, Alexandre de. Direitos humanos fundamentais : teoria geral – comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil – doutrina e jurisprudência. 12. ed. São Paulo: Atlas, 2021, p. 161), em ordem a mitigar o impacto do ato decisório" (STF, RE 1301250, Min. Rosa Weber, voto proferido em 22.09.23, julgamento não finalizado, destacamos).

Ou seja, não apenas o acesso a dado telemáticos demanda decisão judicial, como essa decisão necessita cumprir os requisitos de proteção de dados, e demonstrar indícios de participação em atividade criminosa do titular dos dados de forma individualizada e fundamentada.

V. CONCLUSÕES

Pelo que foi até aqui exposto, é possível concluir:

(1) a proteção a dados pessoais, inclusive em meios digitais, é, na atualidade brasileira, direito fundamental, por conta do disposto no inciso LXXIX do art. 5º da Constituição, inserido pela EC 115/2022;

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

(2) a aplicação do dispositivo é imediata, considerando a disciplina contida no art. 5º, § 1º, da CF;

(3) considerando o princípio da unidade da Constituição, é razoável afirmar que, mesmo diante da ausência de lei eventualmente limitando em alguma medida esse direito, o acesso a dados pessoais para fins de investigação criminal ou instrução processual é possível mediante ordem judicial, à vista do disposto no art. 5º, XII, da CF;

(4) dados pessoais, nos termos da legislação brasileira, são informações relacionadas a pessoa natural identificada ou identificável, existentes em meios físicos ou digitais;

(5) o núcleo essencial da proteção de dados pessoais está em seus princípios fundamentais, tal como delineados na no art. 2º da Lei Geral de Proteção de Dados, dos quais se destaca a autodeterminação informativa;

(6) a autodeterminação informativa, transposta para a área das investigações e repressões criminais, significa a possibilidade de que o titular tenha algum nível de controle sobre os seus dados, o que demanda necessariamente a intervenção judicial na condição de ator não interessado;

(7) a anterior jurisprudência desse Supremo Tribunal Federal, no sentido de que a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação de dados, e não dos dados em si, é insustentável na atualidade, diante da mutação constitucional operada pela EC 115/2022.

VI. TESE PROPOSTA

Com o exclusivo propósito de colaborar para a discussão posta nesses autos, o IBCCrim sugere como tese a ser adotada a seguinte: o acesso a dados pessoais de pessoa natural identificada ou identificável, existentes em meios físicos ou digitais, para fins de investigação criminal ou instrução processual, só é

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

possível mediante ordem judicial que respeite os princípios relativos ao direito fundamental à proteção de dados, com a individualização do investigado e do objeto da investigação.

Brasília, 12 de dezembro de 2023

RENATO STANZIOLA VIEIRA:94331286649
Assinado de forma digital por RENATO STANZIOLA VIEIRA:94331286649 Dados: 2023.12.12 18:02:54 -03'00'

Renato Stanziola Vieira
OAB/SP 189.066

DEBORAH MACEDO DUPRAT DE BRITTO PEREIRA
Assinado de forma digital por DEBORAH MACEDO DUPRAT DE BRITTO PEREIRA Dados: 2023.12.12 17:44:59 -03'00'

Deborah Duprat
OAB/DF 65.698

Raquel Lima Scalcon
OAB/RS 86.286

ANDRE DA ROCHA FERREIRA
Assinado de forma digital por ANDRE DA ROCHA FERREIRA Dados: 2023.12.12 17:29:11 -03'00'

André da Rocha Ferreira
OAB/RS 102.517

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br