PROPOSTA DE TESE

Nome: Bárbara Prado Simão		
Área de Atividade: Terceiro Setor / Pesquisa		
Unidade/Regional (DPE/SP): Central		
Instituição/Organização/Movimento Social: InternetLab		
Endereço: Rua Bela cintra, 468		
	Bairro: Consolação	
CEP: 01415-000	Cidade: São Paulo	
Telefone.: 11 99544-9008		Fax
E- mail.: barbara.simao@internetlab.org.br		

SÚMULA
Dados armazenados em dispositivos eletrônicos somente podem ser acessados mediante ordem judicial, ainda que o dispositivo tenha sido apreendido em flagrante delito e que tenha sido registrado o consentimento durante a abordagem.
ASSUNTO
O assunto da presente proposta diz respeito ao acesso a dados armazenados em dispositivos eletrônicos apreendidos por forças policiais durante abordagens ou em flagrante delito, e seu uso para a finalidade de instrução processual penal. A tese trata da necessidade de ordem judicial prévia para seu acesso e uso, rechaçando a possibilidade de obtenção do consentimento do investigado titular de dados ou de sua presunção.
ITEM ESPECÍFICO DAS ATRIBUIÇÕES INSTITUCIONAIS DA DEFENSORIA PÚBLICA

Exercer a defesa dos direitos e interesses individuais, difusos, coletivos e individuais homogêneos (Art. 4º, VIII, LC 80/1994).

Exercer, mediante o recebimento dos autos com vista, a ampla defesa e o contraditório em favor de pessoas naturais e jurídicas, em processos administrativos e judiciais, perante todos os órgãos e em todas as instâncias, ordinárias ou extraordinárias, utilizando todas as medidas capazes de propiciar a adequada e efetiva defesa de seus interesses; (Redação dada pela Lei Complementar nº 132, de 2009). (Art. 4º, V, LC 80/1994).

META DO PLANO DE ATUAÇÃO RELACIONADA (SE HOUVER)

FUNDAMENTAÇÃO JURÍDICA

Abaixo, apresentamos a fundamentação da presente tese em três eixos, o primeiro deles (i) quanto às garantias no âmbito da Convenção Americana de Direitos Humanos; outro (ii) quanto à proteção constitucional e infraconstitucional dos referidos dados pessoais como comunicações passíveis de sigilo, juntamente com uma breve exposição da jurisprudência dos tribunais superiores sobre a matéria; e (iii) quanto à impossibilidade de obtenção ou presunção de consentimento do investigado, titular de dados, nesses casos.

A proteção à vida privada é consagrada no art. 11 da Convenção Americana de Direitos Humanos, ratificada pelo Brasil em setembro de 1992 e promulgada pelo Decreto n. 678/1992. O art. 11.2 estabelece que ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou correspondência. Já o art. 11.3 garante a proteção da lei contra tais ingerências. A jurisprudência da Corte Interamericana de Direitos Humanos (Corte IDH) estendeu o entendimento de "correspondência" a outras formas de comunicação, como as conversas telefônicas, nos casos Tristán Donoso vs Panamá e Escher e outros vs Brasil [Tristán Donoso (parágrafo 55); Escher (parágrafo 114)]. Nestes, a Corte IDH retomou o argumento de que o âmbito da privacidade se caracteriza por estar isento e imune às invasões ou agressões abusivas ou arbitrárias por parte de terceiros ou da autoridade pública [Tristán Donoso (parágrafo 55); Escher (parágrafo 113)]. As restrições ao gozo e exercício do direito devem estar claramente previstas em lei (em sentido formal e material), perseguir um fim legítimo e cumprir os requisitos de idoneidade, necessidade e proporcionalidade, isto é, devem ser necessárias em uma sociedade democrática [Tristán Donoso (parágrafos 56 e 77); Escher (parágrafos 116 e 130)].

O acesso a dados armazenados em dispositivos eletrônicos apreendidos por forças policiais durante abordagens ou em flagrante delito implica uma ingerência no direito

à privacidade, cuja dispensa de prévia ordem judicial não se adequa ao teste tripartite acima mencionado. A ingerência abusiva ocorre seja no acesso ao conteúdo de comunicações, seja na verificação de outros dados a elas associados. No caso Escher e outros vs Brasil, a Corte IDH afirmou que a proteção do art. 11 da Convenção Americana compreende tanto conteúdo das comunicações quanto "qualquer outro elemento do processo comunicativo," como os dados que identificam uma comunicação (ex: registros de chamadas) [parágrafo 114]. A Corte IDH ressaltou, ainda, que a fluidez informativa existente na atualidade coloca o direito à vida privada das pessoas em uma situação de maior risco, "devido à maior quantidade de novas ferramentas tecnológicas e à sua utilização cada vez mais frequente," devendo o Estado "assumir um compromisso com o fim de adequar aos tempos atuais as fórmulas tradicionais de proteção do direito à vida privada" [parágrafo 115].

A matéria objeto da tese é abordada também, direta ou indiretamente, por diversos diplomas legais. Principiologicamente, predominam os dispositivos da Constituição Federal, da Lei de Interceptações e do Marco Civil da Internet, além, mais recentemente, da Lei Geral de Proteção de Dados (LGPD). O Art. 5º, XII, da Constituição Federal garante o sigilo de comunicações, ressalvando a possibilidade de "quebra" de comunicações telefônicas, mediante ordem judicial, para fins de investigação e instrução processual penal. O inciso X do mesmo art. 5º garante, ainda, a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas naturais. A Lei de Interceptações (Lei n. 9.296/1996), por sua vez, em regulamentação do referido Art. 5º, XII, CFB, trata da quebra de sigilo do "fluxo de comunicações" mediante a colaboração de empresas de telecomunicações e/ou a instalação de grampos e escutas ambientais. Por sua vez, o Marco Civil da Internet (Lei n. 12.695/14) estabelece a necessidade de ordem judicial (art. 7º, III) para o acesso a dados guardados por um intermediário (como provedores de aplicações). Merece menção aqui também a LGPD (Lei n. 13.709/18), que estabelece regras para o tratamento de dados pessoais no país, impondo seus princípios também à atividade de investigação e repressão de infrações penais (Art. 4º, III, d; IV, § 1º).

A segunda turma do Supremo Tribunal Federal (STF), em decisão de 20/10/2020 no HC 168052, relatada pelo Min. Gilmar Mendes, declarou a nulidade de provas obtidas sem ordem judicial a partir do acesso ao celular de um homem abordado por policiais. Com base em conversas realizadas no aparelho por meio do aplicativo WhatsApp, a polícia procedeu a ação de busca e apreensão em sua residência, que resultou em sua prisão por tráfico de drogas. O ministro relator, em aplicação dos princípios da "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", além de menção à proteção à privacidade, aos dados pessoais, à vida privada, ao fluxo de comunicações e às comunicações privadas dos usuários da internet, estabelecidos pelo Marco Civil da Internet, decidiu por acatar o argumento de que tais dados somente podem ser acessados mediante prévia decisão judicial.

Neste julgado, o STF superou o entendimento de que haveria alguma diferença entre "fluxo de dados" e "dados armazenados", esposado por parte da jurisprudência e pelo próprio STF até então. Com efeito, o HC 91.867/PA, julgado pelo STF em abril de 2012, que também defendia tal interpretação restritiva do art. 5º, XII da CFB, foi explicitamente reformado pela Corte na nova decisão de 2020. Na interpretação superada, "partia-se da compreensão que os dados em si não eram objeto de proteção, mas somente as comunicações realizadas." A interpretação sofreu modificações em vista da crescente importância e centralidade das tecnologias digitais para os indivíduos

e sociedade, de que se resulta a necessidade de protegê-la com maior zelo do que a ordem jurídica previa ser necessário há pouco menos de uma década. Nas palavras do relator, "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".

Trata-se, assim, de "típico caso de mutação constitucional", em que "a modificação das circunstâncias fáticas e jurídicas, a promulgação de leis posteriores e o significativo desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos smartphones leva, nos dias atuais, à solução distinta [da tomada anteriormente pela Corte]."

Entendimento similar foi proferido pelo Superior Tribunal de Justiça (STJ) em julgamento de 19/04/2016, no HC 51.531/RO, e relatado pelo Min. Nefi Cordeiro, onde se decidiu que "ilícita é a devassa de dados, bem como das conversas de WhatsApp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial." Em seu voto, o Min. relator ressalta: "Nas conversas mantidas pelo programa WhatsApp, que é forma de comunicação escrita, imediata, entre interlocutores, tem-se efetiva interceptação inautorizada de comunicações. É situação similar às conversas mantidas por e-mail, onde para o acesso tem-se igualmente exigido a prévia ordem judicial", também em aplicação dos diplomas legais trazidos pelo STF. A decisão do STJ é paradigmática, já que estabeleceu, pela primeira vez na jurisprudência superior do país, a proteção específica sobre informações armazenadas em dispositivos eletrônicos.

Os dois casos acima descritos estabelecem importante base jurídica para o entendimento acerca do acesso a dados de celulares nessas situações. Tratam-se, em resumo, de dados protegidos pelo sigilo de comunicações e pela proteção à vida privada (Art. 5º, X e XII da Constituição Federal), protegidos ainda pela ordem infraconstitucional de forma sistemática e principiológica, aplicando-se a eles o Art. 3º da Lei de Interceptações, que exige autorização judicial prévia para a "quebra" desse sigilo, e o Art. 7º, III, do Marco Civil da Internet, que estabelece o direito de "inviolabilidade e sigilo de comunicações privadas armazenadas, salvo por ordem judicial". A estes, adicionam-se os princípios da Lei Geral de Proteção de Dados, que também se aplicam às atividades de investigação e repressão de infrações penais (Art. 4º, § 1º da LGPD), tais como a autodeterminação informativa, a inviolabilidade da intimidade, e o respeito à privacidade.

Se a necessidade de ordem judicial é ponto central a esta tese, outro argumento correlato deve também ser abordado. Especificamente, deve-se rechaçar a tese de que o consentimento para acesso aos dados armazenados em celulares apreendidos nessas situações pode ser validamente concedido pelo sujeito de determinada abordagem policial, e, muito menos, que possa ser presumido de qualquer maneira.

Faz-se referência, aqui, a julgados de tribunais de justiça em que o consentimento foi considerado validamente concedido em vista da ausência de informação ou prova nos autos de que tenha ocorrido coação policial ou de que o acusado tenha se oposto ao acesso ao seu celular. Ou, ainda, a julgados onde o fornecimento da senha do aparelho pelo indivíduo foi considerado como indicativo suficiente de concessão do consentimento.

Este entendimento carece de fundamentação. Por se tratarem de dados pessoais legalmente protegidos, como se viu acima, e considerando-se a situação fática de sua obtenção (celulares apreendidos por forças policiais) e a finalidade de seu tratamento (instrução processual penal, ou como meio de prova penal) não se pode falar de obtenção de consentimento válido para seu tratamento, sendo a ordem judicial a única maneira legítima de acessá-los e tratá-los nessa hipótese. Isso porque a ordem jurídica brasileira dá ao consentimento para tratamento de dados pessoais importantes limites, com o intuito de empoderar o indivíduo, titular de dados, a controlar de maneira livre e informada o que é feito com suas informações pessoais. Trata-se, também, de decorrência do princípio da autodeterminação informativa, princípio estabelecido pelo Art. 2º, II, da LGPD.

Mais concretamente, o Art. 7º, VII, do Marco Civil da Internet, assegura aos titulares o direito de "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei". De forma similar, mesmo que o artigo específico não se aplique ao caso em apreço, o Art. 5º, XII, da LGPD, define o consentimento como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada." As adjetivações do consentimento – "livre, informado e inequívoco", ou "livre, expresso e informado" – buscam exatamente garantir a autodeterminação informativa do titular de dados e os princípios constitucionais e infraconstitucionais acima descritos. Nesse sentido, e como extensão da necessidade de o consentimento ser inequívoco ou expresso, a LGPD estabelece ainda que este deve ser concedido "por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (Art. 8º, caput), e o Marco Civil, ainda, que sua coleta deve "ocorrer de forma destacada das demais cláusulas contratuais" (Art. 7º, IX).

Em interpretação sistemática e principiológica do que se expôs até aqui, é clara a impossibilidade de obtenção de consentimento válido no caso de acesso a celulares apreendidos em flagrante delito ou abordagens policiais. Em primeiro lugar, não há que se falar em consentimento inequívoco ou expresso (tampouco por escrito), no caso de mero fornecimento de uma senha, e muito menos no caso de simples ausência de provas ou informações nos autos que apontem que ele não tenha sido concedido. Em segundo, há também óbvios vícios na possibilidade de o consentimento ser livre e informado. Afinal, trata-se de situação de uso de forças policiais e de ambiente muito provavelmente intimidatório, onde é discutível a autonomia do indivíduo de livremente consentir com o uso de seus dados pessoais, não havendo nessa situação, ainda, possibilidade razoável de o titular ser informado suficientemente sobre que uso será feito de seus dados pessoais.

Vai justamente nesse sentido o entendimento de "manifestação de vontade livre" no âmbito do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), regulação que inspirou a elaboração da LGPD brasileira. Segundo as diretrizes do Comitê Europeu de Proteção de Dados (European Data Protection Board), instância que reúne representantes das autoridades de proteção de dados do bloco europeu, o elemento 'livre' na qualificação do consentimento implica uma verdadeira possibilidade de escolha e controle para os titulares dos dados. Complementa que, como regra geral, o GDPR "prevê que se o titular dos dados não puder exercer uma verdadeira escolha, sentir-se coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido." O claro desequilíbrio de poder entre quem solicita acesso a informações pessoais e o titular dos dados é,

portanto, situação que compromete a validade do consentimento. De forma relacionada, o consentimento não é considerado como fundamento suficiente para autorizar o tratamento de dados pessoais para efeitos de prevenção, investigação ou repressão de infrações penais no âmbito da Diretiva da União Europeia 2016/680 (Law Enforcement Directive), destinada a regular o tratamento de dados pessoais para esses fins, o que se depreende do considerando 35 combinado ao artigo 8º da Diretiva.

Assim, o consentimento não pode servir de maneira a substituir a ordem judicial nesses casos. O argumento é especialmente fortalecido quando se considera o direito fundamental à não autoincriminação (Art. 5º, LVII da Constituição Federal). Não há que se falar em obtenção de consentimento para a finalidade de produzir provas contra si mesmo. Essa linha argumentativa é defendida pelo próprio STF no referido HC 168052 de 2020. Ali, frisa-se a necessidade de ordem judicial como único meio válido de acesso a tais dados: "Essas medidas [de acesso a aparelhos telefônicos e a residência de suspeitos] devem ser submetidas à prévia decisão judicial, enquanto garantia procedimental in concreto através da qual sejam analisados e registrados, especificamente, os fundamentos que possam afastar os direitos fundamentais envolvidos. Ou seja, a existência de prévia decisão judicial é capaz de demonstrar a necessidade, adequação e proporcionalidade da pretensão dos órgãos de segurança de acesso aos dados, informações e residência dos suspeitos. Permite, ainda, o controle desses fundamentos."

FUNDAMENTAÇÃO FÁTICA

Avanços tecnológicos têm impactado diretamente as atividades de investigação e persecução penal. A multiplicação de dispositivos conectados à internet tem tornado o acesso a dados armazenados em dispositivos ou por eles acessados uma importante questão quanto às condições de sua obtenção e utilização para fins de instrução processual.

Especificamente quanto ao acesso a dados armazenados em dispositivos eletrônicos apreendidos em abordagens policiais ou situações de flagrante delito, e ao seu uso para fins de instrução processual penal, a jurisprudência nacional tem encontrado diferentes interpretações, não obstante a existência de precedentes nos tribunais superiores do país que exigem ordem judicial para que o procedimento seja possível.

Diante disso, é certo que o suposto consentimento do titular dos dados não substitui a necessidade de ordem judicial, a qual constitui o único meio válido de acesso às informações.

SUGESTÃO DE OPERACIONALIZAÇÃO

A operacionalização seguirá caso a caso. De forma geral, deverão ser consideradas nulas quaisquer provas obtidas sem ordem judicial prévia a partir de dados armazenados em dispositivos apreendidos em flagrante delito ou abordagens policiais, assim como outras provas delas resultantes. Não se poderá coletar ou presumir o consentimento do investigado nesses casos.

INDICAÇÃO DA PERSPECTIVA/ENFOQUE DE GÊNERO E RAÇA RELACIONADA À TESE, SE HOUVER.

MANIFESTAÇÃO PROCESSUAL PRÉ-FORMATADA

AO JUÍZO DA ___ª VARA .... DO FORO REGIONAL DE .... DA COMARCA DE .... DO ESTADO DE SÃO PAULO

Ementa da petição:

Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Autos n°

Ação de....

NOME, brasileiro/a, solteir/a, profissão, portador/a da cédula de identidade RG nº yyy, inscrito/a no CPF sob o nº yyyy, residente e domiciliado/a na Rua yyyy, nº yyy, bairro, cidade/SP, CEP yyyy, telefone(s) xxxx, *e-mail* xxxxx, por intermédio da **DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO**, dispensada de apresentar instrumento de mandato, vem, respeitosamente, à presença de Vossa Excelência, expor e requerer o que segue.

I. PRERROGATIVAS DA DEFENSORIA PÚBLICA

Esclarece-se, inicialmente, que aos/às membros/as da Defensoria Pública é garantida a prerrogativa de contagem em dobro de todos os prazos e a intimação pessoal mediante o encaminhamento dos autos com vistas, previstas nos incisos I e II do artigo 128 da Lei Complementar 80/94, bem como no artigo 186, do Código de Processo Civil/2015.

II. JUSTIÇA GRATUITA

A parte assistida é pobre na acepção jurídica do termo, não podendo arcar com as custas processuais e honorários advocatícios sem prejuízo de seu próprio sustento e de sua família, conforme declaração de necessidade anexa, fazendo, portanto, jus aos benefícios da justiça gratuita, na forma do art. 4º da Lei 1.060/50, alterado pela Lei 7.510/86, e do art. 98 do Código de Processo Civil.

III. FATOS

Trata-se de ...

É a síntese.

IV. MÉRITO (TESE INSTITUCIONAL)

A presente ação questiona a utilização de dados em instrução processual penal obtidos sem ordem judicial prévia, em frontal violação aos dispositivos constitucionais e infraconstitucionais sobre a matéria. Com efeito, na hipótese dos autos, a autoridade policial acessou dados armazenados no dispositivo eletrônico do autor sem autorização de um juízo competente, o que não encontra respaldo no ordenamento jurídico brasileiro, conforme a jurisprudência do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF).

Nesse sentido, é fundamental notar que a Constituição Federal Brasileira garante o sigilo das comunicações, ressalvando a possibilidade de "quebra" de comunicações telefônicas, **mediante ordem judicial**, para fins de investigação e instrução processual penal (art. 5º, XII). Ainda a nível constitucional, é garantida a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas naturais (art. 5º, X).

Concretizando os mandamentos constitucionais, especialmente o disposto no art. 5º, XII, a Lei de Interceptações (Lei n. 9.296/1996) trata da quebra de sigilo do "fluxo de comunicações" mediante a colaboração de empresas de telecomunicações e/ou a instalação de grampos e escutas ambientais. Por sua vez, o Marco Civil da Internet (Lei n. 12.695/14) estabelece a necessidade de ordem judicial (art. 7º, III) para o acesso a dados guardados por um intermediário (como provedores de aplicações). Além disso, a LGPD (Lei n. 13.709/18) estabelece regras para o tratamento de dados pessoais no país, impondo seus princípios também à atividade de investigação e repressão de infrações penais (Art. 4º, III, d; IV, § 1º).

Como se percebe, o ordenamento pátrio tutela a privacidade e a proteção dos dados pessoais como valores fundamentais. A atuação da autoridade policial no presente caso é manifestamente inconstitucional e ilegal.

Abaixo, serão apresentadas as razões específicas que conduzem à conclusão de invalidade do uso dos dados do autor para fins de instrução processual penal. Em primeiro lugar, será abordada a jurisprudência dos tribunais superiores no Brasil quanto à matéria. Na sequência, a presente ação trata da impossibilidade de obtenção ou presunção de consentimento do investigado, titular de dados, nesses casos. Por fim, serão analisadas as garantias em questão no âmbito da Convenção Americana de Direitos Humanos.

IV.1. Do entendimento do STF e do STJ - nulidade da medida

A segunda turma do Supremo Tribunal Federal (STF), em decisão de 20/10/2020 no HC 168052, relatada pelo Min. Gilmar Mendes, declarou a nulidade de provas obtidas sem ordem judicial a partir do acesso ao celular de um homem abordado por policiais. Com base em conversas realizadas no aparelho por meio do aplicativo WhatsApp, a polícia procedeu a ação de busca e apreensão em sua residência, que resultou em sua prisão por tráfico de drogas. O ministro relator, em aplicação dos princípios da proteção à intimidade e à vida privada, bem como ao princípio da

proporcionalidade nas intervenções estatais, decidiu por acatar o argumento de que tais dados somente podem ser acessados mediante prévia decisão judicial.

Como se percebe, a hipótese é similar à discutida na presente ação. O STF reconheceu expressamente a necessidade de ordem judicial para que seja possível à autoridade policial acessar os dados armazenados contidos no celular do investigado. Vale destacar que, no julgado mencionado, a Corte superou o entendimento de que haveria alguma diferença entre "fluxo de dados" e "dados armazenados", esposado por parte da jurisprudência e pelo próprio STF até então.

Com efeito, o HC 91.867/PA, julgado pelo STF em abril de 2012, que também defendia tal interpretação restritiva do art. 5º, XII da CFB, foi explicitamente reformado pela Corte na nova decisão de 2020. Na interpretação superada, "partia-se da compreensão que os dados em si não eram objeto de proteção, mas somente as comunicações realizadas". A interpretação sofreu modificações em vista da crescente importância e centralidade das tecnologias digitais para os indivíduos e sociedade, de que se resulta a necessidade de protegê-la com maior zelo do que a ordem jurídica previa ser necessário há pouco menos de uma década. Nas palavras do relator, "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' (*grifos nossos*).

Trata-se, assim, de "típico caso de mutação constitucional", em que "a modificação das circunstâncias fáticas e jurídicas, a promulgação de leis posteriores e o significativo desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos smartphones leva, nos dias atuais, à solução distinta [da tomada anteriormente pela Corte]."

Entendimento similar foi proferido pelo Superior Tribunal de Justiça (STJ) em julgamento de 19/04/2016, no HC 51.531/RO, e relatado pelo Min. Nefi Cordeiro, onde se decidiu que "ilícita é a devassa de dados, bem como das conversas de WhatsApp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial." Em seu voto, o Min. relator ressalta: "Nas conversas mantidas pelo programa WhatsApp, que é forma de comunicação escrita, imediata, entre interlocutores, tem-se efetiva interceptação inautorizada de comunicações. **É situação similar às conversas mantidas por e-mail, onde para o acesso tem-se igualmente exigido a prévia ordem judicial**" (*grifos nossos*), também em aplicação dos diplomas legais trazidos pelo STF. A decisão do STJ é paradigmática, já que estabeleceu, pela primeira vez na jurisprudência superior do país, a proteção específica sobre informações armazenadas em dispositivos eletrônicos.

Como se vê, os dois casos acima descritos estabelecem importante base jurídica para o entendimento acerca do acesso a dados de celulares nessas situações. Trata-se, em resumo, de dados protegidos pelo sigilo de comunicações e pela proteção à vida privada (Art. 5º, X e XII da Constituição Federal), e ainda pela ordem infraconstitucional de forma sistemática e principiológica, aplicando-se a eles o Art. 3º da Lei de Interceptações, que exige autorização judicial prévia para a "quebra" desse sigilo, e o Art. 7º, III, do Marco Civil da Internet, que estabelece o direito de "inviolabilidade e sigilo de comunicações privadas armazenadas, salvo por ordem judicial". A estes, adicionam-se os princípios da Lei Geral de Proteção de Dados, que também se aplicam às atividades de investigação e repressão de infrações penais (Art.

4º, § 1º da LGPD), tais como a autodeterminação informativa, a inviolabilidade da intimidade, e o respeito à privacidade.

IV.2. Da impossibilidade de obtenção ou presunção de consentimento do investigado

Se a necessidade de ordem judicial é ponto central da matéria discutida na presente ação, outro argumento correlato deve também ser abordado. De maneira específica, deve-se rechaçar a tese de que o consentimento para acesso aos dados armazenados em celulares apreendidos nessas situações pode ser validamente concedido pelo sujeito de determinada abordagem policial, e, muito menos, que possa ser presumido de qualquer maneira.

Faz-se referência, nesse ponto, a julgados de tribunais de justiça em que o consentimento foi considerado validamente concedido em vista da ausência de informação ou prova nos autos de que tenha ocorrido coação policial ou de que o acusado tenha se oposto ao acesso ao seu celular. Ou, ainda, a julgados onde o fornecimento da senha do aparelho pelo indivíduo foi considerado como indicativo suficiente de concessão do consentimento.

Com todas as vênias, este entendimento não possui fundamentação idônea. Por se tratarem de dados pessoais legalmente protegidos, como se viu acima, e considerando-se a situação fática de sua obtenção (celulares apreendidos por forças policiais) e a finalidade de seu tratamento (instrução processual penal, ou como meio de prova penal) não se pode falar de obtenção de consentimento válido para seu tratamento, sendo a ordem judicial a única maneira legítima de acessá-los e tratá-los nessa hipótese.

Como se viu, a ordem jurídica brasileira dá ao consentimento para tratamento de dados pessoais importantes limites, com o intuito de empoderar o indivíduo, titular de dados, a controlar de maneira livre e informada o que é feito com suas informações pessoais. Trata-se, também, de decorrência do princípio da autodeterminação informativa, princípio estabelecido pelo Art. 2º, II, da LGPD.

De maneira ainda mais concreta, o Art. 7º, VII, do MCI assegura aos titulares o direito de "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei". De forma similar, mesmo que o artigo específico não se aplique ao caso em apreço, o Art. 5º, XII, da LGPD, define o consentimento como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada." As adjetivações do consentimento – "livre, informado e inequívoco", ou "livre, expresso e informado" – buscam exatamente garantir a autodeterminação informativa do titular de dados e os princípios constitucionais e infraconstitucionais já mencionados na presente ação.

Nesse sentido, e como extensão da necessidade de o consentimento ser inequívoco ou expresso, a LGPD estabelece que este deve ser concedido "por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (Art. 8º, caput), e o Marco Civil, ainda, que sua coleta deve "ocorrer de forma destacada das demais cláusulas contratuais" (Art. 7º, IX).

Em interpretação sistemática e principiológica do que se expôs até aqui, é nítida a impossibilidade de obtenção de consentimento válido no caso de acesso a celulares apreendidos em flagrante delito ou em abordagens policiais. Em primeiro lugar, não há que se falar em consentimento inequívoco ou expresso (tampouco por escrito), no caso de mero fornecimento de uma senha, e muito menos no caso de simples ausência de provas ou informações nos autos que apontem que ele não tenha sido concedido.

Em segundo, há também óbvios vícios na possibilidade de o consentimento ser livre e informado. Afinal, trata-se de situação de uso de forças policiais e de ambiente muito provavelmente intimidatório, onde é discutível a autonomia do indivíduo de livremente consentir com o uso de seus dados pessoais, não havendo nessa situação, ainda, possibilidade razoável de o titular ser informado suficientemente sobre que uso será feito de seus dados pessoais.

É nesse sentido o entendimento de "manifestação de vontade livre" no âmbito do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), regulação que inspirou a elaboração da LGPD brasileira. Segundo as diretrizes do Comitê Europeu de Proteção de Dados (European Data Protection Board), instância que reúne representantes das autoridades de proteção de dados do bloco europeu, o elemento "livre" na qualificação do consentimento implica uma verdadeira possibilidade de escolha e controle para os titulares dos dados. Complementa que, como regra geral, o GDPR "prevê que se o titular dos dados não puder exercer uma verdadeira escolha, sentir-se coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido".

Há um claro desequilíbrio de poder entre quem solicita acesso a informações pessoais e o titular dos dados, o que evidentemente compromete a validade do consentimento. De forma relacionada, o consentimento não é considerado como fundamento suficiente para autorizar o tratamento de dados pessoais para efeitos de prevenção, investigação ou repressão de infrações penais no âmbito da Diretiva da União Europeia 2016/680 (Law Enforcement Directive), destinada a regular o tratamento de dados pessoais para esses fins, o que se depreende do considerando 35 combinado ao artigo 8º da Diretiva.

Assim, o consentimento não pode servir de maneira a substituir a ordem judicial nesses casos. O argumento é especialmente fortalecido quando se considera o direito fundamental à não autoincriminação (Art. 5º, LVII da Constituição Federal). Afinal, não há que se falar em obtenção de consentimento para a finalidade de produzir provas contra si mesmo.

Essa linha argumentativa é defendida pelo próprio STF no referido HC 168052 de 2020. Ali, frisa-se a necessidade de ordem judicial como único meio válido de acesso a tais dados: "Essas medidas [de acesso a aparelhos telefônicos e a residência de suspeitos] **devem ser submetidas à prévia decisão judicial**, enquanto garantia procedimental in concreto através da qual sejam analisados e registrados, especificamente, os fundamentos que possam afastar os direitos fundamentais envolvidos. Ou seja, **a existência de prévia decisão judicial é capaz de demonstrar a necessidade, adequação e proporcionalidade da pretensão dos órgãos de segurança de acesso aos dados, informações e residência dos suspeitos**. Permite, ainda, o controle desses fundamentos" (*grifos nossos*).

IV.2. Do entendimento no âmbito da Convenção Americana de Direitos Humanos.

Como se viu, a jurisprudência dos tribunais superiores brasileiros exige ordem judicial para que a autoridade policial possa acessar dados contidos em dispositivos eletrônicos. Nesses termos, o entendimento do STF e do STJ está em consonância com os julgados da Corte Interamericana de Direitos Humanos (Corte IDH), como se passa a expor.

A proteção à vida privada é consagrada no art. 11 da Convenção Americana de Direitos Humanos, ratificada pelo Brasil em setembro de 1992 e promulgada pelo Decreto n. 678/1992. O art. 11.2 estabelece que ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou correspondência. Já o art. 11.3 garante a proteção da lei contra tais ingerências.

A jurisprudência da Corte IDH estendeu o entendimento de "correspondência" a outras formas de comunicação, como as conversas telefônicas, nos casos Tristán Donoso vs Panamá e Escher e outros vs Brasil [Tristán Donoso (parágrafo 55); Escher (parágrafo 114)]. Assim, a Corte IDH retomou o argumento de que o âmbito da privacidade se caracteriza por estar isento e imune às invasões e agressões abusivas ou arbitrárias por parte de terceiros ou da autoridade pública [Tristán Donoso (parágrafo 55); Escher (parágrafo 113)]. As restrições ao gozo e exercício do direito devem estar claramente previstas em lei (em sentido formal e material), perseguir um fim legítimo e cumprir os requisitos de idoneidade, necessidade e proporcionalidade, isto é, devem ser necessárias em uma sociedade democrática [Tristán Donoso (parágrafos 56 e 77); Escher (parágrafos 116 e 130)].

O acesso a dados armazenados em dispositivos eletrônicos apreendidos por forças policiais durante abordagens ou em flagrante delito implica uma ingerência no direito à privacidade, cuja dispensa de prévia ordem judicial não se adequa ao teste tripartite acima mencionado. A ingerência abusiva ocorre seja no acesso ao conteúdo de comunicações, seja na verificação de outros dados a elas associados.

Com efeito, no caso Escher e outros vs Brasil, a Corte IDH afirmou que a proteção do art. 11 da Convenção Americana compreende tanto conteúdo das comunicações quanto "qualquer outro elemento do processo comunicativo," como os dados que identificam uma comunicação (ex: registros de chamadas) [parágrafo 114]. A Corte IDH ressaltou, ainda, que a fluidez informativa existente na atualidade coloca o direito à vida privada das pessoas em uma situação de maior risco, "devido à maior quantidade de novas ferramentas tecnológicas e à sua utilização cada vez mais frequente," devendo o Estado "assumir um compromisso com o fim de adequar aos tempos atuais as fórmulas tradicionais de proteção do direito à vida privada" [parágrafo 115].

Diante do exposto, a Defensoria Pública do Estado de São requer que este MM. Juízo anule toda e qualquer prova obtida pela autoridade policial a partir do acesso irregular aos dados armazenados no dispositivo eletrônico do autor. Como se demonstrou de maneira ampla, a ausência de ordem judicial autorizando a medida implica em sua completa invalidade, em nome da privacidade, da intimidade, da

proteção dos dados pessoais, da presunção de inocência e do direito à não autoincriminação.

V. PEDIDOS

Ante o exposto, requer-se:

a. O deferimento dos benefícios da justiça gratuita, por se tratar de pessoa hipossuficiente e sem condições para arcar com as taxas e despesas processuais sem prejuízo de sua própria subsistência, nos termos do art. 98 e ss do CPC;

b. A observância das prerrogativas garantidas aos/às membros/as da Defensoria Pública, notadamente a intimação pessoal e a contagem em dobro de todos os prazos processuais previstas nos incisos I e II do artigo 128 da Lei Complementar 80/94, bem como no artigo 186, do Código de Processo Civil/2015;

c. O acolhimento das preliminares arguidas ...

d. Caso não se entenda pelo acolhimento das preliminares suscitadas, sejam, ainda assim, acolhidas as alegações de mérito, ...

e. Seja, ao final, julgado procedente/improcedente o pedido, por todas as razões de fato e de direito ora sustentadas.

Provará o alegado por todos os meios de prova em direito admitidos.

Termos em que espera deferimento.

Cidade, data.

NOME

Xª Defensoria Pública da Unidade xxx

Link - MODELO DE PEÇA