DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.2 >

DENNYS ANTONIALLI (ED.)
NATHALIE FRAGOSO (ED.)

GISELA AGUIAR WANDERLEY
JACQUELINE DE SOUZA ABREU
KÁTIA MARIA AMARAL JANGUTTA
MARIA LUCIANO
MANUEL MONTEIRO GUEDES VALENTE
RAFAEL F. MARCONDES DE MORAES

SÃO PAULO, 2019

INTERNETLAB
pesquisa em direito e tecnologia

DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.2 >

DENNYS ANTONIALLI (ED.)
NATHALIE FRAGOSO (ED.)

GISELA AGUIAR WANDERLEY
JACQUELINE DE SOUZA ABREU
KÁTIA MARIA AMARAL JANGUTTA
MARIA LUCIANO
MANUEL MONTEIRO GUEDES VALENTE
RAFAEL F. MARCONDES DE MORAES

SÃO PAULO, 2019

INTERNETLAB
pesquisa em direito e tecnologia

InternetLab é uma organização sem fins lucrativos dedicada à produção de pesquisa acadêmica aplicada com impacto em políticas públicas de tecnologia e Internet no Brasil.

Citação sugerida
ANTONIALLI, Dennys; FRAGOSO, Nathalie (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. II. São Paulo. InternetLab, 2019.

Avenida Ipiranga 344 cj 11B | 01046-010 | São Paulo | SP | Brasil
ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA
www.internetlab.org.br

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Direitos fundamentais e processo penal na era digital: doutrina e prática em debate / Dennys Antonialli, Nathalie Fragoso [editores]. -- São Paulo: InternetLab, 2019. -- (Doutrina e prática em debate; v. 2)

Vários autores.
Bibliografia.
ISBN 978-85-92871-02-4

1. Direito processual penal **2.** Direitos fundamentais **3.** Processo penal **4.** Tecnologia e direito **5.** Tecnologias da informação e comunicação **I.** Antonialli, Dennys. **II.** Nathalie Fragoso. **III.** Série.

19-28697 **CDU-343.1:004**

Índices para catálogo sistemático:
1. Direito e tecnologia : Direito processual penal **343.1:004**
Cibele Maria Dias - Bibliotecária - CRB-8/9427

AUTORES /

< DENNYS ANTONIALLI >

Doutor em Direito Constitucional pela Universidade de São Paulo. Mestre em Direito pela Stanford Law School, EUA. Mestre pela Bucerius Law School e WHU Otto Beisheim School of Management, Alemanha. Bacharel em Direito pela Universidade de São Paulo. Foi pesquisador visitante do Alexander von Humboldt Institute for Internet and Society e da Stanford Law School. Fundador e coordenador do Núcleo de Direito, Internet e Sociedade da Faculdade de Direito da USP (NDIS-USP). Foi professor doutor do Departamento de Direito do Estado da Faculdade de Direito da USP entre 2017 e 2018. É Diretor Presidente do InternetLab, centro independente de pesquisa em Direito e Tecnologia.

< GISELA AGUIAR WANDERLEY >

Mestra em Direito, Estado e Constituição pela Universidade de Brasília (2017). Graduada em Direito pela Universidade de Brasília (2014).

< JACQUELINE DE SOUZA ABREU >

Doutoranda em Direito na Faculdade de Direito da Universidade de São Paulo e advogada no Barroso Fontelles, Barcellos, Mendonça & Associados. Mestra em direito pela University of California, Berkeley (EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em direitos fundamentais. Graduada em direito pela Universidade de São Paulo. Foi pesquisadora-júnior na FGV DIREITO SP e assistente de pesquisa visitante do Berkman Klein Center for Internet and Society da Harvard University. Participou do Summer Doctoral Programme do Oxford Internet Institute e coordenou a área "Privacidade e Vigilância" no InternetLab, centro independente de pesquisa em direito e tecnologia.

< KÁTIA MARIA AMARAL JANGUTTA >

Desembargadora do Tribunal de Justiça do Estado do Rio de Janeiro. Mestra em Direito pela Universidade Gama Filho (UGF). Graduada em Direito pela Universidade do Estado do Rio de Janeiro (UERJ).

< MANUEL MONTEIRO GUEDES VALENTE >

Doutor em Direito pela Universidade Católica Portuguesa. Professor Associado da Universidade Autónoma Luís de Camões. Presidente do Instituto de Cooperação Jurídica Internacional. Professor Convidado do Mestrado e Doutorado em Ciências Criminais da PUC-RS. Professor Convidado da ESP/ANP – Polícia Federal. Investigador Integrado do Ratio Legis – Centro de I&D da UAL. É Of-Counsel da Rogério Alves & Associados – Sociedade de Advogados e Of-Counsel da Feldens-Madruga (Brasil).

< MARIA LUCIANO >

Mestranda em filosofia e teoria geral do direito pela Universidade de São Paulo, com graduação em direito pela mesma universidade. Durante a graduação, foi bolsista dos Programas de Tutoria Científico-Acadêmica e de Estímulo ao Ensino de Graduação (PEEG) da USP, e do Programa de Educação Tutorial (PET) – Sociologia Jurídica, do Ministério da Educação. Foi pesquisadora na FGV Direito SP e no InternetLab.

< NATHALIE FRAGOSO >

Doutora em Direito pela Universidade de São Paulo. Bacharela em Direito pela Faculdade de Direito da Universidade de São Paulo (2012). Coordenadora da área "Privacidade e Vigilância" no InternetLab, centro independente de pesquisa em Direito e Tecnologia.

< RAFAEL CARLSSON GAUDIO CUSTÓDIO >

Advogado e Pesquisador. Graduado em Direito pela Pontifícia Universidade Católica de São Paulo.

< RAFAEL FRANCISCO MARCONDES DE MORAES >

Doutorando e Mestre em Direito Processual Penal pela Faculdade de Direito da Universidade de São Paulo (USP). Professor concursado da Academia da Polícia Civil do Estado de São Paulo (Acadepol). Delegado de Polícia do Estado de São Paulo.

SUMÁRIO /

APRESENTAÇÃO DOS EDITORES /

A tecnologia tem impactado diretamente as atividades de investigação criminal. Com a multiplicação de dispositivos conectados à internet e o advento de diferentes tecnologias de vigilância, o dia-a-dia das autoridades de investigação passou a envolver não somente novas fontes de prova como também novas questões a respeito das possibilidades de obtenção e utilização para fins de instrução processual.

Para avançar o debate acerca das garantias do efetivo processo penal e da tutela de direitos fundamentais, como os direitos à privacidade e ao sigilo das comunicações em face das novas tecnologias, o InternetLab, centro independente de pesquisa em direito e tecnologia, com apoio institucional da Faculdade de Direito da Universidade de São Paulo (FDUSP), organiza, anualmente, o congresso "Direitos Fundamentais e Processo Penal na Era Digital".

A segunda edição do congresso, que aconteceu nos dias 20 e 21 de agosto de 2018, tratou especificamente dos métodos e estratégias das autoridades de investigação para a obtenção de dados armazenados e sua relação com as balizas impostas para a atuação da polícia nas ruas e nas redes. As palestras e intervenções dos participantes foram registradas e estão disponíveis para acesso online.

Esta obra reúne artigos e contribuições que, além de aprofundarem grande parte das discussões iniciadas durante o congresso, contribuem para a atualização das doutrinas jurídicas que se propõem a guiar os operadores do direito processual penal na era digital.

Boa leitura,
DENNYS ANTONIALLI
NATHALIE FRAGOSO
São Paulo, agosto de 2019

01.

PREFÁCIO: O PROCESSO PENAL NAS RUAS DO BRASIL

Rafael C. G. Custódio

Quando falamos em Direitos Fundamentais e Processo Penal na Era Digital, como muito bem problematizado pelo InternetLab em seus encontros anuais, é comum que nós, operadores do Direito, foquemos nas questões legalistas do assunto, privando-nos de refletir – e por isso propor – sobre os aplicadores das normas no dia-a-dia das ruas. No caso, os agentes das forças de segurança.

Esse aspecto é importante, porque nossas polícias, em especial a militar, são as agências de segurança mais produtivas do Estado. Estima-se que cerca de 90% das pessoas privadas de liberdade no país tenham sido presas em flagrante pelas polícias militares. Isso significa que Polícia Federal e Civis - estas sim idealizadas para investigar crimes, produzir provas e entregá-las para análise do Ministério Público - possuem papel lateral no cumprimento de seu papel. Significa, também, que se prende tão somente acusados de crimes menos graves e menos complexos, como o pequeno comércio ilícito de drogas, deixando de apurar as grandes redes criminosas, cada vez mais fortalecidas.

Em outras palavras, o processo penal nas ruas do Brasil é o das PMs estaduais, e não o dos gabinetes e fóruns. Nesse sentido, ao discutirmos, por exemplo, produção de provas e ações de investigação policial no país, e seu diálogo com aplicativos e celulares, é imperativo olharmos para essas instituições e suas práticas diárias, vez que é dali que praticamente todo o sistema penal se movimenta.

E o sistema se movimenta através de práticas cotidianas lastreadas na violência e ilegalidade como métodos centrais

/ NOSSAS POLÍCIAS, MAIS DE 30 ANOS DEPOIS DO REGIME DE EXCEÇÃO MILITAR, AINDA SÃO IDEALIZADAS PARA TRATAR O CIDADÃO COMO UM INIMIGO /

de consumação. Em geral jovens e adolescentes das classes baixas, moradores das periferias das cidades, são vítimas diárias de buscas pessoais – previstas em lei – que na prática significam presunção de culpa, tapas no rosto, chutes em todo o corpo, socos, ameaças, extorsão e, não menos raro, homicídios autuados nas hipóteses de excludente de ilicitude. Tudo isso, claro, sob o aval de um Judiciário de matriz autoritária, que acaba legitimando as práticas violentas das ruas.

Quando então discutimos novos procedimentos de investigação capitaneados por nossas polícias estaduais percebemos que o Direito, na verdade, pouco importa. Exemplos? O acesso ao celular do "suspeito" é livre, o acesso às mensagens de texto e ligações é livre, até mesmo a entrada no domicílio é livre; enfim, Constituição e processo penal não passam de distantes miragens. Esse material investigativo é então esquentado pelos agentes de segurança e merecerão, como já dissemos, a chancela de um judiciário que não se constrange em legitimar um sistema de investigação e repressão paralelo – desde que, claro, praticado contra os pobres do país.

Esta sistemática é uma das explicações pelas quais os índices de violência policial no país nunca arrefecem, o número de presos só aumenta, o perfil do preso segue o mesmo (jovem, negro, que vive em situação de vulnerabilidade) e não se investiga os crimes mais complexos.

No Brasil, parece que discorrer sobre as polícias que temos é assunto exclusivo de sociólogos e, eventualmente, de apresentadores de televisão, quando algum fato "explosivo" é consumado. No mais, os operadores do Direito fingimos que a doutrina, e mesmo a jurisprudência, tratam com forças policiais legalistas, técnicas, estruturadas e treinadas para garantir direitos (como, aliás, prega nossa Constituição Federal). Nada mais distante disso.

A bem da verdade, nossas polícias, em que pese terem passado mais de 30 anos do regime de exceção militar, ainda são idealizadas para tratar o cidadão comum como um inimigo potencial a ser eliminado. Essa ideologia belicista explica os índices alarmantes não só de letalidade policial como os episódios de violência cometidos contra a população civil.

Nesse contexto nada alentador seria preciso que fossem fortalecidos os mecanismos de controle da atividade policial, que o Ministério Público de fato exercesse seu papel constitucional de controle externo das polícias, que o Judiciário enfim absorvesse o texto constitucional e internacional de direitos como baliza intransponível de convencimento, que se combatesse com rigor a corrupção e abusos das forças de segurança, entre outras medidas.

Resumidamente, precisamos que o processo penal nas ruas do país se curve à legalidade.

02.

OS DIREITOS E GARANTIAS DOS CIDADÃOS INVESTIGADOS NA ERA DIGITAL[1]

Manuel Monteiro Guedes Valente

1. Agradecemos ao Doutor DENNYS ANTONIALLI e à Doutora MARTA SAAD pelo amável convite para participar deste evento científico do InternetLab e da Faculdade de Direito da Universidade de São Paulo. O texto que se publica corresponde em parte à conferência de abertura que proferimos no II Congresso Internacional – Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab e Faculdade de Direito da Universidade de São Paulo, no dia 20 de agosto de 2018. Foi escrito e corrigido respetivamente em São Paulo, 19 de agosto de 2018, no Maksoud Plaza (17:54), e Porto Alegre, 25 de março de 2019, no Radisson (18:50).

1. INTRODUÇÃO

Em primeiro lugar, queremos dar os parabéns à organização por este evento sobre um tema que nos deve ocupar nos próximos tempos: o Direito e o mundo digital. É importante que as Faculdades de Direito tenham centros de I&D sobre a internet – o digital – e o Direito, promovendo uma multidisciplinaridade científica e um diálogo entre os vários saberes.

Costumamos dizer aos nossos alunos que temos de começar a pensar a *teoria da infração* para a era e o mundo digital, para a nova realidade robótica e para os novos desafios que devemos enfrentar de modo a que possamos fazer *metamorfoses* [Beck] e não mudanças abruptas e sem qualquer fundamento lógico-jurídico-científico. As mudanças [abruptas] não respeitam a epistemologia, a teleologia, a axiologia e a sistemática da *ratio iuris*, mas tão-só da *ratio legis* da imperatividade inata à norma.

O centro de I&D InternetLab é um exemplo dessa preocupação: estudar o presente com as preocupações e os ensinamentos do passado e os olhos no futuro.

2. A METAMORFOSE JURÍDICA NECESSÁRIA

Falamos de Ulrich Beck por uma simples razão. Como sabem, os seus últimos escritos foram dedicados à *metamorfose do mundo*, obra que não terminou. Quis o destino que assim fosse, porque as metamorfoses não se extinguem nem se completam. As metamorfoses são contínuas e ocorrem dia-a-dia. Lembramo-nos de uma afirmação simples, mas profunda deste grande pensador, que passamos a citar:

> Os idosos nasceram como seres humanos, mas, como no romance Metamorfose, de Kafka, acordaram de manhã como insetos chamados "analfabetos digitais". As gerações mais jovens, ao contrário, já nasceram como "seres digitais". O que foi acondicionado na palavra mágica "digital" tornou-se parte da sua "bagagem genética" (Beck 2018: 242).

Duas questões são, desde já, de salientar: se os *insetos digitais* continuam seres humanos, *i. e.*, se pensam e agem como seres humanos; e se é possível olhar para os *seres digitais* como seres humanos ou se lhes resta um pouco de humanidade. Estas duas questões estão intimamente ligadas com o Direito como ciência do ser humano e como dimensão material da justiça.

A esquizofrenia digital, por um lado, tem destruído a lógica racional dos problemas inerentes ao Direito penal – *v. g.*, quanto aos elementos da ação [humana], tipicidade, ilicitude, culpabilidade [inexigibilidade de conduta diversa][2] e punibilidade[3] –, ao Direito processual penal – *v. g.*, validade da prova recolhida de uma base ou de uma rede de contatos e correio de e-mails de uma empresa – e ao Direito penitenciário – *v. g.*, a restrição em ações disciplinares por os presos efetuarem comunicações não autorizadas ou filmagens e postagens por meio de aparelhos celulares não autorizados.

2. Quanto à discussão da inexigibilidade como causa de exclusão da culpa e da ilicitude, da responsabilidade pelo facto, Jorge de Figueiredo Dias. Direito Penal. Parte Geral – Tomo I. Questões Fundamentais. a Doutrina Geral do Crime. 2ª Edição. Coimbra: Coimbra Editora, 2007, pp. 278-280, 602- 627 (604-606), 963-964.

3. Cf. Jorge de Figueiredo Dias. Direito Penal. Parte Geral – Tomo I.... 2ª Edição, pp. 237-238.

Mas no espaço do Direito processual penal [e em parte no penitenciário] o efeito esquizofrênico é sobremaneira superior: *p. e.*, uma postagem em rede social de que o cidadão *A* ou *B* praticou um determinado crime tem mais valor do que uma decisão judicial e tem o efeito condenatório imediato daquele ser humano mesmo que não tenha cometido o crime de que é acusado na postagem. É condenado e morre para a vida em sociedade. Os insetos *analfabetos digitais* assimilam esta doutrina demolidora e *assumem como facto um não facto*, porque o seu *analfabetismo tolhe-lhes a capacidade de raciocínio e de pensamento límpido sobre os factos* como aconteceu com o inseto de Kafka.

Os *seres digitais* são, por outro lado, *geneticamente estruturados para o domínio do digital sobre si mesmos: vivem nele e dele não saem*; são uma íntegra parte do mundo – era – digital, *i. e.*, são a *sociedade internético-personocêntrica*[4].

Como olham desse mundo para os valores que nos regem e como vão reger o futuro segundo valores que não têm expressão sistemática e axiológica, os algoritmos e os bites geram, assim, uma nova normatividade *acientífica*[5] e, em consequência, *assistemática*, *ateleológica* e *axiologicamente desraizada*.

Entremos mais nas questões do nosso tema em concreto e que nos têm preocupado nos últimos tempos, como, por exemplo, refletimos no artigo publicado na revista *Corpus Delicti* dedicado a: *O Reforço dos Princípios Constitucionais na Obtenção de Prova no Mundo Digital*[6].

4. Construímos este tópico científico-filosófico-jurídico há mais de cinco anos, tendo a sua primeira fundamentação no nosso Os Desafios do Processo Penal do Estado Democrático de Direito: A Sociedade Internético-Personocêntrica. Disponível em: http://www.ibadpp.com.br/1773/, 2014.

5. Construção retirada da teoria da acientificidade da tecnologia despida de valores e de princípios científicos apresentada por Jürgen Habermas. Técnica e Ciência como "Ideologia". Tradução do alemão Technik und Wissenschaft als «Ideologie» de Artur Mourão. Lisboa: Edições 70, 2006.

6. Cf. o nosso O (reforço dos) princípios constitucionais na obtenção de prova no mundo digital. Uma necessidade premente. In: Corpus Delicti – Revista de Direito de Polícia Judiciária. ano 2, N. 3. jan-jun 2018, pp. 11-25.

Vivemos uma metamorfose da vida, em que nos devemos preocupar em retirar positividade dos males e das coisas menos benéficas, ou seja, tratar dos "efeitos colaterais positivos dos males" (Beck 2018: 16). E, por isso, temos de deixar o metodismo jurídico de que tudo gira à volta do Direito – como a ideia ancestral de que o sol girava à volta da terra – e olhar os demais saberes científicos.

O mesmo se passa dentro do Direito, em que as áreas do saber se conflitam e se fecham sobre si mesmas e não conseguem ver que a *ciência jurídica é uma unidade de um todo, é um só sistema* – unidade de um todo[7] – e não vários sistemas; impondo-se, desta feita, que a *ratio iuris* impere (Canaris[8]) e se abandone a ideia de que o caminho a percorrer é de mudança, quando na verdade é [deve ser] de metamorfose porque se exige que se subsuma esta nova dinâmica paradigmática aos valores e à sua concordância prática de modo a que não se desague em extremos positivistas – validade total da prova ou invalidade total da prova – e, nessa medida, promovamos uma justiça inexistente [ou injustiça premente e existente] ou a violação do direito à justiça como um dos mais sagrados valores da democracia[9]. A mais que este evento, salvo erro nosso, integra-se no projeto *Privacidade e Vigilância* do InternetLab, mas não deve ser alheado dos demais projetos, em especial do *Liberdade de Expressão*, onde, em Portugal, tem surgido uma crescente pendência jurídico-criminal e jurídico-civil. Vejamos.

7. Seguindo o pensamento de Emanuel Kant, inscrito na Crítica da Razão Pura, de que sistema é a unidade dos diversos conhecimentos de e numa ideia, Michael Pawlik considera sistema como uma ciência de um todo racional coerente interno organizado. Cf. Michael Pawlik. Teoria da ciência do direito penal, filosofia e terrorismo. Tradução do alemão de Eduardo Saad-Diniz. São paulo: LiberArs, 2012, pp. 11-13.

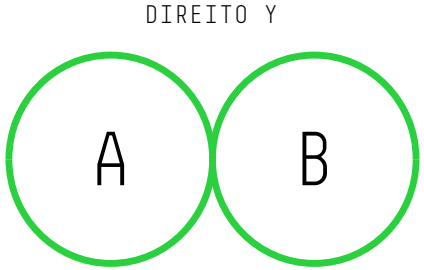
8. Claus-Wilhelm Canaris. *Pensamento Sistemático e Conceito de Sistema na Ciência do Direito*. Tradução do alemão Systemdenken und *Systembergriff in der Jurisprudenz* de António Menezes Cordeiro. 4ª Edição. Lisboa: Fundação Calouste Gulbenkian, 2008.

9. Acompanhamos Jacques Derrida no sentido de podemos ter justiça sem democracia, mas nunca teremos democracia sem justiça. Cf. Jacques Derrida. Força de lei: *o fundamento místico da autoridade*. São Paulo: M. Fontes, 2010.

3. A FALSA IDEIA DE QUE TUDO SE PODE: A RESTRIÇÃO DE DIREITOS

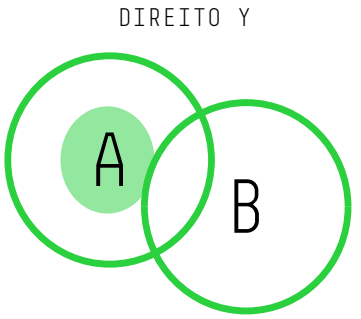
Hoje as pessoas pensam que podem escrever e dizer tudo nas redes sociais por considerarem que estão em um Estado de [total] liberdade de expressão, olvidando, assim, que os limites se extinguem com a afirmação de cada um dos nossos [seus] direitos fundamentais pessoais. O direito de liberdade de expressão e o direito de e à informação não são ilimitados. Aceção que muitas vezes os seres digitais esquecem e embarcam na onda que todos pensam conseguir surfar.

A afirmação de cada um dos nossos direitos fundamentais pessoais tem, *ab initio*, um limite inexorável: o direito dos demais seres humanos que, como valores vitais e essenciais à vida em comunidade [bem jurídico] não podem ser lesados ou colocados em perigo de lesão. O exercício de direitos deve ocorrer em plena harmonia e em equilíbrio – equidade – sob pena de negarmos o sistema assente na construção de garantia, de segurança e de coesão social. *A* e *B* devem exercer o seu direito *Y* em pleno respeito pela liberdade um do outro sob pena de entrarmos em esferas jurídicas de inadmissível intrusão. Veja-se a imagem sequente que representa a convivência harmoniosa em sociedade dos sujeitos *A* e *B* independentemente de estarmos ou não na era digital, cujos espaços de domínio devem ser respeitados e cultivados sob pena de lesarmos ou colocarmos em perigo de lesão esse direito, valor e bem jurídico *Y*.



Mas sabemos que nem sempre a vida se rege segundo este padrão sistêmico e que é necessário entrarmos no domínio do direito *Y* de *A* ou de *B*. Mesmo admitindo-se uma restrição do direito *Y*[10] de *A* e de *B*, nunca essa restrição pode ferir o núcleo central do direito *Y* de qualquer um dos sujeitos em confronto, sob pena de negarmos esse direito *Y* ao titular em restrição [*A* ou *B*]. O núcleo desse direito *Y* é o designado mínimo ético, valor inexorável, inabalável e inalienável pelo seu titular [sob pena de se negar a ordem jurídica de um Estado], é o espaço -fragmento – do bem jurídico tutelado [ou a tutelar], por dignidade e carência, pelo direito penal.

10. Falamos em restrição de direitos em respeito pelo consagrado artigo 18º [nº 2] da CRP, sendo que, em democracia, não podemos nem é admissível falar em suspensão de direitos, mas sim em suspensão do exercício de direitos [artigo 19º da CRP].



Uma das questões que se levantam, desde logo e em termos criminais, é saber se a *postagem* de um comentário lesivo de um bem jurídico de uma pessoa – singular/física ou coletiva/jurídica – *pode ou não servir de prova em sede de processo-crime*. Este dilema também se coloca, nas empresas ou nas entidades públicas, em sede de procedimento disciplinar.

O busílis da questão está no *modus operandi* da obtenção de prova e da sua inserção processual. A doutrina e jurisprudência portuguesa e alemã consideram, majoritariamente, que essa postagem pode ser fundamento da *notitia criminis*. As autoridades policiais e judiciárias podem admitir a inserção dessa postagem como início do processo-crime e respetiva investigação criminal, mas não podem considerar, logo de imediato, que estamos perante uma *lesão a um bem jurídico* praticada por uma determinada pessoa, e *produzida por um determinado perfil da rede em que se encontra*. Apesar de existir uma preocupação das redes sociais, plataformas informáticas, por meio p. e. das URL[11], em saber e conhecer a identidade do registo, é de relembrar que *nem sempre o perfil corresponde ao verdadeiro ser humano identificado* como *A* ou *B* ou *C*. Muitas vezes estamos perante *um sistema de espelhos de postagem* [ou sistema de postagem em espelho], em que a imagem que aparece é distorcida em relação à imagem real e original, em que a imagem pública e fonte de relações jurídicas digitais não corresponde à imagem real. Esta operação ilícita pode configurar uma conduta criminógena de *manipulação [com prévio furto] de identidade e de perfil*, assim como *utilização indevida do perfil ou da identidade* de uma determinada pessoa, podendo enquadrar o tipo legal de crime de *falsidade informática*, previsto e punido pelo artigo 3º da Lei do Cibercrime[12], podendo, assim, gerar uma *lesão ou colocar em perigo de lesão a segurança das relações jurídicas produzidas por meio informático e digital*. Esta factualidade [sistema de espelho] será [ou terá de ser] apurada pela perícia [informática] científica.

11. Sigla que significa *Uniform Resource Locator*, i. e., Localizador Uniforme de Recurso, que é o endereço disponível em uma rede

12. Aprovada pela Lei nº 109/2009, de 15 de setembro, que transpôs para a ordem jurídica portuguesa a Decisão Quadro nº 2005/222/JAI, do Conselho Europeu, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre o Cibercrime do Conselho da Europa.

Como notícia do crime é admitida a sua inserção no processo. Outra coisa é saber se essa imagem digitalizada ou impressa junto ao processo-crime pode ser utilizada como prova contra uma determinada pessoa física ou jurídica suposta autora do *post*[13].

13. O Tribunal da Relação do Porto decidiu que a prova da **titularidade da conta do Facebook** e o **conteúdo** na mesma divulgado **não obedece a qualquer princípio de prova legal de natureza digital**, a obter através da pesquisa de dados informáticos e sua apreensão, mas apenas submetido ao **princípio da livre apreciação da prova** [Ac. TRP de 13.09.2017]. Itálico e negrito nossos.

4. DA NOTÍCIA DO CRIME E RESPECTIVA PRESERVAÇÃO DA PROVA: A TUTELA JURISDICIONAL [E NO MÍNIMO JUDICIÁRIA] DOS DIREITOS DOS VISADOS. QUESTÕES PREMENTES

No mínimo três situações distintas podem ocorrer e que são importantes em termos de tutela dos direitos da personalidade e direitos fundamentais pessoais, consagrados constitucionalmente: (*i*) uma coisa é a vítima ter acesso direto a esse *post*; (*ii*) outra coisa é ter acesso ao mesmo por interposta pessoa; e, ainda, (*iii*) outra é ter acesso ou conhecimento de que existe um *post* lesivo dos seus direitos fundamentais pessoais a circular e a ser comentado numa rede social. Aqui também se pode colocar ou avocar a *autotutela jurídica*, mas não a iremos tratar nesta sede.

Quanto à primeira (*i*) situação – a vítima [ofendido] tem acesso direto ao *post* porque integra o grupo da rede –, a mesma tem o direito de apresentar uma denúncia criminal e entregar a imagem ou o vídeo lesivo dos seus direitos para que se fundamente a comunicação de um crime. O ofendido[14] tem o

14. Entenda-se ofendido aquele que é titular do direito – bem jurídico – lesado com uma conduta humana, ou na letra da lei «o titular dos interesses que a lei especialmente quis proteger com a incriminação», nos termos do artigo 113.º do CP e dos artigos 67.º-A e 68.º, n.º 1, alínea a) do CPP, ambos portugueses.

direito de dispor da informação base do crime de que é vítima e de as fornecer no ato da denúncia. Consideramos que estamos no quadro da auto disposição do domínio informativo e não necessita de qualquer autorização judicial para a fornecer às autoridades públicas: polícia e judiciário. Assim entendeu o Tribunal da Relação de Guimarães quando decidiu que a *transcrição de mensagens SMS do telemóvel de um queixoso que espontaneamente as fornece, pode valer como prova, apesar de não ter sido ordenada pelo juiz. Só será necessária a intervenção do JIC quando quem fornece aquelas mensagens não puder dispor delas*[15].

15. Cf. o Ac. TRG de 15.04.2012.

Na segunda situação, (*ii*) o acesso ao *post* ou vídeo lesivo é indireto, pelo que dever-se-á optar por comunicar às autoridades policiais e judiciárias o *factum criminis* de modo a desenvolverem as diligências adequadas à aquisição do elemento material lesivo dos bens jurídicos penalmente tutelados; cabendo àquelas o dever de levantar um auto de notícia criminal e solicitar à autoridade judiciária competente o devido mandado de busca e apreensão digital[16]; mas, neste caso e avocando-se o princípio da *concordância prática* que implica a verificação de determinados pressupostos da aquisição da notícia criminal – *v. g.*, a indispensabilidade investigatória e a certeza de que a mesma prova seria obtida pelos meios normais de obtenção de prova –, não nos parece negativo ou ilegal que esse *post* ou vídeo possa ser entregue por esse outrem àquelas autoridades ou à própria vítima para que esta lhes dê o devido

16. Veja-se que o Tribunal da Relação do Porto já decidiu que a "jurisprudência tem equiparado as mensagens SMS às cartas de correio, distinguindo se ainda estão fechadas ou se foram já abertas pelo destinatário. Porém, a Lei do Cibercrime alterou esta abordagem: a **leitura de mensagens guardadas num cartão de telemóvel por um agente policial sem autorização do seu dono ou do JIC é prova proibida, em nada relevando que as mesmas tivessem sido ou não abertas e lidas pelo destinatário pois que a lei não distingue entre essas duas situações"**. Cf. o Ac. TRP de 12.09.2012. Negrito e itálico nossos. Esta mesma jurisprudência aplica-se ao conteúdo das redes sociais gravado em um celular.

/ O ARGUMENTO DE QUE AS PRÓPRIAS PESSOAS SE EXPÕEM NAS REDES SOCIAIS NÃO DIMINUI A FORÇA JURÍDICA DOS SEUS DIREITOS FUNDAMENTAIS /

/ TEMOS DE COMEÇAR A PENSAR A TEORIA DA INFRAÇÃO PARA A ERA DIGITAL, PARA QUE POSSAMOS FAZER METAMORFOSES E NÃO MUDANÇAS ABRUPTAS /

encaminhamento: conhecimento às autoridades policiais e judiciárias[17].

Quer na primeira situação, quer na segunda situação, em especial quando o terceiro ou a vítima é que comunicam a notícia criminal, as autoridades policiais devem solicitar o devido mandado de busca e apreensão digital de modo a garantir a originalidade e integridade do elemento material constitutivo do crime: originalidade e integridade dos elementos probatórios. Impõe-se, nestes casos, que a lacragem da apreensão do material informático, gravado em CD, ou outro equipamento digital, ou do aparelho detentor da matéria objetiva dos tipos de crime seja efetuada e a cadeia de custódia da prova não seja quebrada[18].

Quanto à terceira situação, (*iii*) as autoridades policiais devem, após o conhecimento da notícia de que, na rede *A* ou *C*, se encontra um *post* ou um vídeo lesivo de bens jurídico-criminais dignos de tutela jurídico-criminal, solicitar os devidos mandados de busca e apreensão digital de modo a poderem salvaguardar a prova legítima, legal e lícita. Cabe, também, prover que a cadeia de custódia de prova não seja violada sob pena de se inutilizar a prova obtida de forma leal e democrática. Mas se houver urgência na preservação e cautela daquela prova, as autoridades policiais podem ordenar ao serviço ou entidade respectiva a *preservação dos dados ou informações essenciais à prova* até que haja o devido mandado de busca e apreensão

17. Veja-se que o Tribunal da Relação do Porto decidiu que:

"I. O Facebook é uma rede social que funciona através da internet, operando no âmbito de um sistema informático pelo que a recolha de prova está sujeita à Lei do Cibercrime – DL 109/2009 de 15/9.

II. **Constitui prova legal a cópia de informação que alguém publicita no seu mural do Facebook sem restrição de acesso**.

III. Só está sujeita à disciplina do **artº 16º 1 e 3 da Lei do Cibercrime a apreensão da informação original inserta na plataforma, esteja ou não disponível".**

Cf. o Ac. TRP de 05.04.2017. Negrito nosso.

18. O STF, em apreciação de habeas corpus, admitiu que, mesmo que haja violação da cadeia de custódia da prova, por meio da quebra do lacre e visualização do conteúdo dos ficheiros, se for por pouco tempo e não se tiver alterado a prova, esta, constante das fitas violadas, pode e deve ser admitida como válida em sede de processo-crime.

digital, nos termos do nº 2 do artigo 12º da Lei do Cibercrime[19]. Esta medida fica sob o regime de confidencialidade por parte da entidade notificada, ou seja, esta assume-se como *fiel depositário* da informação essencial à prova.

Veja-se que as autoridades policiais podem, do mesmo modo, atuar se estivermos no âmbito de pesquisa de dados informáticos essenciais à produção de prova no futuro em sede de julgamento, como determina o artigo 15º da Lei do Cibercrime[20]; ou seja, desde que se verifiquem as *causas de justificação* – alíneas *a*) [*consentimento*] e *b*) [*estado de necessidade justificante* ou *legítima defesa* ou *direito de necessidade*] do 3º do artigo 15º da Lei do Cibercrime –, sejam cumpridas as formalidades de *controlo jurisdicional* [garantia] por meio da comunicação à autoridade judiciária[21] – alíneas *a*) e *b*) do nº 4 do artigo 15º da Lei do Cibercrime –, assim como o *princípio da especialidade* do fundamento da autorização judicial – nº 5 do artigo 15º da Lei do Cibercrime.

Como se pode verificar, as policiais criminais detém instrumentos jurídicos suficientes para procederem à aquisição, conservação e tratamento da prova obtida no meio digital. Sendo que atuam sob a égide das designadas *medidas cautelares e de polícia*, extraordinárias, urgentes e *periculum in mora*, cabendo-lhes comunicar de imediato a sua atividade às autoridades judiciárias: Ministério Público e Juiz das Liberdades. O mesmo se passa no quadro das *apreensões digitais*, como decorre do artigo 16º da Lei do Cibercrime[22], com exceção de apreensões que tenham ou visam como foco a atividade ilícita de *advocacia, médica, bancária* e *jornalística* ou conflitem com estas atividades. Temos, aqui, uma *tutela jurídico-constitucional reforçada* que não pode se postergada apenas porque estamos no âmbito digital.

Desde já somos da opinião de que o nº 1 do artigo 16º da lei do Cibercrime obedece ao regime exposto no artigo 187º, nº 1 do CPP português, submetendo a pesquisa – busca – informática e a apreensão dos dados ao princípio da indispensabilidade para a *descoberta da verdade* e da impossibilidade objetiva de obter prova por meio menos oneroso. Só uma unidade normativa e hermenêutica podem trazer segurança jurídica ao sistema como um todo organizado racionalmente.

Mas a regra é sempre, como determina o CPP e o comando constitucional – artigo 32º, nº 4 da CRP –, a prévia autorização da autoridade judiciária: *v. g.*, Juiz de Instrução Criminal.

Consideramos que estamos perante uma questão de *inconstitucionalidade material* quanto aos artigos que admitem que basta a autorização do Ministério Público para aceder e apreender a informação e dados dos sistemas digitais, quando, estando perante uma ofensa ou restrição de direitos fundamentais pessoais – reserva da intimidade da vida privada e familiar, palavra escrita e falada, imagem, artigo 26º da CRP –, a autorização deve ser judicial, fundamentada e exige que exista previamente um processo-crime [artigos 26º, nº 2, 32º, nº 4, 34º, nº 4, 35º e 205º da CRP].

É um tema que tem de ser discutido, porque o argumento de que se as próprias pessoas de livre e espontânea vontade expõe a sua vida particular nas redes sociais e nas comunicações digitais, elas autodiminuem a força jurídica tutelante dos seus direitos fundamentais pessoais, não colhe e é contrária ao

19. **Artigo 12º – Preservação expedita de dados**: (...) 2 - A **preservação** pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou **quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária** e transmitir-lhe o relatório previsto no artigo 253º do Código de Processo Penal. (...)

20. Artigo 15º da Lei do Cibercrime. Disponível em https://bit.ly/2RWytAd

21. Autoridades judiciárias em Portugal são os juízes, os juízes de instrução criminal e os magistrados do Ministério Público, por força da al. b) do artigo 1º do CPP português.

22. Artigo 16º da Lei do Cibercrime. Disponível em https://bit.ly/2RWytAd

próprio artigo 18º, nºs 2 e 3 da CRP. São dimensões distintas e díspares que não podem ser confundidas: uma é a autodeterminação expositiva; a outra é essa informação própria da sua autodeterminação expositiva ser fundamento de prova criminal. A pessoa expõe, não autoriza a utilização dessa informação ou desses dados para fins criminais, ou seja, não presta prévio consentimento, não produz uma declaração de ciência e de vontade. A postagem ou a colocação do vídeo não é uma declaração de vontade, mas tão-só uma declaração de ciência.

Mas há outros pontos que merecem a nossa preocupação. Desde logo a *admissibilidade* por alguma doutrina – mais policial e/ou de teor securitária e belicista – e por alguma jurisprudência de as *fontes digitais*, em especial as redes sociais de acesso e uso maciço pelas pessoas descuidadas e alienadas do mundo real e jurídico, como (*i*) *fontes de informação policial*, (*ii*) *convertidos em fontes de obtenção de prova* e o (*iii*) *resultado dessa recolha subsumir-se como prova penal*.

No que respeita às redes abertas como *(i) fontes de informação policial*, desde que a rede aberta seja de acesso comum e não seja uma rede de acesso restrito, em que qualquer ser humano à face da galáxia pode consultar e ler as postagens e ver os vídeos ou outra informação ou dados disponíveis, considera-se que não haverá problemas de legalidade e licitude desde que a mesma não configure meio de prova ou prova. Mas se estivermos no quadro de informação e dados de acesso restrito a um grupo de pessoas singulares ou coletivas, cuja partilha daquela assenta na base de confiança, de relações profissionais, de relações universitárias, políticas, religiosas ou de outra índole, o acesso policial só devia ser admissível por meio de uma autorização judicial – juiz –, uma vez que estamos perante um *infiltração policial* que deve merecer os maiores cuidados de fiscalização prévia e de controlo contínuo da atuação dos elementos policiais. Caso assim não seja, consideramos que estamos perante a obtenção de informação de forma antidemocrática, desleal, ilegítima e ilegal, quiçá ilícita, cuja admissibilidade deve ser vetada e a valoração proibida, assim como toda a prova que tiver sido obtida por meio dessas informações policiais legalmente viciadas não deve ser admitida nem valorada.

As redes abertas *(ii) convertidas em fontes de obtenção de prova* é, em absoluto, de rejeitar. Uma coisa são as situações próprias de urgência e *periculum in mora* – medidas cautelares e de polícia no âmbito criminal –, outra coisa são as redes abertas como fonte natural e legal de obtenção de prova em que as pessoas se autoincriminam sem o saberem ou se autoincriminam por instigação de membros ou, até mesmo, do elemento policial, atuando como agente encoberto[23]. Falamos aqui em agente encoberto porque o elemento policial está dentro de uma rede digital totalmente aberta, em que a sua função é apurar se está ou vai ocorrer um crime para promover uma ação imediata de *terminus* da ação criminal. O agente policial não tem a função de recolher prova e de se dar a conhecer aos demais membros da rede ou plataforma digital, mas tão-só a de estancar um crime que possa ocorrer no espaço digital ou naquele espaço digital.

23. Mas que passa a ser provocador/instigador e autor mediato do crime [artigo 26º do CP português].

Se a rede for restrita ou fechada, a ordem jurídica considerada no seu todo impõe que a atuação do agente policial revista a figura do *agente infiltrado*, que tem a função de ganhar a *confiança dos demais membros do grupo restrito ou fechado*, cujo acesso até pode ser livre, mas o contato e a assimilação de informação restrita, e possa *obter informações* e, por esse método, possa *obter meios de prova* ou *provas* destinadas a *prevenir* e a *reprimir crimes*. Parece ser este o entendimento que se retira do artigo 19º da Lei do Cibercrime[24].

24. Artigo 19º da Lei do Cibercrime. Disponível em https://bit.ly/2RWytAd

O recurso ao agente infiltrado, de acordo com a lei portuguesa, para fins de *repressão criminal* – investigação criminal –, carece de autorização do Ministério Público e posterior ratificação do Juiz de Instrução Criminal – o que desde já merece a nossa crítica por estar ferido de inconstitucionalidade material (artigo 32º, nº 4 da CRP) – e, para fins de *prevenção criminal*, carece de autorização do Juiz de Instrução Criminal. Estamos a falar de um dos meios ocultos de obtenção de prova que devia sempre merecer sempre a prévia tutela jurisdicional: *i. e.*, prévia autorização judicial e fundamentada.

Este dispositivo legal coloca dúvidas porque remete para dois regimes diferenciados: por um lado e nos termos do nº 1, o recurso ao agente infiltrado segue o regime previsto na lei do agente infiltrado físico [Lei nº 101/2001, de 25 de agosto], mas, por outro e nos termos do nº 2, se for necessário recorrer a meios e dispositivos informáticos, o regime a seguir é o previsto para as interceptações de comunicações [artigos 187º a 190º do CPP].

Como temos defendido a autorização de recurso a agente infiltrado – quer para investigação quer para prevenção criminal – é da competência do Juiz das liberdades, por força do nº 4 do artigo 32º da CRP[25]. Mas o legislador ordinário decidiu que o Ministério Público pode autorizar o recurso ao agente infiltrado, desde que já esteja em curso um processo crime – com a finalidade de investigação criminal –, cabendo-lhe comunicar ao JIC para que este, em 72 [setenta duas] horas derrogue ou ratifique a autorização do MP. Acresce que a ratificação pode ser tácita, nos termos do nº 4 do artigo 3º da Lei nº 101/2001. Este regime, segundo uma interpretação literal das normas – em especial da previsto no nº 1 do artigo 19º da Lei do Cibercrime –, admite que o recurso ao agente infiltrado digital seja ou possa ser autorizado pelo Ministério Público, interpretação normativa esta que consideramos ser materialmente inconstitucional por violação do nº 4 do artigo 32º conjugado com o nº 2 do artigo 18º, ambos da CRP[26].

25. Cf. o nosso *Teoria Geral do Direito Policial*. 5ª Edição. Coimbra: Almedina, 2017, pp. 595-597.

Mas a autorização do agente infiltrado digital para efeitos de prevenção criminal carece sempre de autorização judicial – JIC – por força do nº 5 do artigo 3º da Lei nº 101/2001 conjugado com o nº 1 do artigo 19º da Lei do Cibercrime[27].

26. Cf. o nosso *Teoria Geral do Direito*. 5ª Edição, p. 596.

Contudo, se existir necessidade na prossecução de implementar o agente infiltrado digital e recorrer a meios e dispositivos informáticos, o regime vigente é o da interceptação de comunicações, previsto os artigos 187º a 190º do CPP. Amplia-se e efetiva-se a *tutela jurisdicional*, exige-se a autorização judicial – JIC –, e devem observar-se todos os *pressupostos formais e materiais* da interceptação de comunicações, em especial a *indispensabilidade para a descoberta da verdade* e a *impossibilidade objetiva de obter prova por meio menos oneroso*[28]. Temos, aqui, um regime híbrido que pode gerar [gera] conflitualidade normativa e insegurança jurídica, que impõe avocar-se a melhor conformidade com a Constituição de modo a evitar interpretações normativas materialmente inconstitucionais.

27. Cf. o nosso ***Teoria Geral do Direito***. 5ª Edição, pp. 596-597.

28. Cf. *caput* do nº 1 do artigo 187º do CPP.

É de frisar que o *catálogo* de crimes âmbito de admissibilidade do recurso ao agente infiltrado digital é (*i*) *fechado* quanto à alínea *a*) e segunda parte da alínea *b*), ambas do nº 1 do artigo 19º da Lei do Cibercrime – *os previstos na presente lei* [falsidade informática (artigo 3º); dano relativo a programas ou outros danos informáticos (artigo 4º); sabotagem informática (artigo 5º); acesso ilegítimo (artigo 6º); intercepção ilegítima de programa protegido (artigo

7º); reprodução ilegítima de programa protegido (artigo 8º)] e os *crimes contra a liberdade e autodeterminação sexual* nos casos em que os *ofendidos* sejam *menores ou incapazes*, a *burla qualificada*, a *burla informática e nas comunicações*, a *discriminação racial, religiosa ou sexual*, as *infrações económico-financeiras*, bem como os *crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos* –, (*ii*) *(semi)aberto* quanto à alínea *b*) do mesmo preceito – os cometidos por meio de um sistema informático – e (*iii*) *modal* como se retira das expressões «pena de prisão de máximo superior a 5 anos» e «ou, ainda que a pena seja inferior, *sendo dolosos*» prevista nessa mesma alínea do mesmo preceito. Como se pode verificar não existe uma consistência sistemática legiferativa, porque reina uma deficiente técnica legislativa pela inexistência de legística.

Do mesmo modo e na mesma linha de raciocínio, consideramos a rede social aberta como fonte originária do *(iii) resultado da recolha de informação e dados de um determinado crime subsumir-se como prova penal*, mesmo que a rede não seja restrita ou fechada. Nesta terceira dimensão de acesso e recolha de prova em redes abertas, a admissibilidade desta só é possível se for precedida de uma autorização judicial e, consequentemente, a respetiva valoração em sede de julgamento. O argumento de que a recolha foi efetuada em uma rede aberta ou aberta restrita ou fechada porque o cidadão escreveu ou disponibilizou um vídeo autoincriminatório não colhe nem deve em um Estado democrático de direito ter qualquer aceitação. Caso assim não ocorra estamos perante uma clara proibição de prova, nos termos do artigo 126º, nºs 1 e 3 do CPP e artigo 32º, nº 8 da CRP.

5. A TUTELA JUSCONSTITUCIONAL REFORÇADA E OS PRINCÍPIOS GARANTIA DOS DIREITOS DOS VISADOS

É de frisar que, como *tutela jurídico-constitucional reforçada* do ser humano na persecução criminal, o requerimento do Ministério Público a pedido ou solicitação da Polícia criminal e o despacho do Juiz que autoriza a infiltração deve estar *fundamentado* – artigo 205º da CRP e artigo 97º do CPP – e, a par dos demais pressupostos materiais e processuais, assim como princípios constitucionais, deve ser demonstrado que estamos perante uma *indispensabilidade para a descoberta da verdade* e uma *impossibilidade objetiva de obtenção de prova por meio de obtenção de prova menos oneroso* para o núcleo de direitos e garantias constitucionais e processuais penais do cidadão visado com a diligência e dos demais cidadãos que com ele se relacionam.

Importa, ainda, relembrar que não basta a recolha da prova ou do meio de prova no espaço digital. Impende sobre as autoridades judiciárias a obrigação de determinar a *perícia ao discurso e ao método difusivo de informação e de dados* sob pena de podermos estar a incriminar uma pessoa que, não obstante lhe ter sido atribuído um perfil e ser utilizado o seu IP, não escreveu, não postou nem colocou qualquer vídeo na rede social. A perícia do discurso ou do método difusivo – perfis digitais – é de extrema importância na tutela e na defesa de inocentes.

Antes de finalizarmos, gostaríamos de afirmar um pequeno *catálogo de princípios, direitos e garantias* que o ser humano deve manter inabaláveis no *mundo digital* quando comete um crime por este meio ou o difunde no espaço digital:

(i) Os *princípios constitucionais processuais penais* mantêm a sua *validade*, *vigência* e *efetividade* no espaço digi-

tal: princípio da constitucionalidade e da legalidade penal material e processual; princípio da reserva de constituição; princípio da proporcionalidade ou da proibição do excesso; princípio da separação de funções ou da estrutura acusatória do processo; princípio da reserva de juiz ou da jurisdicionalidade; princípio da fundamentação das decisões judiciais e judiciárias; princípio *ne tenetur se ipsum accusare* ou proibição à autoincriminação; princípio da lealdade democrática; princípio do contraditório, do devido processo legal, da ampla defesa; princípio da indisponibilidade das competências constitucionais e infraconstitucionais;

(ii) Os *princípios processuais penais* a destacar neste quadro são: os princípios da *indispensabilidade* para a descoberta da verdade e da *impossibilidade objetiva* de obtenção de prova por meio menos oneroso; princípio da *inadmissibilidade de provas* diretas ou indiretas – efeito-à--distância – de provas feridas de nulidade insanável ou de ilegalidade e ilicitude; princípio da *concordância prática* dos meios de investigação face às finalidades do processo penal – descoberta da verdade material prática processual judicial e válida; realização da justiça; defesa e garantia dos direitos e liberdades de todos os seres humanos; restabelecimento da paz jurídica e social –; princípio da *vinculação ao fim* do meio de obtenção de prova mesmo no espaço ou na era digital.

Acrescentamos que metamorfosear o Direito, sem o mudar, no sentido de lhe subsumirmos a nova dinâmica – a era digital –, de a submetermos à ordem jurídica que deve, com rigor e cientificidade, assumir as funções[29] de *(i) garantia*; *(ii)* de *segurança*; *(iii)* de *coesão social*; e *(iv)* de *equilíbrio* como as bases de uma *ratio iuris* incrustada em uma *epistemologia*, *teleologia* e *axiologia sistematizadas* sob a égide da *dignidade da pessoa humana*.

29. Quanto ao debate sobre as dimensões funcionais do Direito, em especial do Direito penal, o nosso *Direito Penal do Inimigo e o Terrorismo*. O "Progresso ao Retrocesso". Reimpressão da 2.ª Edição – versão portuguesa. Coimbra: Almedina, 2018, pp. 123-130.

Nesse sentido, a dimensão *garantia* engancha o primado de que o Direito penal identifica e determina por lei *os modelos comportamentais humanos com relevância penal* e só os *modelos negativos relevantes tipificados podem ser sujeitos aos juízos de antijuridicidade e de censurabilidade* e ser *submetidos à punibilidade* previamente expressa dentro de um processo-crime de acordo com uma lei prévia que limite o poder de punir. Esta dimensão encerra em si a barreira intransponível da força esmagadora do *ius puniendi* sobre os direitos fundamentais pessoais, *i. e.*, os cidadãos, como "pessoas de direito (*Rechtspersonen*) no papel de destinatários responsáveis de normas".[30]

Já a segurança, dimensão meeira da dimensão *garantia*, arreiga-se em uma dupla pretensão: a *pretensão interna que afirma da ideia do* «eu» poder, socialmente integrado, viver em segurança, o que implica "uma relação de cuidado para consigo"[31]; e uma *pretensão externa que emerge da exigência que cada pessoa detém em ver tutelada jurídico-criminalmente a sua relação de segurança*, que se afirma na ideia do «nós» poder em comunicabilidade com o «outros» poder.

30. Cf. Klaus Günther. Teoria da Responsabilidade no Estado de Direito Democrático de Direito. Tradução de Flávia Portella Püschel e Marta Rodriguez de Assis Machado. São Paulo: Editora Saraiva, 2009, p. 17]. Cf. também José de Faria Costa. Noções Fundamentais de Direito Penal...4ª Edição, p. 15.

31. Cf. José de Faria Costa. Noções Fundamentais de Direito Penal... 4ª Edição, p. 15.

É de frisar, ainda, que a dimensão *coesão social* exige uma *relação comunicacional de coesões: normativa, pessoal e social, a par da relação predisposta política de substrato constitucional*. O Direito penal garantista e humanista e imbuído de uma função de equilíbrio impõe que *a ordem jurídico-criminal funcione "como cimento agregador de todo o*

multiversum que a ordem jurídica constitui"[32] e se afirme como reforço coevo do ser humano como uma unidade: pessoa humana. A coesão social ressalta como tarefa do Direito penal e não como valor em si mesmo. Como tarefa, a *coesão* apresenta-se como um valor densificado e densificador de todos os valores jurídicos penalmente relevantes e essenciais à vida em comunidade.

32. Cf. José de Faria Costa. Noções Fundamentais de Direito Penal... 4ª Edição, p. 15.

Por fim, a dimensão ou função de *equilíbrio* de tutela de bens jurídicos e de defesa do delinquente face ao poder punitivo estatal implica a assunção de uma tridimensionalidade de repartida: dimensão *garantia*, a dimensão *segurança* e a dimensão *coesão*.

6. BREVE CONCLUSÃO

Face ao exposto, gostaríamos de vos dizer que esta preocupação deve ser transversal a todas as áreas científicas do Direito, sendo de destacar o Direito civil, o Direito Constitucional, o Direito penal, o Direito processual penal e o próprio Direito administrativo, uma vez que a tecnologia desenvolvida na e da era digital permite, hoje, com a vossa simples condução do vosso veículo automóvel ou motociclo elaborar o vosso perfil de ser humano[33]: vida pessoal privada e familiar, vida social, vida económica, vida financeira, vida política. Sob o manto de uma presunção de qualidade do veículo, a cada segundo de condução do nosso veículo estamos a transmitir dados concretos da nossa vida que podem ser um dia mais tarde utilizados como perfis criminais ou de tendências criminais: as investigações

33. Por meio de algoritmos da tecnologia digital automóvel.

de campo avançado já estão implementadas através da nova tecnologia automóvel, que, no caso, se enquadrariam como medidas ou providências de "combate preventivo do crime". Essas investigações são designadas pela doutrina e jurisprudência alemã como medidas de prevenção de "*Vorfeld* (campo avançado)", que, quando não existe o mínimo perigo, se designam de providências de "*combate preventivo do crime (vorbeugende Bekämpfung von Straftaten*)", e, quando existe perigo abstrato e concreto de possibilidade de ulterior prática de crimes, providências *"para perseguição criminal (futura) de crimes* (*Vorsorge für die Verfolgung von Straftaten*)".[34] As providências de "*combate preventivo do crime (vorbeugende Bekämpfung von Straftaten*)" tem como escopo a prevenção e o afastamento de "perigos (crimes) possíveis antes de se atingir o limiar do perigo concreto", conquanto as providências *"para perseguição criminal (futura) de crimes* (*Vorsoge für die Verfolgung von Straftaten*)" se destinam a recolher e tratar provas para uma ulterior perseguição criminal e punibilidade de crimes que ainda não foram praticados, mas que se revela possível e provável, "num futuro incerto", a sua prática. Estamos a chegar ao *Minority Report*.[35]

34. Cf. na linha do Tribunal Constitucional alemão, COSTA ANDRADE, Manuel da, *"Bruscamente no Verão passado"*, p. 131.

35. Sobre este assunto a nossa tese de doutoramento, *Do Ministério Público e da Polícia. Prevenção Criminal e Ação Penal como Execução de uma Política Criminal do Ser Humano*. Lisboa: UCE, 2013, pp. 299-328.

Face a esta crua e dura realidade, com a qual colaboramos e pela qual nos deixamos embrulhar, concordamos com Beck quando defende que devemos abandonar a ideia de mudança e optar pela *metamorfose* em que possamos tratar, melhor, aproveitar os *efeitos colaterais positivos dos males* da vida em sociedade.

03.

ACESSO A DADOS ARMAZENADOS EM DISPOSITIVOS MÓVEIS PARA FINS DE INVESTIGAÇÃO: A LICITUDE DA PROVA E A ATUAÇÃO DO PODER JUDICIÁRIO

Kátia Maria Amaral Jangutta

Eu não tenho o hábito de palestrar, sou magistrada. Estou há 30 anos no Poder Judiciário do Rio de Janeiro e a minha tarefa diária é ler processos e julgar. Ao longo desses 30 anos, muita coisa mudou. Nos meus primeiros anos de magistratura, como juíza ainda de primeiro grau, quase não se ouvia falar em crimes como o tráfico de drogas e meios de obtenção de prova como a interceptação telefônica, que surge com a Constituição de 88. Não existia sequer a Lei das Interceptações (Lei n. 9296/96). Os crimes com que eu lidava eram crimes hoje considerados banais, como furto e roubo.

A transformação foi realmente imensa nesse período e, com isso, surge também a necessidade da adaptação da investigação policial. A investigação policial é, como sabemos, um método, uma forma de reconstruir o fato. Na investigação, no entanto, não estão presentes nem o juiz, nem o Ministério Público. Está presente a autoridade policial, frequentemente um policial militar. O processo vai ser formado a partir da história que as autoridades presentes no momento da investigação contarão.

Elas informarão o delegado e o Ministério Público, o Ministério Público contará ao juiz, e, a partir disso, o juiz poderá tomar uma decisão. Evidentemente, a investigação dos fatos é uma grande responsabilidade do trabalho policial. Ela poderia ser comparada a uma pesquisa científica, não fosse a necessidade adicional de obedecer a determinados parâmetros colocados pelas normas processuais e garantias constitucionais. Isto é, a investigação está sujeita a métodos e parâmetros legais, que constituem sua condição de validade.

Nesse ponto, é interessante olhar para a teoria das provas criminais, sobretudo a identificação. É importante identificar as garantias constitucionais que tutelam os bens jurídicos mais importantes e a posição jurídica que é ocupada pela pessoa que está sendo alvo de uma investigação ou sendo presa em flagrante. A teoria das provas criminais observa esses dois pontos e deve ser considerada no exame dessas investigações. Nesse sentido, é importante verificar a plausibilidade da imputação e evitar investigações desnecessárias. Não adianta prender ilegalmente, nem trazer ao processo provas ilegítimas ou ilícitas, pois aquilo vai conduzir a uma nulidade.

A investigação demanda instrumentos e conhecimentos próprios. Hoje o que se tem tentado com o Plano Nacional de Segurança Pública é dar meios, subsídios e conhecimentos às pessoas que trabalham com a investigação para que possam efetivamente fazer uma investigação de qualidade. Não se pode mais trabalhar com aquele espírito do investigador antigo, que desconhecia os meios tecnológicos e o que efetivamente se colhe em um tablet, *smartphone* ou conta de e-mail. É preciso dotar essas pessoas de conhecimento técnico para que se possa fazer uma investigação mais rica e que conduza a um resultado efetivo, seja positivo ou negativo, de condenação ou de absolvição, mas um resultado que seja quase 100 % justo. É esse o dilema diário dos magistrados. A cada processo, quando se encerra o julgamento, a pergunta que se impõe é se foi feita a melhor justiça. É muito bom quando se tem os elementos seguros dentro do processo atribuídos àquela pessoa que está sendo acusada; ou quando não se tem e podemos absolver com tranquilidade, justiça e segurança.

Pois bem, a tecnologia veio evoluindo. Na época em que se começou a realizar interceptações telefônicas, várias discussões surgiram nos tribunais. A lei 9.296/96 regulamentou o artigo 5º, XII da Constituição Federal, que trata do sigilo das comunicações.[1] Antes de se falar em *smartphones*, também já se trabalhava com outras medidas de investigação, como as quebras de sigilos bancário e fiscal, e as medidas de descapitalização previstas no

1. Art. 5º 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."

Código de Processo Penal do art. 125 ao art. 144 – sequestro e arresto.

Nos últimos tempos, passamos a ter também os meios digitais e os elementos colhidos através do acesso aos *smartphones*, como é o caso das comunicações em WhatsApp, MSN, Skype etc. O que nós vemos mais frequentemente nos processos são as provas colhidas por meio do WhatsApp. Hoje, as organizações criminosas, as facções criminosas de tráfico e as milícias recorrem ao WhatsApp como meio de comunicação. A interceptação telefônica ainda é usada para fins de investigação, mas nós temos tido nos processos muitas apreensões de telefones celulares, que ensejam discussões sobre a licitude dessa prova; sobre a existência e extensão do consentimento do acesso ao celular; e se houve autorização judicial ou não. Essa discussão começou a surgir nos tribunais há alguns anos. A matéria já chegou ao STJ [Superior Tribunal de Justiça][2] e em alguns pontos está afetada para que o STF [Supremo Tribunal Federal] decida.[3] Justamente por serem matérias ainda muito novas, as questões ainda não estão consolidadas pelo STF. Não obstante estão efetivamente todos os dias nos nossos tribunais.[4]

Aqui nós trabalhamos com essas provas e falamos de um direito probatório de terceira geração. Como mencionou o professor Manuel Valente, o direito probatório de terceira geração é caracterizado por essas provas invasivas de alta tecnologia, que permitem alcançar resultados que aqueles métodos tradicionais não permitiriam. Além das provas obtidas por meio do acesso a celulares, também são provas de terceira geração os exames de DNA, diversos tipos de exames psicológicos, os keyloggers, que são os programas espiões, dentre outros. As provas de terceira geração, aliás, estão em várias áreas do direito, não só na área criminal.

Inicialmente, nós tivemos uma decisão do Supremo Tribunal Federal de 2012 em um Habeas Corpus, já trabalhada pela doutrina, na qual o ministro Gilmar Mendes reputou lícita a análise de registros telefônicos armazenados em um aparelho de telefonia celular durante uma prisão em flagrante, sem a necessidade de autorização judicial.[5] Em sua argumentação, afirmou-se que verdade não se tratava da comunicação dos dados, mas apenas dos dados em si.[6] Posteriormente, em 2016, tivemos uma outra decisão da 6ª Turma do STJ no Habeas Corpus 51.531/RO, relata pelo do Ministro Nefi Cordeiro, no qual ele entendeu pela ilicitude da devassa de dados, o que já foi um avanço em relação à decisão anterior.[7] No caso, o telefone celular também havia sido apreendido e houve invasão dos dados sem a prévia autorização judicial.

Na nossa legislação, o Marco Civil da Internet (Lei 12.965/14) assegura a inviolabilidade e o sigilo das comunicações pela internet, exigindo a prévia autorização judicial para acessar esses dados.[8]

2. [Nota da editora] Sobre decisões paradigmáticas do STJ envolvendo a legalidade de provas obtidas mediante o acesso a telefones celulares ver: STJ. Quinta Turma. Habeas Corpus 66.368/PA. Recurso Ordinário em Habeas Corpus 51.531/RO. Recurso Ordinário em Habeas Corpus 89.981/MG.

3. [Nota da editora] Está pendente de julgamento no Supremo Tribunal Federal, com repercussão geral, o Recurso Extraordinário com Agravo nº 1.042.075/RJ, no qual se discute a legalidade da prova obtida mediante o acesso ao celular do réu. No caso, em uma tentativa de roubo, o acusado deixou cair seu celular na cena do crime e fugiu. A vítima recolheu o aparelho e entregou-o à polícia, que por meio da análise das fotos e registros de chamada conseguiu identificar e localizar o acusado.

4. [Nota da editora] Sobre a jurisprudência dos tribunais estaduais a respeito do acesso de autoridades policiais a celulares em abordagens e flagrantes ver: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza; MASSARO, Heloisa; LUCIANO, Maria. Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. *Revista Brasileira de Ciências Criminais*, vol. 154, ano 27, p. 177-214, abr. 2019

5. STF. Segunda Turma. Habeas Corpus 91.867/PA. Min. Rel. Gilmar Mendes, j. 24 abr. 2012.

6. [Nota da editora] Sobre o escopo de proteção do art. 5º, XII, da Constituição Federal, cf. ANTONIALLI, Dennys, et al. Vigilância sobre as comunicações no Brasil, São Paulo: InternetLab, 2017.
Disponível em https://bit.ly/2raLh6S

7. STJ. Sexta Turma. Recurso Ordinário em Habeas Corpus 51.531/RO. Min rel. Nefi Cordeiro, j. 19 abr. 2016.

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

Além da previsão do Marco Civil da Internet, a Lei 9.296/96 já exigia autorização judicial para as interceptações telefônicas. Existem, portanto, alguns parâmetros para as investigações em situações que envolvam o acesso a telefones celulares, tablets e computadores; ou seja, é necessário que haja a prévia autorização judicial.

Nesse ponto há algumas diferenciações, como na hipótese de haver uma autorização do titular daquele celular. Em muitos processos os policiais afirmam que o indivíduo teria consentido. Isso eu falo da prática, porque é o que eu vejo ali todo dia. O policial diz: "não, mas ele permitiu, eu peguei o telefone, não tinha senha, eu abri." Nesses casos, algumas decisões admitiam aquela prova como válida, porque, como o telefone não tinha senha e era acessível a qualquer pessoa, qualquer coisa que se retirasse dali valeria como prova. Inicialmente se aceitou essa argumentação, mas, posteriormente, passou-se a discutir que outras pessoas ali estão envolvidas. Hoje um telefone dispõe de agenda telefônica, notas, e-mails, fotografias, e todo tipo de compromisso e informações. Tudo é colocado no *smartphone*, desde informações sigilosas e dados bancários, até informações relativas a outras pessoas. Então, deve haver a autorização judicial mesmo nos casos em que há autorização do titular do telefone, porque o acesso afeta outras pessoas.

Essa discussão envolvendo a legalidade das provas obtidas mediante acesso a telefones celulares foi abordada pela 2ª Câmara Criminal do Tribunal de Justiça do Rio de Janeiro no julgamento de uma apelação.[9] No caso, dois sujeitos, um adulto e um adolescente, haviam sido presos perto de um ponto de venda de drogas em uma comunidade de Niterói, no Rio de Janeiro. Isso ocorre todos os dias, é corriqueiro. Perto deles havia uma gran-

9. TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. 2ª Câmara Criminal. Apelação n. 0066620-61.2015.8.19.0002. Des. rel. Kátia Maria Amaral Jangutta, j. 25 jul. 2017.

/ DEVE HAVER ORDEM JUDICIAL MESMO NOS CASOS EM QUE HÁ AUTORIZAÇÃO DO TITULAR DO TELEFONE, PORQUE O ACESSO AFETA OUTRAS PESSOAS /

de quantidade de drogas, uma sacola com muita maconha e cocaína. Os policiais chegaram, prenderam-nos e, com o réu, foi encontrado um *smartphone* contendo fotografias portando um fuzil e um rádio transmissor. Como o réu e o adolescente estavam próximos da droga, os policiais prenderam ambos, arrecadaram a droga, o telefone, apreenderam tudo e levaram para a delegacia. No processo não se esclarece como as fotos desapareceram dali, porque não se conseguiu acessá-las posteriormente, mas os policiais informaram à autoridade policial que acessaram o telefone celular mediante autorização do réu e que viram as tais fotos. Eles afirmaram que, como ele estava junto com o adolescente, num ponto de venda de drogas e havia entorpecentes perto, eles estariam envolvidos em tráfico de drogas e em associação criminosa. Eles foram denunciados por esses dois crimes, incidindo sobre o adulto ainda a causa de aumento do artigo 40, VI, da Lei de Drogas (Lei n. 11.343/06),[10] por ter envolvido um adolescente. Na justiça da Infância e Juventude, o adolescente foi absolvido de todas as imputações. Como nós não tivemos acesso à sentença da justiça especializada, não conheço os fundamentos da absolvição.

10. Art. 40. As penas previstas nos arts. 33 a 37 desta Lei são aumentadas de um sexto a dois terços, se: VI - sua prática envolver ou visar a atingir criança ou adolescente ou a quem tenha, por qualquer motivo, diminuída ou suprimida a capacidade de entendimento e determinação.

No caso do outro réu, em primeira instância ele foi absolvido pelo crime de tráfico, foi retirada a causa de aumento do artigo 40, VI, da Lei de Drogas, e ele foi condenado só pela associação criminosa. Em seu fundamento, o juízo afirmou que na fase policial o réu teria confirmado a existência da foto em seu telefone celular. O réu haveria justificado que estava posando para os amigos para mostrar uma arma de *airshot*. Ele não admitiu que fizesse parte do tráfico, nem que fosse traficante. Ainda assim o juízo de primeira instância, ao condená-lo, utilizou essa afirmação e essa prova obtida por meio do telefone celular.

Em face da condenação, o réu apelou. Na apelação a defesa argumentou que mesmo que o réu tenha reconhecido a existência da foto e que nela segurava a arma, e ainda que os policiais tenham afirmado que apreenderam o telefone celular e que nele havia fotos do réu posando com uma arma, a prova era ilícita e não poderia ter servido para a condenação porque ela não fora obtida com autorização judicial. Não se podia invadir o telefone do réu e condená-lo com base nos depoimentos dos policiais e em seu depoimento extrajudicial posteriormente negado em juízo - no qual ele teria confirmado a existência das fotos, mas negado que fizesse parte do tráfico, afastando a imputação.

Esse processo é de 2015 e foi um dos primeiros a aparecer na 2ª Câmara Criminal envolvendo comunicações no WhatsApp. Estudando o caso, chegamos à conclusão de que efetivamente a prova era ilícita e que ela não poderia servir para condenar o réu, justamente porque não havia prévia autorização judicial. Em nossa fundamentação, nós nos baseamos em decisões anteriores do direito comparado, em casos dos Estados Unidos [*Riley vs. Califórnia*], Canadá [*Respondent vs. Fearon*] e Espanha [*Sentencia 115/2013*].[11] No direito comparado eu sinto que ainda há discussões para ambos os lados e que essa situação não é pacífica, com a existência de decisões contrárias tanto em um país como no outro.

11. [Nota da editora] Sobre casos do direito comparado ver: ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. In: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. *Direitos Fundamentais e Processo Penal na Era Digital:* doutrina e prática em debate. Vol. 1. São Paulo: InternetLab, 2018.

O que tentamos mostrar na votação desta apelação na 2ª Câmara Criminal é que a lei brasileira exige efetivamente o respeito ao art. 5º, XII, da Constituição Federal, e ao art. 7º, II e III, do Marco Civil da Internet, não servindo para fins de condenação apenas aquela dita "autorização do réu" para acessar seu celular. Nós chegamos a essa

conclusão e a decisão acabou sendo unânime. No acórdão eu citei outros casos do STJ a respeito dessa matéria. Nós fizemos uma pesquisa e vimos que no STJ essa matéria é praticamente unânime, no sentido de que há a necessidade da autorização judicial. No STF, por outro lado, ainda há um recurso afetado para decisão, para que se forme uma posição.[12]

Outra questão discutida na sessão foram as situações envolvendo mandado de busca e apreensão, na hipótese de a polícia dispor do mandado e, durante a diligência, encontrar um tablet, um computador, ou um telefone. Com o simples mandado de busca, sem nenhuma autorização para que se faça uma devassa nos dados armazenados naqueles aparelhos, a polícia pode ou não acessar esses dados? Inicialmente entendeu-se que com o simples mandado de busca e apreensão era possível acessar todos os dados armazenados, e que essa prova era lícita. Todavia, naquele momento eu já entendia que apenas com um mandado de busca com autorização judicial para fazer a devassa de dados eventualmente encontrados em aparelhos é que essa prova seria admitida para eventual condenação. Esse é o caminho que vem sendo tomado no tribunal, no STJ e em algumas decisões do STF; os mandados de busca e apreensão nas investigações policiais têm que estar dotados de determinação judicial para eventual necessidade de devassa de dados em aparelhos tecnológicos que sejam encontrados em poder dos réus. Essa tem sido a orientação.

12. Recurso Extraordinário com Agravo nº 1.042.075/RJ.

No STJ também há um Recurso em Habeas Corpus do ministro Reynaldo Soares da Fonseca, no qual se entendeu que houve violação da intimidade em uma vistoria realizada pela Polícia Militar em um aparelho celular sem uma autorização judicial.[13] No Tribunal de Justiça do Rio de Janeiro também há decisões em correições parciais nesse sentido. O que é importante então? Que esteja claro que a autoridade policial não pode fazer as devassas nos aparelhos celulares sem a devida autorização judicial.

13. STJ. Quinta Turma. Recurso Ordinário em Habeas Corpus 89.981/MG. Min rel. Reynaldo Soares da Fonseca, j. 5 dez. 2017

Não obstante, na hipótese de uma emergência, no caso de crimes que estão em consumação, a exemplo de uma extorsão mediante sequestro, é necessário ponderar os bens jurídicos em conflito. Nesses casos há, de um lado, uma violação da intimidade, mas, de outro, temos a vida da vítima que está correndo risco. Então, em determinados crimes, excepcionalmente, a polícia poderia dispor dos aparelhos e acessar os dados sem autorização judicial. Contudo, nessa hipótese ela deverá desabilitar a conexão do celular da rede mundial de computadores para que as informações não sejam obtidas em tempo real, limitando a consulta àquela troca de mensagens feita a respeito daquele delito em específico. Isso seria uma exceção a esse tipo de prova. Na 2ª Câmara Criminal nós não tivemos nenhum caso de extorsão ou outro crime no qual a vida da vítima estivesse em jogo naquele momento, mas na discussão com os meus colegas de outras câmeras nós chegamos mais ou menos a essa conclusão. Eu tenho visto também alguma jurisprudência e doutrina nesse sentido.

Fugindo um pouco dos casos em si, considero atualmente que dotar efetivamente a polícia dos meios necessários para investigação é importante. Hoje se fala muito da fusão da informação. A fusão da informação é justamente essa reunião de possibilidades, órgãos, e pessoas, para que se possa colher os melhores métodos de obtenção de informações e de investigações. No Brasil, por exemplo, nós temos a Delegacia da Polícia Federal e a Agência Brasileira de Inteligência (Abin), criada pela Lei 9.883/99, que trabalham com essa questão da fusão de informação. Nos Estados Unidos há o Sistema Integrado de Informações sobre justiça, que é uma organização

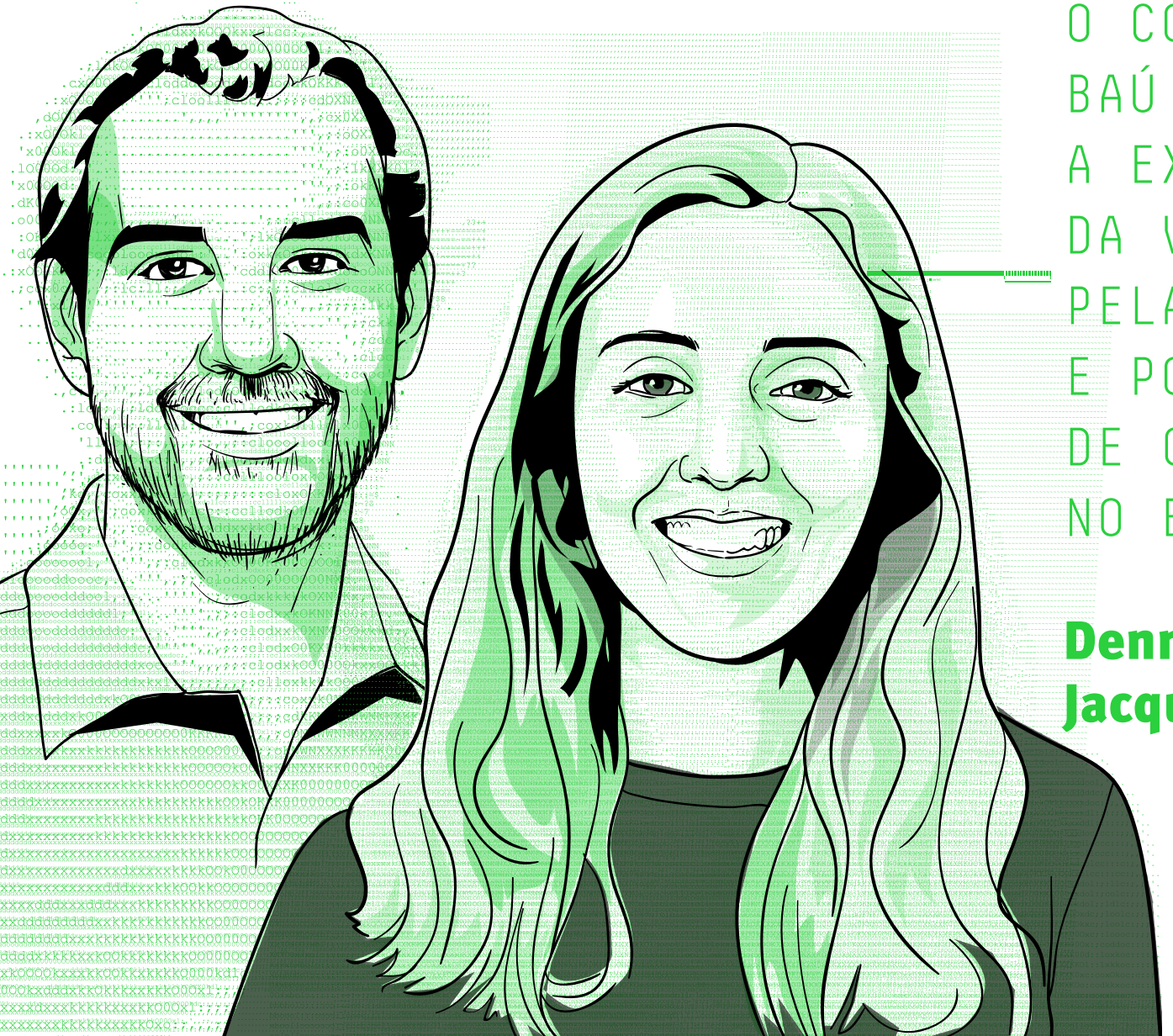
do terceiro setor e, portanto, não está ligado a essas tecnicalidades e dificuldades do setor público, valendo-se dessa cooperação com o setor privado e o terceiro setor para enriquecer a investigação. Isso funciona muito bem nos Estados Unidos e eu entendo que esse também é o espírito da nossa Constituição de 88. Apesar de não ser ainda totalmente aplicado, o governo tem tentado incentivar diversas práticas, como no caso do Plano Nacional de Segurança de 2017. O espírito é efetivamente o de que todos têm que colaborar para a segurança pública, tanto os setores públicos quanto os setores privados, as empresas, e a sociedade de uma forma geral. Deve haver essa fusão de informações, porque, quanto mais rico, maior capacidade e mais tecnologias de informação – a TI hoje é importantíssima para as investigações -, melhor será a investigação. O que se faz bem na investigação permite posteriormente uma melhor avaliação pelo Ministério Público quando que ele recebe os autos do inquérito.

É o que eu sempre digo, quem relata os fatos é a polícia e, depois, o juiz avalia a plausibilidade da história. Afinal, a polícia não investiga sob condições ideais: está exposta à precariedade e à vulnerabilidade. A história chega da maneira como ela viu, encontrou, e conseguiu contar. Então quanto mais rica, minuciosa e segura essa história puder chegar, melhor. Se há uma autorização do juiz, se o Ministério Público analisou, se a autoridade policial analisou e pode fazer um pedido baseado em dados seguros e lícitos, sem desperdício de recursos e tempo, melhor será a decisão, tanto do juízo de primeira instância quanto do juízo de segunda instância. Isso é o que nós aguardamos e para o que nós trabalhamos.

No Rio de Janeiro eu componho um conselho de vitaliciamento dos juízes novos. Durante dois anos, os juízes ficam em vitaliciamento e eu faço parte do conselho que os supervisiona. Ouço suas ideias a respeito dessas questões. Eu sempre digo que o juiz hoje tem que tentar estar o mais próximo possível dos fatos, porque quanto mais eles se afastarem, mais difícil será o julgamento. O estar próximo não quer dizer que ele seja parcial ou que ele vá se envolver. No Brasil, nós estamos desenvolvendo um sistema acusatório, no qual o juiz fica em princípio equidistante das partes, ao mesmo tempo em que participa. Então, quanto mais seguro o juiz estiver daquilo que está sendo feito, melhores serão as decisões e maior segurança jurídica haverá.

Senhores, isso era o que eu tinha a dizer a vocês. Perdoem qualquer falha na exposição; como eu disse, não sou palestrante, mas espero ter podido colaborar de alguma forma.

04.



O CONTO DO BAÚ DO TESOURO: A EXPANSÃO DA VIGILÂNCIA PELA EVOLUÇÃO E POPULARIZAÇÃO DE CELULARES NO BRASIL*

Dennys Antonialli
Jacqueline de Souza Abreu

* Este artigo foi originalmente publicado nos anais do V Simpósio LAVITS - Rede latino-americana de estudos sobre vigilância, tecnologia e sociedade.

01. INTRODUÇÃO

A chegada de telefones celulares foi certamente um avanço para as comunicações em tempo real. A independência de dispositivos fixos permitiu que as pessoas alcançassem e fossem alcançadas a qualquer momento, revolucionando a forma como interagem entre si. A capacidade de transportar dispositivos telefônicos a qualquer lugar também deu origem a uma série de diferentes usos e aplicações, transformando telefones celulares em objetos (muito) inteligentes; uma das características mais importantes da tecnologia do telefone móvel é a conectividade com a Internet.

Ao provocar uma transformação na forma como as pessoas se comunicam, possibilitando a substituição das chamadas telefônicas tradicionais por aplicações de mensagens instantâneas, e-mails e até chamadas de voz sobre IP habilitadas para web, os telefones celulares também se tornaram um tesouro de informações de comunicações, particularmente para autoridades de segurança pública. Além dos registros detalhados sobre quando, onde e por quanto tempo as comunicações ocorreram, essas novas formas de troca de informações também podem armazenar todo esse conteúdo e muito mais, como lista de contatos, fotos, notas, listas de leitura, histórico de páginas visitadas, dados de localização.

Dado que o acesso a dados de comunicações é uma estratégia de investigação bastante disseminada no Brasil, este artigo descreve as formas como a "revolução do *smartphone*" permitiu novas formas de vigilância no Brasil. Apesar de a Constituição Federal brasileira de 1988 garantir o sigilo das comunicações, ela inclui uma exceção para fins de investigação e processo penal, a qual foi regulamentada na Lei de Interceptações (Lei 9.296/1996). Desde então, as circunstâncias em que esse acesso é concedido mudaram significativamente, muito em razão da evolução e popularização de celulares.

Beneficiando-se de doutrinas desatualizadas e avançando interpretações expansivas, algumas autoridades policiais e representantes do Ministério Público têm reivindicado que o acesso ao conteúdo de comunicações armazenadas e a metadados deva seguir regras muito menos estritas do que as da Lei de Intercepções. Essas reivindicações estão sendo frequentemente consideradas adequadas pelo Judiciário, estabelecendo precedentes influentes. Além disso, a "Operação Lava Jato", investigação nacional sobre o maior esquema de corrupção da história, proporcionou um impulso para narrativas que reforçam capacidades investigativas, consolidando uma expansão sistemática de prerrogativas de vigilância, particularmente para a obtenção de evidências armazenadas em dispositivos eletrônicos.

O trabalho aborda a falta de correspondência entre a popularização do serviço de telefonia e a evolução dos telefones celulares, de um lado, e as proteções fornecidas às comunicações e dados pela legislação brasileira, de outro. Para isso, apresentamos evidências empíricas sobre a evolução e uso dessas tecnologias no Brasil e fornecemos uma visão geral das leis, práticas e jurisprudência de vigilância no país, mapeando os principais problemas que surgiram envolvendo acesso a dados de telefonia móvel.[1]

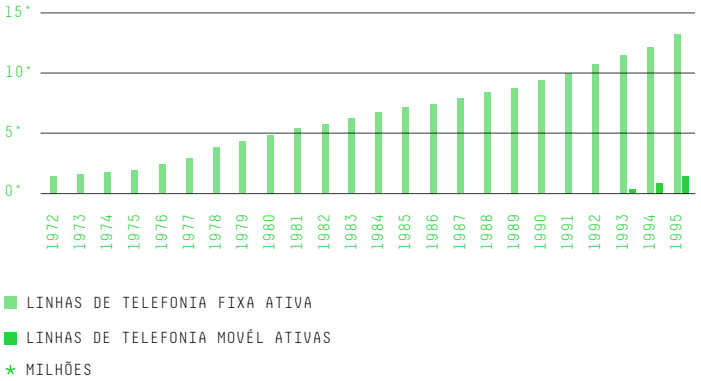
1. Este trabalho é um sumário dos resultados apresentados em (Abreu & Antonialli, 2017).

02. A REVOLUÇÃO DA TELEFONIA CELULAR NO BRASIL

A chegada do primeiro telefone no Brasil remonta ao final do século XIX, mas foi apenas nos anos 1950 que a indústria começou a florescer. No final dessa década, cerca de mil companhias telefônicas ofertavam serviços às áreas urbanas do país.

Ainda passavam, entretanto, por desafios operacionais devido à falta de padronização e interoperabilidade. Para uma população de 70 milhões, não havia mais de 1 milhão de linhas telefônicas instaladas (Neves, 2002). De 1960 a 1996, o setor de telecomunicações viveu uma rígida intervenção do Estado. Mesmo assim, não experimentou a expansão em massa. Em 1995, havia apenas 13 milhões de celulares fixos no Brasil, agora com uma população de 162 milhões.

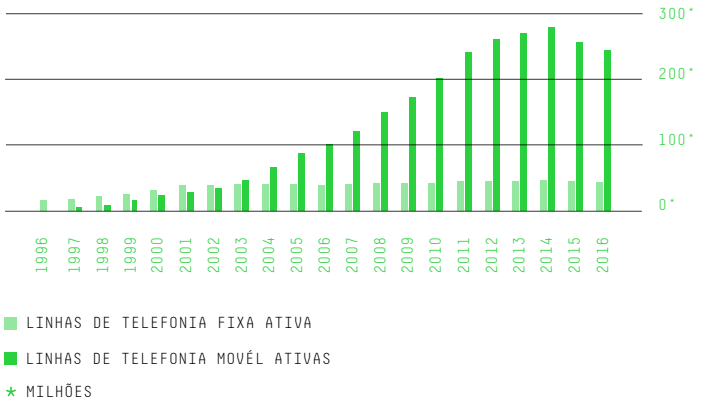
GRÁFICO 1. USO DE TELEFONIA NO BRASIL
(1972-1995)



FONTE: AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES 2016, 192-4.

Com a privatização do setor de telecomunicações em 1996, o objetivo da universalização dos serviços de telefonia ganhou fôlego. Para essa transformação, a introdução da tecnologia de telefonia móvel foi de extrema importância. A quantidade de assinaturas fixas ativas triplicou em 10 anos (13 milhões em 1995 para 39 milhões em 2005), mas desde 2010 estabilizou em cerca de 43 milhões. Por outro lado, a quantidade de assinaturas de telefones celulares aumentou dramaticamente, atingindo um pico de 280 milhões em 2014. A população brasileira era de 204 milhões no mesmo ano.

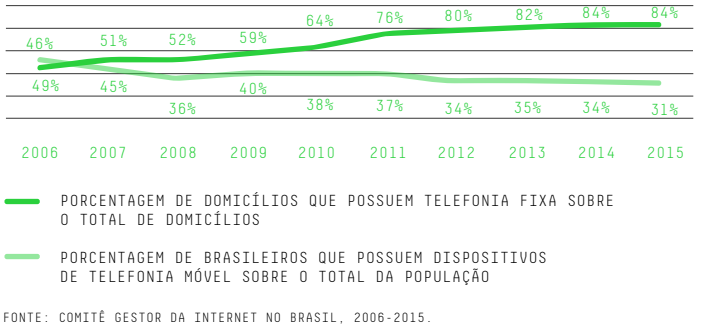
GRÁFICO 2. USO DE TELEFONIA NO BRASIL
(1996-2016)



FONTE: AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES 2016, 192-4.

Não só a grande maioria dos brasileiros (84%) agora possui telefones celulares, como também o número de telefones fixos está em declínio, confirmando que os celulares cresceram em importância como meio de comunicação (Gráfico 3).

GRÁFICO 3. USO DE TELEFONIA FIXA E MÓVEL NO TEMPO
(2006-2015)

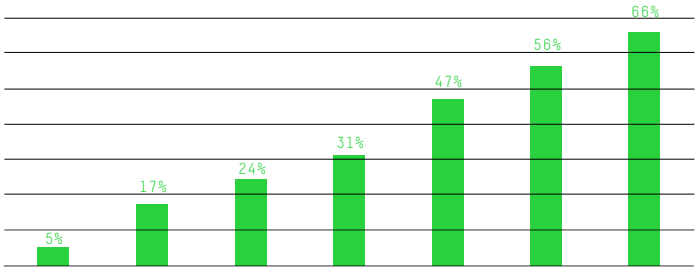


FONTE: COMITÊ GESTOR DA INTERNET NO BRASIL, 2006-2015.

Seguindo uma tendência global, no Brasil, os smartphones estão ganhando presença. Como os números abaixo mostram (Gráfico 4), a porcentagem de brasileiros que usam celulares para acessar a Internet - uma atividade típica do uso de smartphones - está crescendo rapidamente. Além disso, uma pesquisa IBOPE Inteligência de 2016, encomendada pela Qualcomm, indicou que a participação de brasileiros que possuem um smartphone passou de 19% em 2014 para 40% em 2016 (IBOPE Inteligência, 2016). Mais recentemente, uma pesquisa da Datafolha lançada no início de 2017, encomendada pela WhatsApp Inc., mostrou que 79% dos brasileiros adolescentes e adultos usam telefones inteligentes para acessar a Internet, atestando o crescimento da penetração desta tecnologia no Brasil (Datafolha, 2016).

Apesar dos números, vale a pena mencionar que a desigualdade social do Brasil também é atestada no uso da tecnologia de telefonia móvel. De acordo com uma pesquisa de 2015 do *think tank* estadunidense Pew Research Center, a proporção de brasileiros adultos que possuem um smartphone muda de acordo com o grupo demográfico (Poushter, 2016). Brasileiros mais jovens, mais educados e de classe superior, mais frequentemente, possuem smartphones. A título de exemplo, enquanto no grupo de renda mais alta 54% possuíam um smartphone, no grupo de baixa renda esse número caia para 25%.

GRÁFICO 4. BRASILEIROS QUE USARAM O CELULAR PARA ACESSAR A INTERNET NOS ÚTILOS TRÊS MESES (PORCENTAGEM SOBRE A POPULAÇÃO)



A alta taxa de penetração da tecnologia de telefonia móvel no Brasil representa, em geral, um marco significativo, não só em termos de expansão do acesso à comunicação de longa distância, mas também a serviços baseados na Internet. Esses são números notáveis em termos de acesso ao conhecimento.

A proliferação de smartphones tem, no entanto, seu lado sombrio: expõe mais brasileiros a novas formas de vigilância, tanto do governo quanto do setor privado. Em termos de vigilância governamental, além das interceptações do conteúdo de comunicações em tempo real, o acesso a metadados e a informações armazenadas tornou-se uma prática comum, seja pela busca e apreensão de dispositivos ou pela devassa destes tipos de dados por meio de empresas de telecomunicações ou provedores de aplicações.

As ameaças decorrentes dessas capacidades expandidas de vigilância seriam menos preocupantes se o direito brasileiro oferecesse aos seus cidadãos salvaguardas robustas em termos de proteção a direitos humanos que os resguardasse de acessos ilegais e abusivos aos seus dados.

Entretanto, como demonstramos na próxima seção, o direito brasileiro não avançou junto com os dispositivos de telefonia móvel, deixando cidadãos – usuários de celulares – vulneráveis à vigilância ilegal e abusiva. A próxima seção oferece um quadro geral do regime legal aplicado e identifica as principais questões que surgem de interpretações ultrapassadas, vácuos, e medidas de controle insuficientes, típica e eficientemente exploradas por autoridades de segurança pública no Brasil.

03. O QUADRO NORMATIVO DA VIGILÂNCIA: AS QUESTÕES CENTRAIS

Apesar de a Constituição Federal brasileira de 1988 proteger o sigilo das comunicações e a privacidade, disputas interpretativas repercutem no grau de proteção que esses direitos garantem contra a vigilância indevida de autoridades do Estado sobre comunicações.

A primeira fragilidade decorre de uma persistente controvérsia sobre o âmbito de proteção conferido ao sigilo das comunicações, garantido no inciso XII do art. 5º ("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"). Dessa redação pouco clara surgem basicamente duas questões interpretativas principais: (i) qual é o objeto de proteção do sigilo: o *conteúdo* das informações comunicadas e transmitidas pelos meios citados (isto é, as correspondências, mensagens telegráficas, dados e telefonemas em si) ou o mero *fluxo* dessas informações por esses meios? (ii) qual(-is) grupo(-s), dentre os quatro listados no inciso, estão submetidos à exceção constitucional que permite a quebra do sigilo ("salvo, no último caso..")?

O entendimento doutrinário até hoje predominante (Ferraz Junior, 1993; Ferreira Filho, 2009, p. 301; Silva, 2008, p. 438), que também encontra eco em decisão do Supremo Tribunal Federal[2] (STF), é no sentido de que *(i)* a proteção do inciso XII do art. 5º não se refere ao conteúdo das informações comunicadas em correspondências, mensagens telegráficas, dados e telefonemas em si, mas sim à sua comunicação, isto é, ao seu *fluxo* enquanto ocorrem e que *(ii)* apenas o sigilo da comunicação por *telefonia*, enquanto está em fluxo, poderia ser restringido para fins de investigação criminal e instrução processual penal, não se estendendo essa possibilidade para o fluxo de dados, telegrafias e cartas. Decorre dessa interpretação o entendimento de que estão excluídos do âmbito de proteção do dispositivo não somente o *conteúdo* de comunicações armazenadas, registradas ou gravadas como também as informações geradas a respeito das circunstâncias nas quais as comunicações ocorreram (metadados).

2. No julgamento do RE 418.416-8/SC, de 10/05/2006, o Min. Rel. Sepúlveda Pertence afirma que a proteção do inciso XII do art. 5º não se refere às informações comunicadas em si, mas à comunicação, ao *fluxo* das mesmas enquanto ocorrem.

Além disso, o entendimento predominante é o de que somente comunicações telefônicas *em fluxo* poderiam ter seu sigilo afastado; essa possibilidade não se aplicaria a comunicações por correspondências, telegrafias e dados, enquanto em fluxo, os quais seriam absolutamente invioláveis. Tal interpretação, mesmo que ainda respaldada por parte da doutrina, não reflete a jurisprudência dos tribunais, que passou a admitir "quebras" do sigilo do fluxo das comunicações de

todos os tipos, isto é, não só de comunicações telefônicas, desde que "proporcionais", quando se fundamentarem em direito fundamental conflitante ou em interesse público.[3] Também não reflete a atuação do Congresso Nacional que, em 1996, ao regulamentar a quebra de sigilo de comunicações telefônicas, como autoriza a Constituição Federal expressamente, também incluiu a possibilidade de se realizar interceptações "telemáticas" (o que abarca interceptações de "dados") na Lei de Interceptações. Em 2014, o Congresso também voltou a explicitamente admitir interceptações de comunicações eletrônicas (que, igualmente, envolvem "dados") no Marco Civil da Internet.

3. No HC 70814/SP, por exemplo, o STF admitiu que a administração penitenciária pode interceptar carta de preso, por razões de segurança pública, disciplina prisional ou preservação da ordem jurídica, com base no art. 41, parágrafo único, da Lei 7210/84.

A partir da constituição, outras leis abordam questões específicas que envolvem o acesso a comunicações por parte de autoridades para fins de investigação criminal. Seja porque elas foram redigidas para um contexto tecnológico diferente ou porque adotaram linguagem ampla, essas leis contêm lacunas que foram e são exploradas por autoridades de segurança pública. Além disso, lacunas em tais textos deixam muitas questões abertas, expondo os usuários de celulares a uma vigilância ainda maior e mais invasiva. Nas subseções abaixo, resumimos as principais circunstâncias que contribuem para acentuar esse problema.

3.1 ACESSO A DISPOSITIVOS ELETRÔNICOS MEDIANTE MANDADOS DE BUSCA E APREENSÃO

A interpretação constitucional restritiva dada ao sigilo das comunicações, qual seja a de que ele só protegeria (conteúdo de) comunicações enquanto estão em *fluxo*, gera uma situação de descompasso normativo: os modernos celulares, *tablets* e computadores armazenam uma enorme quantidade de informações, fotos e comunicações que oferecem retratos fieis e detalhados de seus donos, mas que não gozariam da mesma proteção de comunicações em fluxo pelo mero fato de agora estarem arquivadas.

A Lei das Interceptações (Lei nº 9.296), de 1996, surgiu para regular a hipótese de aplicação da exceção constitucional ao sigilo das comunicações, determinando as circunstâncias nas quais as autoridades do Estado podem ter acesso a comunicações telefônicas e telemáticas enquanto *em fluxo*, seja por meio da realização de interceptações junto a empresas de telefonia ou do emprego de grampos ou escutas ambientais. Para tanto, estabeleceu um regime jurídico rigoroso, que envolve o preenchimento de requisitos mais difíceis de ser atendidos. Esses requisitos estão previstos no art. 2º da lei e exigem *(i)* a configuração de indícios razoáveis da autoria ou participação em infração penal; *(ii)* a inexistência de outros meios de prova; e *(iii)* o envolvimento em crimes de maior gravidade. A lei estabeleceu também um limite temporal para realização dessa medida (15 dias, renováveis).

Diferente é a situação da proteção (a conteúdo) de comunicações armazenadas, isto é, as que não estão mais em trânsito. A legislação infraconstitucional toca a questão em duas leis diferentes. Quando o acesso a essas comunicações se dá por meio de um intermediário, que detém os dados (como é o caso de provedores de aplicações de Internet), os dispositivos aplicáveis são aqueles previstos no Marco Civil da Internet, o qual determina que o acesso ocorra mediante "ordem judicial" (art. 7º, III) nas hipóteses e na forma que a lei o estabelecer (art. 10, § 2º), sem, entretanto, explicitar requisitos substantivos de padrão probatório.

Quando o acesso se dá diretamente no aparelho apreendido, o regime não é claro. Não há regras específicas desenhadas e aplicadas para a busca de dispositivos *eletrônicos*, dando lugar a discricionariedade judicial, insegurança jurídica e abusos. Diante disso, pode-se dizer que, atualmente, comunicações armazenadas, registradas em celulares e computadores, provavelmente por anos a fim, gozam de um grau de proteção menor do que comunicações em *fluxo*, cujo acesso se encontra regulamentado de forma mais rigorosa pela Lei de Interceptações.

Este paradoxo já começa a ser identificado e contestado em artigos de opinião (Antonialli, Brito Cruz, & Valente, 2016; Maranhão, 2016). Na doutrina, também já começa a se argumentar que o art. 5º, XII da Constituição deveria garantir proteção irrestrita a *conteúdo* de comunicações, estejam elas em fluxo ou armazenadas, com a implicação de que toda quebra de sigilo de conteúdo deveria seguir os requisitos atuais da Lei das Interceptações (Sidi, 2015, pp. 111–8).

O Superior Tribunal de Justiça (STJ), em julgamento de setembro de 2016, já afastou essa tese. Na mesma decisão, afirmou a legalidade da prova obtida por celulares apreendidos no âmbito da Operação Lava Jato mediante mandado de busca e apreensão, mesmo sem autorização judicial específica que delimitasse a "busca virtual".[4] No Recurso Extraordinário 418.416-8/SC, julgado em 2006, o Supremo Tribunal Federal também admitiu que o mero mandado de busca e apreensão já legitima acesso a dados armazenados em computadores.

4. STJ. Recurso em Habeas Corpus nº 75.800-PR. Ministro Felix Fischer, julgado em 15.09.2016. Disponível em: https://bit.ly/2NLgtuj.

Apesar de separadas por dez anos, as duas decisões demonstram quão penetrantes são as raízes do entendimento de que dados armazenados não estão protegidos pelo direito ao sigilo das comunicações na jurisprudência nacional, o qual alimenta o descompasso normativo entre a proteção de comunicações em fluxo e comunicações armazenadas.

/ A PROLIFERAÇÃO DE SMARTPHONES TEM SEU LADO SOMBRIO: EXPÕE MAIS BRASILEIROS A NOVAS FORMAS DE VIGILÂNCIA /

/ A LEGISLAÇÃO NÃO AVANÇOU JUNTO COM OS APARELHOS CELULARES, DEIXANDO SEUS USUÁRIOS VULNERÁVEIS À VIGILÂNCIA ILEGAL E ABUSIVA /

3.2 ACESSO A DISPOSITIVOS ELETRÔNICOS APÓS PRISÃO EM FLAGRANTE

Um cenário igualmente problemático é o de quando o acesso a dados armazenados em dispositivos eletrônicos – principalmente celulares – se dá durante ou logo após uma prisão em flagrante. Quando autoridades policiais realizam prisões em flagrante, procedem à busca de objetos e produtos do crime portados pelo preso, para coleta de elementos que constituirão o auto de prisão em flagrante e como medida de segurança das próprias autoridades. Nesse cenário, tem-se questionado se é permitido às autoridades policiais acessar também dados armazenados no celular portado pelo preso. A prisão em flagrante autoriza a devassa não só à pessoa em si e/ou ao seu domicílio, mas também a tudo que está salvo eletronicamente junto em dispositivos do preso? Outra vez a controvérsia sobre o regime de proteção de dados (conteúdo de comunicações e metadados) *armazenados* surge.

Não há convergência nos tribunais superiores acerca da legalidade desse acesso e das provas daí obtidas. Em julgado de 2012, o STF decidiu que a análise de registros telefônicos (metadados) de celular apreendido após prisão em flagrante não caracteriza violação ao sigilo das comunicações (art. 5, inciso XII), porque sua proteção abarcaria "comunicações de dados e não dados em si" e porque "comunicação telefônica e registros telefônicos recebem proteção jurídica distinta".[5] Em 2007, o STJ já havia decidido de forma semelhante: a verificação de histórico de chamadas efetuadas e recebidas após prisão em flagrante não configura quebra ilegal de sigilo, porque as informações não foram obtidas por intermediário (empresas telefônicas) e nem se obteve conhecimento de conteúdo de conversas efetuadas.[6] Em 2016, por outro

5. STJ. Habeas Corpus nº 91.867/SP. Min. rel. Gilmar Mendes, j. 24.04.2012.

6. STJ. Habeas Corpus nº 66.368/PA. Min. rel. Gilson Dipp, 5ª Turma, j. 05.06.2007.

lado, agora lidando com um *smartphone* e demonstrando-se ciente da enorme quantidade de dados que um celular moderno produz e armazena, o STJ decidiu que a verificação de histórico de conversas do WhatsApp (conteúdo) em celular apreendido após flagrante constitui quebra de sigilo, isto é, é ilegal na falta de ordem judicial autorizadora.[7]

Em tribunais estaduais, a apreciação do tema permanece casuística. Nos Tribunais de Justiça do Paraná[8], do Rio de Janeiro[9] e do Espírito Santo[10], foram encontrados julgados de 2016 que consideram que o acesso a dados de celular apreendido após flagrante prescinde de autorização judicial. A fundamentação utilizada é o art. 6º do Código de Processo Penal (CPP), o qual autoriza autoridades policiais a apreenderem objetos que tiverem relação com o fato delituoso e colherem todas as provas que servirem para o esclarecimento do fato e suas circunstâncias Essa posição também é encontrada na doutrina (Barreto & Férrer, 2016). No Tribunal de Justiça do Distrito Federal[11] e na Quarta Vara Federal Criminal em São Paulo[12] há decisões em favor da necessidade de autorização judicial, tendo em vista que o acesso a dados armazenados em celulares apreendidos constitui "busca virtual" e que celulares modernos deixaram de ser apenas instrumentos de conversação de voz. Na Sétima Vara Federal Criminal em São Paulo, juiz considerou que prova obtida da verificação de mensagens de WhatsApp são ilegais; por outro lado, policiais estariam autorizados a consultar os últimos registros telefônicos para descobrir "comparsas".[13]

7. STJ. Recurso Ordinário em Habeas Corpus nº 51.531/RO. Min. rel. Nefi Cordeiro. 6ª Turma, j. 19.04.2016.

8. TRIBUNAL DE JUSTIÇA DO PARANÁ. Habeas Corpus nº 1547585-9/PR. Rel. Maria José de Toledo Marcondes Teixeira. 5ª Câmara Criminal, j. 14.07.2016.

9. TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. Apelação Criminal 01963693720158190001 RJ. Rel. Marcus Henrique Pinto Basílio, Primeira Câmara Criminal, j. 17.05.2016.

10. TRIBUNAL DE JUSTIÇA DO ESPÍRITO SANTO. Apelação Criminal 00070812320148080030. Rel. Sérgio Luiz Teixeira Gama, 2ª Câmara Criminal, j. 24.02.2016.

11. TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS. Apelação Criminal 20150110776509 0023326-92.2015.8.07.0001. Rel. João Timóteo de Oliveira, 2ª Turma Criminal, j. 03.11.2016.

12. "Provas obtidas em celular de preso em flagrante são ilícitas". Consultor Jurídico. 26 de setembro de 2015. Disponível em: https://bit.ly/2LF7tnP.

13. Policiais causam anulação de provas por vasculharem WhatsApp sem autorização, 10 de março de 2017, Disponível em: https://bit.ly/2Xi1Qhq.

3.3 ACESSO A DADOS PROTEGIDOS POR CRIPTOGRAFIA DE PONTA-A-PONTA

O WhatsApp é o aplicativo de mensagens eletrônicas mais popular no país. Segundo uma pesquisa encomendada pela empresa, 9 entre 10 portadores de celular no Brasil usam o aplicativo (Datafolha, 2016). Principalmente após a implementação da criptografia de ponta-a-ponta pelo aplicativo em abril de 2016, o uso dessa tecnologia de proteção da confidencialidade de mensagens também se tornou motivo de controvérsia no Brasil. Isso porque a implementação dessa criptografia impossibilita a realização de interceptações telemáticas – a captura das conversas de alvos específicos em tempo real, mesmo mediante ordem judicial. Como a empresa também não armazena mensagens pretéritas em seus servidores, não é possível obter nenhum tipo de conteúdo de conversa com a empresa no âmbito de investigações. Tal obstáculo técnico esteve por trás de decisões de bloqueio contra o aplicativo (Abreu, 2016). Para os juízes envolvidos nesses casos, uma tecnologia que impede a realização de interceptações seria contrária à exceção prevista no inciso XII do art. 5º da Constituição Federal, que autorizaria o acesso a comunicações telefônicas em tempo real para fins de investigação criminal ou instrução processual penal. O STF, na Ação Direta de Inconstitucionalidade 5527 e na Arguição de Descumprimento de Preceito Fundamental 403, que analisam a compatibilidade de bloqueios do WhatsApp com a

Constituição Federal, também foi instado a se manifestar sobre a o impasse (Abreu, 2017; Barros, 2016).

Mais uma vez, o que se discute é o alcance da proteção constitucional ao sigilo das comunicações. Se o art. 5, XII só admite quebra de sigilo de comunicações *telefônicas em fluxo,* não seriam apenas interceptações telefônicas que deveriam ser "grampeáveis"? Comunicações de dados seriam invioláveis? Em se tratando de tecnologia imprescindível para a confidencialidade de dados, a discussão não está só limitada a esses termos e envolve também necessariamente privacidade, liberdade de expressão e segurança individual, coletiva e nacional. Apesar da amplitude constitucional da questão, vale também destacar que, atualmente, não há na legislação brasileira obrigação oponível aos desenvolvedores de aplicativos de mensagens no sentido de construírem a arquitetura de seus serviços de modo a permitir interceptações. Isso porque as obrigações previstas na Lei das Interceptações e em resoluções da ANATEL se destinam apenas a empresas de telefonia e provedores de conexão, mas não a provedores de aplicações de Internet (Abreu & Antonialli, 2016).

3.4 ACESSO A DADOS DETIDOS POR EMPRESAS DE TELEFONIA

Além de questões decorrentes da interpretação da constituição, as leis federais que regem a capacidade de vigilância do Estado para fins de aplicação da lei também apresentam problemas. A falta de clareza e salvaguardas e mecanismos de controle insuficientes expõem usuários de telefones celulares à vigilância abusiva.

Uma delas é a Lei das Organizações Criminosas (Lei Federal no. 12850/13), que conferiu a certas autoridades a prerrogativa de acessar dados cadastrais sem ordem judicial. O seu art. 15 dispõe que "o delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito" (grifo adicionado). Tal disposição repete o art. 17-B da Lei dos Crimes de Lavagem de Dinheiro (Lei nº 9.613/99), incluído pela Lei nº 12.683/2012.

Mesmo antes da sanção de tal previsão legal, autoridades policiais já defendiam a interpretação segundo a qual dados cadastrais não seriam resguardados pelos dispositivos constitucionais que protegem a privacidade e o sigilo das comunicações (art. 5, incisos X e XII), porque não se confundiriam com conteúdo de comunicações telefônicas. Em 2016, acolhendo tal posicionamento, o Tribunal Regional Federal da 3ª Região sustentou que a operadora Claro, que em 2013 impetrou mandado de segurança contra ofícios da Polícia Federal requisitando dados cadastrais de chips apreendidos, tem a obrigação de revelar dados de cadastro mesmo sem ordem judicial.[14]

Cabe ainda ressaltar que, apesar de a possibilidade de acesso a tais informações por mera requisição às empresas estar prevista nas leis sobre crimes de *organização criminosa* e de *lavagem de dinheiro*, as autoridades citadas pretendem também que o acesso por requisição não esteja limitado apenas a investigações e persecuções no âmbito de tais crimes, uma vez que o legislador não teria expressamente limitado tais competências apenas aos fins das leis em que se inserem (Aras, 2012). Na prática, tais autoridades utilizam essas previsões para fun-

14. TRIBUNAL REGIONAL FEDERAL 3ª REGIÃO. Apelação/Reexame Necessário nº 0000108-56.2013.4.03.6110/SP. Rel. Des. Johonson di Salvo, j. 03.03.2016. Disponível em: https://bit.ly/2JkqdpI . A decisão modificou sentença de primeira instância em favor da Claro.

damentarem requisições de dados a prestadoras de serviços de telefonia; apenas se a companhia negar o pedido é que a questão é analisada judicialmente. A falta de quaisquer requisitos formais ou materiais para entregar a informação deixa esses procedimentos ainda mais discricionários.

Desde a promulgação da Lei das Organizações Criminosas, as autoridades competentes, mas principalmente delegados de polícia, também têm requisitado registros telefônicos a companhias telefônicas *sem* autorização judicial, com base em interpretação combinada dos arts. 15, 17 e 21 dessa Lei.

Pelo já citado art. 15, "o delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço" mantidos por empresas telefônicas e provedores de internet. O art. 17 obriga, entretanto, as companhias à guarda de "registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais" por 5 anos, os quais serão mantidos "à disposição das autoridades mencionadas no art. 15". O *caput* do art. 21, por sua vez, criminaliza a recusa ou omissão de "dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia, no curso de investigação ou do processo", com pena de reclusão de 6 meses a 2 anos, e multa. Diante disso, tais autoridades têm requisitado, além dos dados cadastrais, registros telefônicos (e alguns até dados de localização), sem autorização judicial. Requisições diretas são feitas a empresas, sob ameaça de que serão punidas, caso não colaborem.

Ação Direta de Inconstitucionalidade (ADI 5063/DF, acima citada) foi proposta perante o Supremo Tribunal Federal contra tais artigos pela Associação Nacional de Operadoras Celulares (ACEL), sob fundamento de violação ao direito à privacidade e ao princípio da legalidade, dada a insegurança jurídica acarretada pela imprecisão das normas.[15] A ação, proposta originalmente em 2013, ainda está pendente de julgamento.

15. A petição da ACEL e exemplos de intimações recebidas por operadoras com base nessa (interpretação da) lei podem ser encontradas em CONJUR, "Operadoras reclamam de pedidos de delegados para quebra de sigilo telefônico", 29 de outubro de 2014, Sobre a ação, ver notícia do site do STF, Disponível em https://bit.ly/30dimRt .

3.5 ACESSO A DADOS DETIDOS POR PROVEDORES DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Desenvolvido no contexto de um extenso debate público e promulgado em 2014, o Marco Civil da Internet (Lei Federal nº 12965/14) é de extrema importância na determinação da legalidade da vigilância estatal na Internet. Entre seus muitos princípios e regras, a lei desenvolve um regime claro de acesso a dados cadastrais, logs e conteúdo de comunicações. Lentamente, porém, encontraram-se maneiras de explorar lacunas e provisões ambíguas.

Ilustração disso são algumas decisões de tribunais estaduais que exigiram a retenção e determinaram a divulgação de informações relacionadas à "porta lógica de origem" por conexão e provedores de aplicações de internet (Brito Cruz, 2016; Lopes, 2016; Opice Blum, 2016). Essa informação não faz parte das definições contidas na lei de "registros de conexão" e "registros de acesso a aplicação", que englobam apenas o endereço IP, data e hora. Afirmando que aquela é informação necessária para "identificar" os usuários – o "propósito" dos mandados de retenção de dados –, a divulgação dessas informações foi confirmada pelos tribunais. De outro lado, o art. 10, § 3º, do Marco Civil da Internet ao menos prevê explicitamente que a disponibilização dos registros de conexão à

Internet e de acesso a aplicações só poderá ser feita por ordem judicial, proteção repetida nos arts. 13, § 5º e 15, § 3º. O art. 22, por sua vez, delimita os fins a que isso poderá ocorrer, qual seja a formação de "conjunto probatório em processo judicial cível ou penal", e estabelece os requisitos a que deve atender o requerimento da "parte interessada" para a concessão da ordem judicial: fundados indícios da ocorrência do ilícito; justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e período ao qual se referem os registros.

Em termos de acesso a dados cadastrais, o Marco Civil dispõe, no § 3º do seu art. 10, que o respeito à proteção a dados pessoais e comunicações privadas garantido no *caput* do artigo "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". Acerca de tal previsão, não há clareza sobre quem são essas 'autoridades administrativas' com poder de requerer diretamente dados cadastrais, o que permite que diversas autoridades governamentais reivindiquem essa prerrogativa para si.

Finalmente, a quebra de sigilo de conteúdo de comunicações eletrônicas em posse de provedores de aplicações de Internet (tais como Google e Facebook) está também prevista no Marco Civil da Internet, nos arts. 7º, III e 10, § 2º, os quais explicitam a necessidade de ordem judicial para tanto. Ao contrário do que ocorre para o fornecimento de registros (art. 22), entretanto, a lei não trata explicitamente dos requisitos formais e materiais que devem ser satisfeitos para que a ordem judicial seja concedida (Mendes & Pinheiro, 2015), o que dá margem a abusos e aplicações casuísticas.

3.6 ACESSO A DADOS DE LOCALIZAÇÃO

Não existe um regime geral de acesso a dados de localização no Brasil. Na prática, as autoridades de segurança pública reivindicam poderes de investigação gerais para fazer pedidos de dados de localização; somente se uma empresa se recusar a cumprir é que o assunto será submetido a um tribunal para revisão. Como a maioria das empresas desafia essas demandas quando não acompanhadas por uma autorização judicial, a proteção desse tipo de informação fica a critério de juízes.

Pelo menos dois exemplos ilustram quão vulnerável é a situação para usuários de telefonia móvel. Primeiro é o de uma decisão do Tribunal de Justiça do Rio Grande do Sul em julho de 2007, que admitiu a possibilidade de quebra de sigilo de dados de localização de usuário de celular devedor de alimentos, nos autos de execução dessa obrigação. O réu em tal ação foi condenado ao pagamento de pensão alimentícia; não realizando o pagamento, nem justificando a impossibilidade de fazê-lo, teve sua prisão decretada. Sua localização foi tentada repetidas vezes, sem sucesso. Em face disso, e em nome da "proteção integral a crianças e adolescentes", a desembargadora admitiu que uma "interceptação telefônica", como a chamou, fosse efetuada com o fim de levantar dados sobre a localização do devedor a partir de seu número de celular.[16] Dado que não existe uma disposição legal nem jurisprudência que limita as violações da confidencialidade dos dados de localização aos casos criminais, e excluindo casos cíveis, esse acesso foi permitido.

16. TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. Agravo de Instrumento n. 70018683508, Desembargadora Maria Berenice Dias. Julgamento: 28.07.07. Disponível em: https://bit.ly/2XSnFIU.

O segundo exemplo está relacionado a um roubo a uma empresa de transportes de valores e de segurança em Ribei-

rão Preto em 2016. A polícia pediu judicialmente que que o Google, a Apple e a Microsoft fornecessem dados de todos os usuários que estiveram a até 500m do local do roubo, em um intervalo de 4 dias. A autoridade policial queria IMEIs (identificadores únicos dos aparelhos celulares), dados de usuário de contas de e-mail e os registros de acesso a elas, histórico de localização e deslocamento, histórico de buscas, senhas e fotos armazenadas na nuvem, tudo dos últimos 30 dias. O juiz de primeira instância concordou com parte do pedido e autorizou a quebra de sigilo dos dados cadastrais, dos lugares guardados no Google Maps e da localização e histórico de viagem dos últimos 30 dias de todos os usuários que estiveram nesses arredores por aqueles dias; o Google não acatou, e impetrou mandado de segurança no Tribunal de Justiça de São Paulo, mas apenas obteve uma redução do escopo do pedido; ainda não se conformando, levou o caso ao Superior Tribunal de Justiça. Só então, em uma liminar, o pedido foi revogado. [17]

17. STJ. Pedido de Tutela Provisória nº 292-SP (2017-0034057-6), Min. Antonio Saldanha Palheiro, j. 24.02.2017. Disponível em: https://bit.ly/2JapWHd.

Os únicos parâmetros que existem em lei para o fornecimento de dados de localização foram adicionados ao CPP em dezembro e possuem aplicação bastante específica. O novo art. 13-B dispõe que "se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso".

Nos detalhes, entretanto, a redação do dispositivo apresenta ambiguidades que podem dar margem a abusos, como por exemplo: *(i)* o *caput* do art. 13-B menciona "crimes relacionados a tráfico de pessoas", sem indicar expressamente a que tipos penais se refere; *(ii)* o mesmo artigo menciona também "meios técnicos" que permitam localizar pessoas: "sinais, informações e outros"; sem especificar quais seriam as "informações", muito menos o que se deve entender por "outros". De acordo com a definição genérica, vale tudo para localizar alguém – só não estaria diretamente incluída no pacote a quebra de sigilo de conteúdo de comunicações, que precisam de autorização específica (art. 13-B, § 2º, I). De acordo com o § 2º do art. 13-B, o "sinal" deve ser fornecido por período não superior a 30 dias (inciso II), renovável uma única vez por igual período. Em uma redação confusa, o inciso III do mesmo parágrafo afirma que "para prazos superiores, será necessária ordem judicial", o que poderia dar lugar à interpretação de que não seria necessária a ordem para prazo inferior – ao contrário do que o caput requer.

Em janeiro de 2017, a Associação Nacional das Operadoras de Celular (ACEL) propôs ação direta de inconstitucionalidade (ADI 5642) contra esses dispositivos, por violarem os art. 5º, incisos X e XII da Constituição (Macedo & Coutinho, 2017).

04. CONCLUSÃO

A regulação de intercepções em tempo real de comunicações de longa distância e da instalação de grampos é um marco no regime legal de vigilância em muitos países. O Brasil não é uma exceção com sua Lei das Intercepções. No entanto, o uso da telefonia e dos próprios telefones mudou drasticamente desde a promulgação de tal legislação em 1996.

Os telefones celulares, de propriedade da grande maioria dos cidadãos brasileiros, são hoje um tesouro de informações de comunicação e, portanto, de evidências valiosas para agentes de segurança pública. Eles não são usados mais apenas

para ligar. Eles armazenam enormes quantidades de informações pessoais que produzimos voluntariamente (nossos textos, fotos, notas, músicas, lista de contatos, histórico de chamadas). Eles também permitem que seus titulares usem serviços de Internet através de aplicativos ou navegadores, que também produzem e armazenam dados no dispositivo ou em outros locais. Inadvertidamente para as pessoas, eles também estão constantemente gerando outros tipos de informação, como dados de localização, para seu próprio funcionamento.

O Brasil carece, entretanto, de um quadro forte que estabeleça limites para o acesso de autoridades de segurança pública ao conteúdo das comunicações e aos metadados armazenados de celulares. Isso significa que, embora a "revolução do smartphone" represente um marco em termos de acesso ao conhecimento e às comunicações no Brasil, também expõe os cidadãos brasileiros - usuários de smartphones - a uma vigilância maior e mais invasiva devido a leis desatualizadas, lacunas e jurisprudência amigável à vigilância. Repensar este quadro jurídico é fundamental para salvaguardar as liberdades individuais e evitar o encolhimento do espaço cívico em uma sociedade conectada (por smartphones).

05. REFERÊNCIAS

ABREU, J. de S. (17 de outubro de 2016). From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp. Disponível em http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/

ABREU, J. de S. (26 de junho de 2017). Public hearing on encryption and WhatsApp blockages: the arguments before the STF. Disponível em *http://bloqueios.info/en/public-hearing-on-encryption-and-whatsapp-blockages-the-arguments-before-the-stf/* Acesso em: 8 de agosto de 2017.

ABREU, J. de S., & Antonialli, D. (2016, July 7). State Surveillance of Communications in Brazil FAQ. Disponível em *https://necessaryandproportionate.org/state-surveillance-communications-brazil-faq* Acesso em: 8 de agosto de 2017.

ABREU, J. de S., & Antonialli, D. (2017). *Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais*. São Paulo: InternetLab. Disponível em http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf

Agência Nacional de Telecomunicações. (2016). *Relatório Anual ANATEL 2016*. Agência Nacional de Telecomunicações.

ANTONIALLI, D., Brito Cruz, F., & Valente, M. G. (24 de novembro de 2016). Smartphones: treasure chests of the Lava-Jato investigation. Disponível em http://www.internetlab.org.br/en/opinion/smartphones-treasure-chests-of-the-lava-jato-investigation/

ARAS, V. (2012). A investigação criminal na nova lei de lavagem de dinheiro. *Boletim IBCCRIM, 237*. Disponível em https://www.ibccrim.org.br/boletim_artigo/4671-A-investigao-criminal-na-nova-lei-de-lavagem-de-dinheiro

BARRETO, A. G., & Férrer, E. F. de A. (2016). Perícia em celular: necessidade de autorização judicial? *Direito & TI*. Disponível em http://direitoeti.com.br/artigos/pericia-em-celular-necessidade-de-autorizacao-judicial/

BARROS, P. P. (21 de novembro de 2016). ADPF 403 in STF: Are WhatsApp Blockings Constitutional? Disponível em: http://bloqueios.info/en/adpf-403-in-stf-are-whatsapp-blockings-constitutional/

BRITO CRUZ, F. (1 de junho de 2016). Comentário, Porta Lógica e provedores de aplicação. Disponível em http://omci.org.br/jurisprudencia/99/porta-logica-e-provedores-de-aplicacao/

Comitê Gestor da Internet no Brasil. (2011). *TIC Domicílios e Empresas 2010 - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil*. São Paulo: Comitê Gestor da Internet no Brasil. Disponível em http://www.cetic.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2010.pdf

Comitê Gestor da Internet no Brasil. (2012). *TIC Domicílios e Empresas 2011 - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil*. São Paulo: Comitê Gestor da Internet no Brasil. Disponível em http://www.cetic.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2011.pdf

Comitê Gestor da Internet no Brasil. (2013). *TIC Domicílios e Empresas 2012 - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil*. São Paulo: Comitê Gestor da Internet no Brasil. Disponível em http://www.cetic.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2012.pdf

Comitê Gestor da Internet no Brasil. (2014). *TIC Domicílios e Empresas 2013 - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil*. São Paulo: Comitê Gestor da Internet no Brasil. Disponível em http://www.cetic.br/media/docs/publicacoes/2/TIC_DOM_EMP_2013_livro_eletronico.pdf

Comitê Gestor da Internet no Brasil. (2015). *TIC Domicílios e Empresas 2014 - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil*. São Paulo: Comitê Gestor da Internet no Brasil. Disponível em http://www.cetic.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf

Comitê Gestor da Internet no Brasil. (2016). *TIC Domicílios e Empresas 2015 - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil*. São Paulo: Comitê Gestor da Internet no Brasil. Disponível em http://www.cetic.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf

Datafolha. (2016). *Hábitos de Uso de Aplicativos, População brasileira, 13 anos ou mais*. Datafolha. Disponível em http://media.folha.uol.com.br/datafolha/2017/01/27/da39a3ee5e6b4b0d3255bfef95601890afd80709.pdf

FERRAZ JUNIOR, T. S. (1993). Sigilo de Dados: o direito à privacidade and os limites da função fiscalizadora do Estado. *Revista Da Faculdade de Direito Da Universidade de São Paulo, 88*, 439–459.

FERREIRA FILHO, M. G. (2009). *Curso de Direito Constitucional* (35th ed.). São Paulo: Saraiva.

LOPES, M. F. (17 de dezembro de 2016). Entrave tecnológico provoca impasse sobre o Marco Civil e anonimato. Disponível em http://www.conjur.com.br/2016-dez-17/entrave-tecnologico-provoca-impasse-marco-civil-anonimato

MACEDO, F., & Coutinho. (25 de janeiro de 2017). Operadoras de celular vão ao Supremo contra lei que obriga repasse de dados a delegados e promotores. *O Estado de São Paulo*. Disponível em http://politica.estadao.com.br/blogs/fausto-macedo/operadoras-de-celular-vao-ao-supremo-contra-lei-que-obriga-repasse-de-dados-a-delegados-e-promotores/.

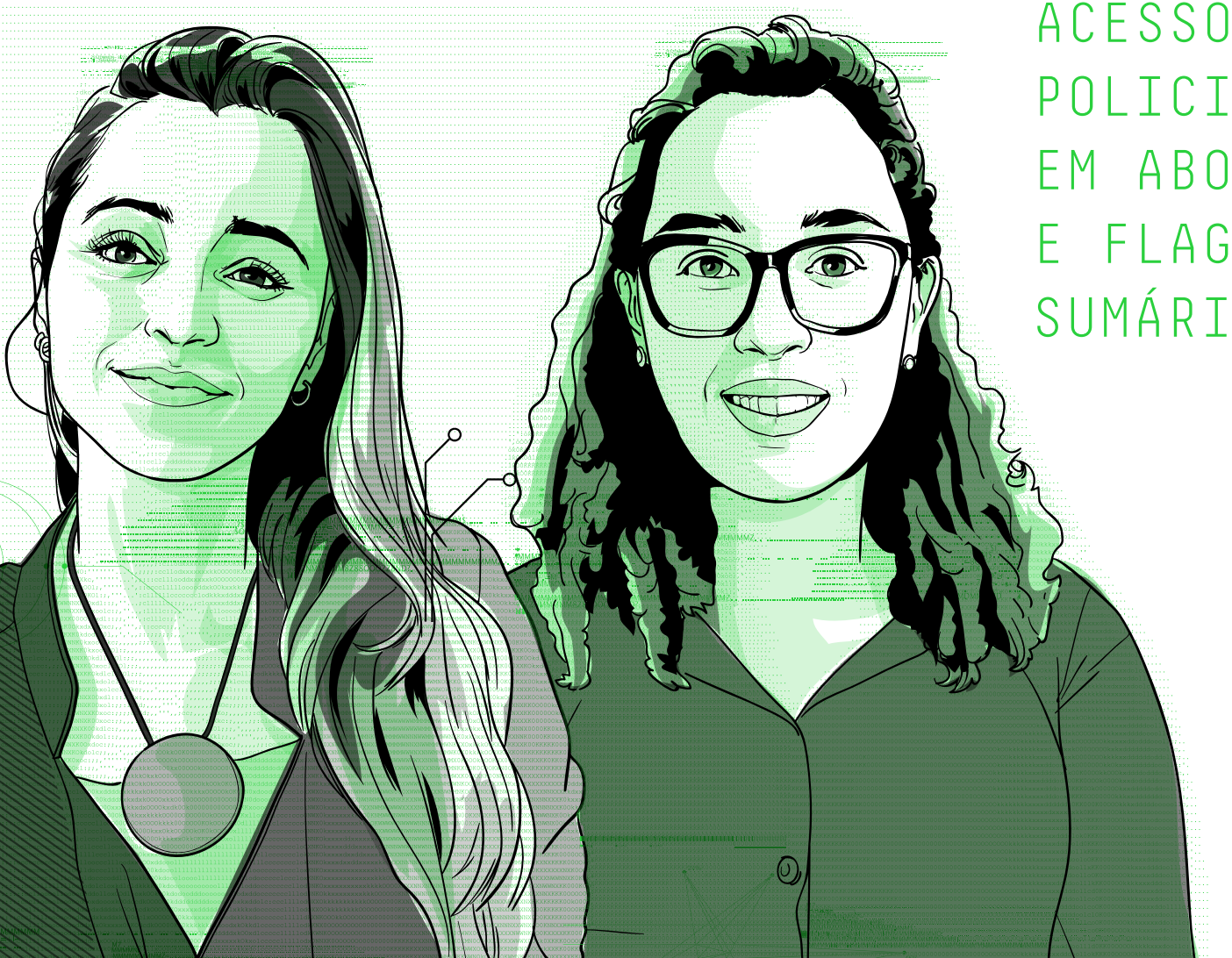
MARANHÃO, J. (12 de maio de 2016). O acesso ao WhatsApp pela operação Lava Jato. Disponível em http://jota.info/artigos/o-acesso-ao-whatsapp-pela-operacao-lava-jato-05122016

MENDES, G. F., & Pinheiro, J. B. (2015). Interceptações e privacidade: novas tecnologias e a Constituição. In G. F. Mendes & I. W. Sarlet (Eds.), *Direito, Inovação e Tecnologia* (Vol. 1). São Paulo: Saraiva.

OPICE BLUM, R. (26 de outubro de 2016). Portas Lógicas de Origem: identificação e caos jurídico. Disponível em http://jota.info/artigos/direito-digital-portas-logicas-de-origem-dificuldade-de-identificacao-e-o-caos-juridico-26102016

SIDI, R. (2015). A interceptação de e-mails e a apreensão física de e-mails armazenados. *Revista Fórum de Ciências Criminais, 4*, 101–121.

SILVA, J. A. (2008). *Curso de Direito Constitucional Positivo* (32nd ed.). São Paulo: Malheiros Editores.



05.

ACESSO DE AUTORIDADES POLICIAIS A CELULARES EM ABORDAGENS E FLAGRANTES: SUMÁRIO EXECUTIVO

Nathalie Fragoso
Maria Luciano

Este é um resumo dos principais resultados do artigo "Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais", publicado na Revista Brasileira de Ciências Criminais, v. 154, 2019, de autoria de Dennys Antonialli, Jacqueline de Souza Abreu, Heloísa Maria Machado Massaro e Maria Luciano.

Listas de contatos, fotos, bloco de notas, listas de leitura, histórico de páginas visitadas, dados de localização, e-mail, mensagens instantâneas e redes sociais... Dados e metadados que espelham muito e cada vez mais a vida privada estão hoje armazenados em celulares. Não à toa, a busca pelos rastros de eventual atividade criminosa através do acesso por agentes do Estado a celulares e ao conteúdo aí acumulado tem ensejado sérias discussões sobre a extensão da proteção à privacidade e os limites da atuação estatal.

01. O QUADRO NORMATIVO

O art. 5, XII, da CF garante o sigilo das comunicações, ressalvando a possibilidade de "quebra" por ordem judicial para fins de investigação e instrução processual penal. A Lei de Interceptações (Lei 9.296/1996), que o regulamenta, refere-se a procedimentos de quebra de sigilo de comunicações *em andamento* mediante a colaboração de empresas de telecomunicações e/ou a instalação de grampos e escutas ambientais.

Não há consenso, no entanto, quanto à extensão da proteção oferecida pelo art. 5º, incisos X e XII da CF, a comunicações *armazenadas*. A disciplina infralegal estabelece que para o acesso a dados guardados por um intermediário (como provedores de aplicações de Internet) é necessária "ordem judicial" (art. 7º, III) nas hipóteses e na forma estabelecida por lei (Marco Civil da Internet, art. 10, § 2º). A controvérsia persiste em relação aos dados armazenados nos dispositivos móveis.

Nesse contexto, foi exarada a decisão do Superior Tribunal de Justiça (STJ) no HC 51.531/RO. Nela, o tribunal deliberou que a verificação de histórico de conversas do WhatsApp em celular apreendido após flagrante constitui quebra de sigilo, sendo ilegal se realizada sem autorização judicial prévia. A decisão é paradigmática, no que estabelece em termos da proteção a dados digitais armazenados, especialmente porque até então os tribunais superiores conferiam parca proteção a informações armazenadas em dispositivos eletrônicos.

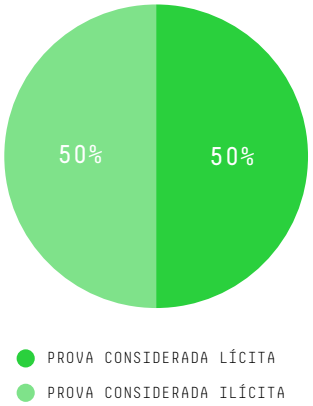
Sob o impulso desta decisão e com o objetivo de compreender a forma como vem sendo enfrentada a questão, cujas implicações são extremamente relevantes para a caracterização das garantias penais realmente experimentadas no país, investigamos a forma como tribunais estaduais brasileiros têm tratado os elementos de prova obtidos através do acesso a dados armazenados em dispositivos celulares por autoridades policiais.

02. O PADRÃO DECISÓRIO DOS TRIBUNAIS ESTADUAIS BRASILEIROS EM MATÉRIA DE ACESSO DE AUTORIDADES POLICIAIS A CELULARES

A pesquisa não alimentou pretensão estatística. Buscou, antes, analisar as decisões coletadas em repositórios eletrônicos de jurisprudência de dez tribunais estaduais (AM, RR, RN, RS, PR, CE, MS, GO, SP e RJ), a partir dos termos de busca "quebra E sigilo E WhatsApp". Os termos refletem, por um lado, a centralidade dos termos "quebra de sigilo" na prática jurídica nacional e, por outro, a popularidade conquistada pelo aplicativo como meio de comunicação instantânea. Foram, finalmente, selecionados e analisados os casos em que o acesso a celulares ocorreu em abordagens policiais ou após flagrante: 49 acórdãos, todos julgados no período de 12/05/2016 a 14/09/2017.

2.1 ACESSO POLICIAL A DADOS ARMAZENADOS EM CELULAR DURANTE ABORDAGENS POLICIAIS

12 dos 49 acórdãos analisados tratavam do acesso a dados armazenados em celulares durante abordagens policiais, i. e., sem prévio flagrante. Em 50% desses casos a prova obtida foi considerada lícita.



Nas decisões que declararam licitude, ou seja, admitiram e valoraram a prova, estiveram presentes argumentos sobre a extensão e aplicabilidade das garantias constitucionais de sigilo das comunicações e de proteção à intimidade e vida privada; o suposto consentimento do acusado; e o princípio do prejuízo.

Em 4 dos 6 casos, os tribunais diferenciam as comunicações em fluxo das comunicações armazenadas, argumentando que a proteção do art. 5º, XII, da Constituição Federal não se aplica aos dados armazenados nos celulares. Em dois desses casos[1], o HC 91.867/PA de 2012 - no qual o STF entendeu o art. 5º, XII, da Constituição Federal protege apenas as comunicações de dados e não os dados armazenados - foi apresentado jurisprudência, assim como O HC 66.368/PA do STJ de 2007, no mesmo sentido.

1. Acórdãos: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Apelação nº 0010539-31.2015.8.16.0017. Rel. Rogério Kanayama, 3ª Câmara Criminal, j. 15.12.2016; TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Habeas Corpus nº 0029887-52.2016.8.16.0000. Rel. Arquelau Araujo Ribas, 3ª Câmara Criminal, j. 27.10.2016.

Em um dos dois casos no qual o suposto consentimento do acusado foi mencionado, ele foi inferido a partir do fornecimento da senha e interpretado como permissão que afastaria o sigilo que pudesse incidir sobre seu aparelho celular[2]. No outro, foi deduzido a partir da ausência de informações nos autos de que o acesso não teria sido autorizado e foi empregado, junto à ponderação de direitos, como argumento para afastar a proteção do sigilo sobre os dados consultados[3]. Já os dois casos[4] em que o princípio do prejuízo fundamentou a decisão, considerou-se que os dados acessados não foram decisivos para a conformação da decisão final, dada a existência de outros elementos nos autos suficientes para fundamentá-la.

2. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Apelação nº 0028132-22.2014.8.16.0013. Rel. José Carlos Delacqua, 2ª Câmara Criminal, j. 14.09.2017.

3. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Habeas Corpus nº 0013171-34.2017.8.26.0000. Rel. Edison Brandão, 4ª Câmara de Direito Criminal, j. 16.05.2017.

4. Acórdãos: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Habeas Corpus nº 0029887-52.2016.8.16.0000. Rel. Arquelau Araujo Ribas, 3ª Câmara Criminal, j. 27.10.2016; TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Habeas Corpus nº 2122381-20.2016.8.26.0000. Rel. Francisco Orlando, 3ª Câmara de Direito Criminal, j. 01.08.2016.

Por outro lado, o HC 51.531/RO do STJ foi o precedente invocado em 100% casos que declararam a nulidade da prova obtida mediante acesso ao celular durante abordagens policiais, sem prévia ordem judicial. Tais acórdãos sustentam a aplicabilidade do sigilo das comunicações às conversas de WhatsApp (cujo histórico fica registrado e armazenado em celulares), embora não revisem a distinção da proteção conferida a comunicações armazenadas e comunicações em fluxo.

Em dois desses casos, o "consentimento" foi considerado para declarar a ilicitude da prova. Em um deles, o relator não

considerou crível que, após nada ter sido encontrado em busca pessoal, o abordado autorizaria o acesso às mensagens de seu aparelho celular e se auto-acusaria[5]. De modo semelhante, no outro caso, o relator argumenta que não se pode falar em consentimento na relação entre cidadão e autoridade policial, quando esta pede que aquele forneça a senha de desbloqueio[6].

Um aspecto interessante a ser notado em todas as decisões é a quase total ausência de considerações acerca da alegada "atitude suspeita" que teria levado à busca pessoal e *virtual*. Os tribunais, de modo geral, não debatem essa questão, nem discorrem sobre a possibilidade dessa "suspeita" justificar a consulta aos dados armazenados em celulares. Isso fica evidenciado pelo fato de que nem sempre o comportamento do abordado considerado pela autoridade policial como estando em "atitude suspeita" foi reproduzido nas decisões, de modo que em vários casos a única informação extraída dos acórdãos foi que a abordagem ocorreu durante patrulhamento de rotina e/ou por "atitude suspeita" do acusado. Dos casos nos quais essa "atitude" foi detalhada na decisão, observamos que foi considerado em "atitude suspeita": o acusado na porta de uma borracharia[7]; o indivíduo com tornozeleira eletrônica nervoso diante da presença policial[8]; o indivíduo em uma motocicleta entregando algo a outro que estava em pé[9];

5. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. Apelação nº 0000424-25.2016.8.19.0051. Rel. Marcus Basilio, 1ª Câmara Criminal, j. 13.12.2016.

6. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL. Apelação nº 0060412-91.2017.8.21.7000. Rel. Diógenes V. Hassan Ribeiro, 3ª Câmara Criminal, j. 17.05.2017

7. TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. Apelação nº 0066620-61.2015.8.19.0002. Rel. Katia Maria Amaral Jangutta, 2ª Câmara Criminal, j. 25.07.2017.

8. TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Apelação nº 0028132-22.2014.8.16.0013. Rel. José Carlos Delacqua, 2ª Câmara Criminal, j. 14.09.2017.

9. TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Apelação nº 0010539-31.2015.8.16.0017. Rel. Rogério Kanayama, 3ª Câmara Criminal, j. 15.12.2016.

/ QUANDO HOUVE DISCUSSÃO SOBRE CONSENTIMENTO, NÃO SE TRATOU DE DEMONSTRÁ-LO; PELO CONTRÁRIO, ELE FOI PRESUMIDO /

/ OS DADOS DE UM INDIVÍDUO ESTARÃO TÃO VULNERÁVEIS QUANTO EXPOSTO FOR SEU TITULAR A ABORDAGENS POLICIAIS E AO CONTROLE PENAL /

dois homens que mexiam no interior de um caminhão[10]; e um automóvel do qual algo foi atirado pela janela[11]. Em outros casos, não se falou em "atitude suspeita", mas em prévia denúncia anônima que levou à abordagem.[12]

No único caso[13] em que o juiz chancela expressamente a abordagem policial decorrente de suposta "atitude suspeita" - "[...] com tornozeleira eletrônica, em liberdade condicional, e (...) muito nervoso com a ação policial [...]" -, a busca *virtual* teve sua licitude justificada não nos termos da abordagem, mas em razão de uma suposta "situação de flagrância". Diverso é o entendimento do também único caso[14] no qual o art. 240, §2º do Código de Processo Penal foi invocado para questionar, e considerar ilegal, a busca pessoal e o consequente acesso ao aparelho celular. Neste, o tribunal sustentou que o requisito da lei processual de que haja "fundada suspeita" demanda elementos objetivos passíveis de serem confirmados por testemunhas. Não obstante, o tribunal não expandiu a análise para o complemento dessa "fundada suspeita", previsto no referido dispositivo legal; nem debateu se, cumpridos os requisitos para a busca pessoal sem ordem judicial, o acesso ao celular, ou seja, a busca virtual, também estaria autorizado.

10. TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Habeas Corpus nº 0029887-52.2016.8.16.0000. Rel. Arquelau Araujo Ribas, 3ª Câmara Criminal, j. 27.10.2016.

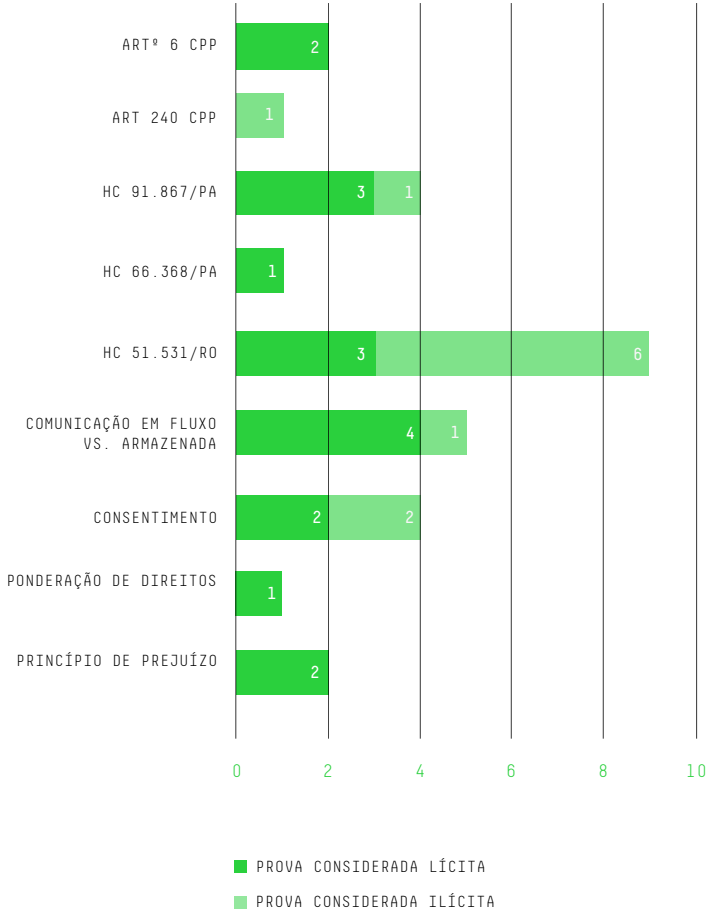
11. TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Habeas Corpus nº 2122381-20.2016.8.26.0000. Rel. Francisco Orlando, 3ª Câmara de Direito Criminal, j. 01.08.2016.

12. TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Apelação nº 0000074-13.2016.8.26.0578. Rel. Walter da Silva, , j. 09.02.2017; TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL. Apelação nº 0060412-91.2017.8.21.7000. Rel. Diógenes V. Hassan Ribeiro, j. 17.05.2017.

13. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Apelação nº 0028132-22.2014.8.16.0013. Rel. José Carlos Delacqua, 2ª Câmara Criminal, j. 14.09.2017.

14. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS. Apelação nº 0233896-74.2014.8.04. Rel. Djalma Martins Costa, 2ª Câmara Criminal, j. 10.07.2016.

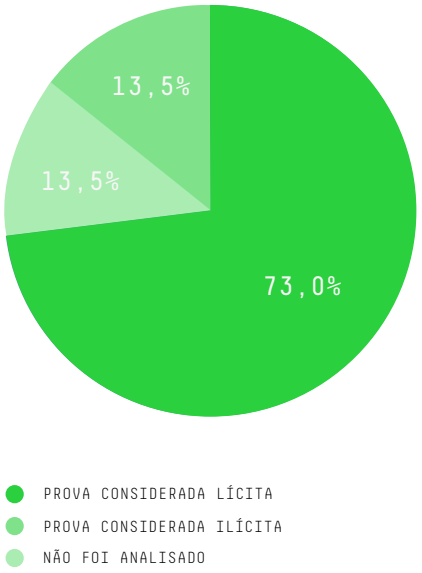
Por fim, cabe notar que o Marco Civil da Internet não é citado em nenhuma das decisões em que há acesso de autoridades policiais a celulares durante abordagens.



2.2 ACESSO POLICIAL A DADOS ARMAZENADOS EM CELULAR APÓS FLAGRANTE DELITO

Entre os 49 acórdãos selecionados, 37 tratam de acesso a celulares ocorridos em decorrência de flagrante delito. Nesse contexto, as autoridades policiais estão autorizadas à busca de objetos e produtos do crime portados pelo detido, para instruir o auto de prisão em flagrante e garantir a segurança das próprias autoridades. A questão que se coloca, entretanto, é se é permitido às autoridades policiais *estender* os limites da busca pessoal "independentemente de mandado" aos dados armazenados no celular.

Em 86,5% dos casos, a prova obtida pelo acesso ao celular após prisão em flagrante não teve sua nulidade declarada. Em 73%, a prova é considerada lícita pelo julgador, e em 13,5%, a alegação de nulidade não é analisada.



O principal argumento utilizado nas decisões é o art. 6º do CPP. Ele determina que, logo que tiver conhecimento de infração penal, a autoridade policial deverá apreender os objetos que tiverem relação com o fato (após liberados por peritos) e colher todas as provas que servirem ao seu esclarecimento e circunstâncias (art. 6º, II e III). A maioria das decisões (21 em 27) que consideraram a prova lícita se baseou nesse argumento para afastar qualquer alegação de quebra ilegal de sigilo.

O art. 240, §2º, do CPP - que autoriza a busca pessoal quando houver fundada suspeita de que o indivíduo esteja ocultando consigo carta, cujo conteúdo possa ser útil ao esclarecimento dos fatos, ou qualquer outro elemento de convicção - é pouco suscitado nas decisões analisadas (4 vezes). Em três acórdãos, este fundamento é acompanhado pelo art.6º,[15] pelo art. 244[16], ou por ambos,[17] do CPP. Assim, no total, em 85,18% dos casos o flagrante delito e a autorização da busca constituem o principal respaldo da conduta policial no acesso a dados de celular.

O debate acerca da extensão da inviolabilidade das comunicações telefônicas e de dados garantida pelo art. 5º, XII, da Constituição Federal também aparece com frequência. Em 14 das decisões analisadas, os julgadores diferenciaram as comunicações em fluxo das comunicações armazenadas, argumentando que os dados armazenados em celulares não seriam alcançados por essa proteção constitucional. Além disso, a ponderação dos direitos e garantias constitucionais apareceu de maneira complementar, na argumentação de que os direitos e garantias constitucionais não são absolutos e na ponderação entre as previsões constitucionais sobre sigilo das comunicações e segurança/ordem pública.

Essas três principais fundamentações acima citadas - art. 6º, II e III do CPP, a distinção da proteção entre comunicações em fluxo e armazenadas e a ponderação entre direitos e garantias constitucionais - foram invocadas, também, pelo Ministro Gilmar Mendes no HC 91.867/PA[18], julgado em abril de 2012, no qual o STF considerou lícita a consulta a registros telefônicos armazenados no celular de corréu acusado de homicídio, após a prisão em flagrante. Antes de chegar ao STF, esse caso já havia sido julgado pelo STJ no HC 66.368/PA[19], em junho de 2007. Estes acórdãos são a principal jurisprudência mobilizada para declaração da licitude da prova produzida mediante acesso a dados armazenados em celulares após flagrante delito, estando presente em 14 casos.

Como reforço argumentativo constatou-se menções ao "princípio do prejuízo" - previsto no art. 563 e art. 566, ambos do CPP - e ao consentimento do acusado.

Nos casos em que houve discussão sobre consentimento, não se tratou de demonstrá-lo; pelo contrário, as decisões se basearam na inexistência de indícios de que não tenha havido consentimento. Em 6 dos 8 casos, a ausência de informação ou prova nos autos de que tenha ocorrido coação policial ou de que o acusado tenha se oposto ao acesso a seu celular foi invocada como indício de consentimento que autorizaria o acesso aos dados armazenados. Nos demais, o suposto fornecimento da senha de acesso[20] foi considerado como indicativo suficiente.

15. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Embargos de Declaração nº 0001279-59.2015.8.26.0272/50000. Rel. Pinheiro Franco, 5ª Câmara de Direito Criminal, j. 01.12.2016.

16. O art. 244 do Código de Processo Penal é fundamentação citada nos casos: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Habeas Corpus nº 0021238-64.2017.8.16.0000, Rel. Antônio Carlos Ribeiro Martins, j.10.08.2017; TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Habeas Corpus nº 0034498-48.2016.8.16.0000. Rel. Lidia Maejima, 4ª Câmara Criminal, j. 08.12.2016.

17. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Habeas Corpus nº 0034498-48.2016.8.16.0000. Rel. Lidia Maejima, 4ª Câmara Criminal, j. 08.12.2016.

18. STF. Habeas Corpus nº 91.867/PA, Brasília, DF, 24 de abril de 2012. Disponível em: https://bit.ly/2JkrFIJ. Acesso em: 23.02.2018.

19. STJ. Habeas Corpus nº 66.368/PA, Brasília, DF, 5 de junho de 2007. Disponível em: https://bit.ly/322SV7b. Acesso em: 23.02.2018.

20. Acórdãos: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Apelação nº 17277-35.2015.8.16.0017. Rel. Dilmari Helena Kessler, 4ª Câmara Criminal, j. 31.08.2017; TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ. Apelação nº 0067551-30.2015.8.06.0001. Rel. Francisco Martonio Pontes de Vasconcelos, 2ª Câmara Criminal, j. 07.06.2017.

Apesar de pouco considerado, o entendimento do STJ no HC 51.531/RO não foi completamente esquecido. Dentre os casos em que a prova foi considerada lícita, em 5 deles, o precedente foi citado *e* afastado, sendo que em 3 (desses 5) o tribunal considerou que não se aplicaria no caso concreto[21]. Nos demais, em um o relator discordou do posicionamento adotado pelo STJ[22]; e, no outro,[23] a nulidade foi afastada com base na alegação de consentimento e na teoria da descoberta inevitável. Vale ressaltar que todos os acórdãos analisados nessa categoria foram decididos depois de abril de 2016 (quando foi julgado o HC do STJ).

Por outro lado, o precedente do STJ foi fundamentação relevante em 4 dos 5 casos que acolheram a nulidade. No único caso em que essa decisão não foi citada[24], a fundamentação baseou-se em linha argumentativa similar à do HC 51.531/RO e mencionou acórdão do STJ de 2017 que veicula posicionamento semelhante. Relevante notar também que, dentre estes 5 casos, dois[25] recuperam e afastam o precedente do STF no HC 91.867/PA, adotando-se argumentação semelhante àquela empregada pelo Ministro Rogério Schietti no HC 51.531/RO.

É ainda relevante notar que apenas 2 decisões citam o Marco Civil da Internet. Ao afastar o HC 51.531/RO, que também estaria lastreado na referida lei, um acórdão afirma que ela se aplica ao "ambiente virtual", "quando os indivíduos estão conectados", não sendo este o caso no acesso direto a dispositivos celulares[26]. Em outro acórdão, a lei é citada, ao contrário, para sustentar que comunicações contidas em celulares são protegidas, sendo necessária ordem judicial para acessá-las.[27] A mesma decisão cita ainda o HC 75.055 do STJ, que também lidou com a legitimidade do acesso de autoridade policial a dados armazenados em celular de agente detido.[28]

Nos 5 acórdãos nos quais não se analisou a licitude ou ilicitude da prova, as razões de decidir foram de natureza processual. Em 3 deles o Habeas Corpus foi considerado via inadequada para a discussão de questões probatórias. Não obstante, esse argumento também apareceu em um HC[29] no qual, após pugnar pela inadequação da via, o relator analisou a questão e considerou a prova como lícita. Em outros dois casos, a questão foi considerada prejudicada diante da superveniência de sentença condenatória durante o trâmite do HC[30]ou em decorrência da resolução de mérito ser mais benéfica aos réus[31].

21. Acórdãos: TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Apelação nº 0019072-94.2015.8.26.0309. Rel. Jaime Ferreira Menino. Julg. 5.04.2017; TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Apelação nº 0020054-28.2015.8.26.0562. Rel. Francisco Orlando, julg. 06.03.2017; TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Apelação nº 0003821-39.215.8.26.0114. Rel. Euvaldo Chaib, j. 01.08.2017.

22. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Apelação nº 0004154-11.2015.8.26.0269. Rel. Figueiredo Gonçalves, 1ª Câmara de Direito Criminal, j. 20.03.2017.

23. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO. Apelação nº 0005625-73.2015.8.19.0052. Rel. Marcus Basilio, 1ª Câmara Criminal, j. 06.12.2016.

24. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL. Habeas Corpus nº 0191856-53.2017.8.21.7000. Rel. Jayme Weingartner Neto, 1ª Câmara Criminal, j. 09.08.2017.

25. Acórdãos: TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO NORTE. Apelação nº 0101239-21.2014.8.20.0003. Rel. Luiz Alberto Dantas Filho, Câmara Criminal, j. 06.09.2016; TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Apelação nº 0015517-67.2015.8.16.0044. Rel. Rogério Coelho, 5ª Câmara Criminal, j. 14.09.2017.

26. Acórdão: TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Apelação n. 0019072-94.2015.8.26.0309. Rel. Jaime Ferreira Menino. J. 5.04.2017.

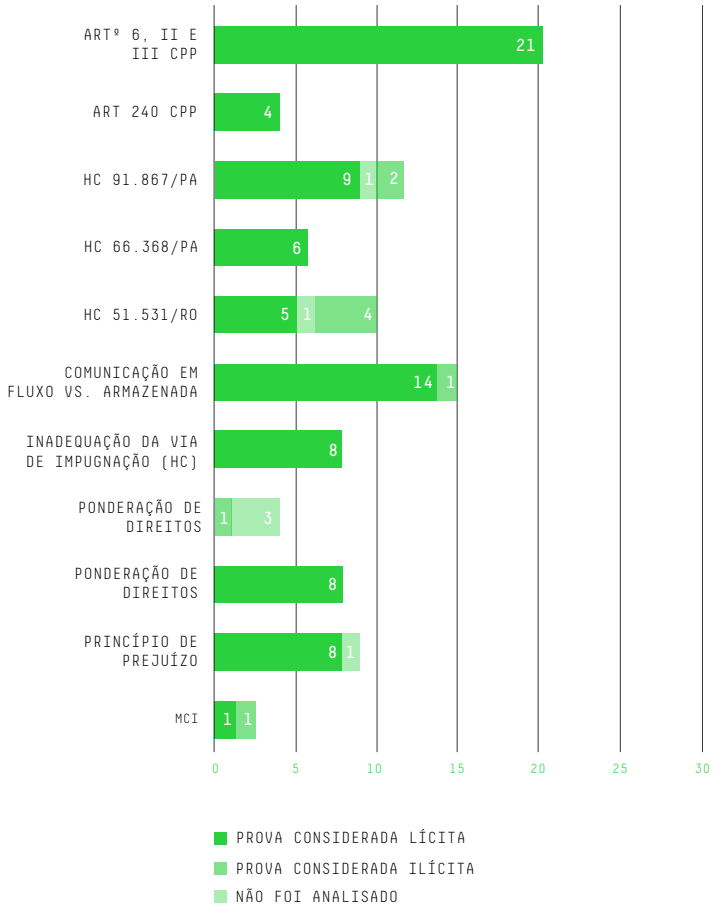
27. Acórdão: TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. Habeas Corpus n. 0191856-53.2017.8.21.7000. Des. Rel. Jayme Weingartner Neto. Julg. 09.08.2017.

28. STJ. Recurso em Habeas Corpus nº 75.055/DF, Brasília, DF, 21.03.2017. Disponível em: https://bit.ly/2XiOpoB. Acesso em: 26.02.2018.

29. Acórdão: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ. Habeas Corpus nº 0021238-64.2017.8.16.0000, Rel. Antônio Carlos Ribeiro Martins, j. 10.08.2017

30. Acórdão: TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Habeas Corpus nº 2116554-91.2017.8.26.0000. Rel. Gilberto Ferreira da Cruz, 15ª Câmara de Direito Criminal, julg. 10.08.2017.

31. Recurso em Sentido Estrito contra decisão de pronúncia, cuja decisão do tribunal foi pela desclassificação do latrocínio, retirando a competência do júri e reenviando o caso para outro órgão analisar as provas: TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL. Recurso em Sentido Estrito nº 0115557-35.2017.8.21.7000. Rel. Sérgio Miguel Achutti Blattes, 3ª Câmara Criminal, j 19.07.2017.



03. CONSIDERAÇÕES FINAIS

Observando os julgados de tribunais estaduais que discutem a licitude do acesso a dados armazenados em celulares por autoridades policiais, constata-se a persistente relevância da distinção antiga entre comunicações em fluxo e comunicações armazenadas no que diz respeito à interpretação do art. 5, XII, da Constituição Federal e uma interpretação do art. 6 do CPP, que autoriza, além do acesso ao objeto, o acesso aos dados nele armazenados. Ambas as linhas argumentativas dialogam mal com as profundas mudanças tecnológicas vividas nas últimas décadas. Aplicativos de mensagens obscurecem o limite final de uma conversa, celulares armazenam hoje informações massivas sobre a vida do usuário e dos indivíduos com quem mantém contato, as buscas virtuais empreendidas num tal contexto, prévio à própria formulação da imputação, não conhecem limite.

Além disso, o HC 51.531/RO do STJ, decidido em abril de 2016, teve influência limitada em cortes inferiores e a "presunção de consentimento" para acesso a celular é esboçada em muitas decisões. Diante de tais elementos, a pesquisa reforça a necessidade de produção doutrinária que discuta a regulamentação das prerrogativas policiais associadas ao flagrante, escopo e justificação da busca pessoal e o sigilo de comunicações, sob pena de perpetuar-se uma situação em que os dados de um indivíduo estarão tão vulneráveis quanto exposto for seu titular a abordagens policiais e ao controle penal, em geral.

06.

PRIVACIDADE E CIDADANIA: OS LIMITES JURÍDICOS DA ATIVIDADE INVESTIGATIVA E A LEGALIDADE DO ACESSO POLICIAL A APARELHOS CELULARES

Gisela Aguiar Wanderley

01. INTRODUÇÃO

No crepúsculo do século XX, a Suprema Corte dos Estados Unidos da América (EUA) fixou a orientação de que um preceito legal não pode ser tão vago a ponto de uma pessoa de inteligência ordinária não ser capaz de determinar previamente qual conduta é lícita e qual conduta é ilícita com base no aludido preceito (*City of Chicago v. Morales*, 527 U.S. 41, 1999). O caso concreto que ensejou a prolação da decisão tinha por referência um decreto proibitivo de vadiagem da cidade de Chicago, o qual proibia os cidadãos de permanecerem em grupo em um espaço público sem um propósito aparente. O objetivo era o de viabilizar a dispersão de gangues na cidade. Assim, caso um policial verificasse um grupo de pessoas ocupando um espaço sem propósito aparente e acreditasse razoavelmente tratar-se de membros de uma gangue, poderia dar uma ordem de dispersão, cuja inobservância configuraria uma violação à lei. O entendimento majoritário da Suprema Corte foi o de que a definição de vadiagem (*loitering*) constante do decreto (permanecer em um espaço sem propósito aparente) não forneceria ao cidadão uma diretriz adequada sobre o que é proibido e o que é permitido e, por isso, tal ato normativo violaria a cláusula do devido processo legal (Décima Quarta Emenda à Constituição dos EUA).

Tal julgado se conecta intimamente a alguns caracteres tidos por essenciais ao Estado de Direito (*Rule of Law*). Mesmo em suas definições mais estreitas (*thin*), compreende-se que o Estado de Direito se ampara no princípio geral de subordinação do poder estatal à lei prévia (governo *sub leges*) estruturada por normas gerais e abstratas (governo *per leges*)[1]. Tal limitação das ações do Estado a leis públicas e prévias tem por efeito tornar possível ao indivíduo prever como as autoridades utilizarão o seu poder e, a partir dessa previsibilidade, orientar e planejar as suas próprias condutas. Assim, a previsibilidade quanto à licitude/ilicitude das condutas confere segurança jurídica ao cidadão para que este oriente os seus comportamentos futuros de acordo com a lei[2] e, inclusive, exerça a prerrogativa cidadã de controlar a licitude dos comandos estatais dirigidos contra si ou contra outrem. Foi essa previsibilidade dos comandos estatais, ínsita ao Estado de Direito e à noção de cidadania, que a Suprema Corte visou a proteger no caso Morales (1999), acima sintetizado.

1. Cf. Bobbio (1986, p. 156–157).

2. Cf. Hayek (1978; 2005).

Vinte anos depois, a questão da previsibilidade dos comandos estatais e da correlata segurança jurídica aos cidadãos ressurge no debate jurídico atinente aos comandos estatais dirigidos aos cidadãos no espaço público urbano. Mas, desta vez, a controvérsia se acopla a novos desafios.

Com efeito, na última década, diversas cortes de diversos países têm se deparado com uma mesma questão jurídica controvertida, atinente a uma realidade fática comum e globalizada: a (i)legalidade de ordens policiais dadas no espaço público urbano a cidadãos para que lhes apresentem os dados constantes de seus aparelhos celulares – especialmente se estiverem sendo considerados suspeitos da prática de um crime.

O contexto da controvérsia é peculiar ao limiar do século XXI, em que a rápida evolução tecnológica propiciou a produção e a comercialização em massa de celulares com alta capacidade de armazenagem e fluxo de dados (*smartphones*) que são portados continuamente pelos cidadãos em praticamente todos os seus deslocamentos diários. Nesse cenário, de forma inevitável, os celulares se tornaram um alvo inequívoco da investigação policial, pois consubstanciam rico repositório de fontes reais de provas de infrações penais. Contudo, a atividade legiferante não acompanhou a rapidez do desenvolvimento tecnológico. Assim, sem preceitos legais específicos, juízes

e tribunais têm enfrentado a necessidade de definir critérios de legalidade para tais meios de obtenção de prova.

Diante de tal contexto e especialmente diante dos últimos julgados sobre o tema pelo Superior Tribunal de Justiça (STJ), este artigo visa a delimitar alguns critérios que possam nortear o debate quanto a legalidade de tais meios de obtenção de prova, a partir da premissa de que a fixação precisa de tais critérios é indispensável à proteção à privacidade pessoal e ao próprio exercício da cidadania nas relações entre indivíduos e policiais no espaço público urbano. Somente pelo prévio conhecimento dos fundamentos e limites da legalidade das ações policiais é que estas poderão ser controladas pelos próprios cidadãos.

02. A JURISPRUDÊNCIA RECENTE DO STJ SOBRE ACESSO A CELULARES PELA POLÍCIA (2016-2018): BUSCA E APREENSÃO, ACESSO A DADOS DE SMARTPHONE E ESPELHAMENTO VIA WHATSAPP WEB

Em maio de 2016, a Sexta Turma do STJ prolatou acórdão paradigmático quanto ao acesso a dados constantes de aparelhos celulares pela polícia ao fixar a tese de que é ilícita "a devassa de dados, bem como das conversas de *WhatsApp*, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial" (RHC 51.531/RO, Rel. Min. Nefi Cordeiro, DJe 09.05.16). O caso concreto tinha por substrato fático a prisão em flagrante de um indivíduo pelos crimes de tráfico e associação para o tráfico de drogas, surpreendido a portar trezentos comprimidos de *ecstasy*. No decorrer da prisão o celular do preso foi apreendido e os dados foram, ato contínuo, acessados e periciados. A perícia foi justificada pela autoridade policial com base no art. 6º, II, III e VII, do Código de Processo Penal (CPP) e a licitude foi chancelada pelas instâncias judiciais ordinárias com base na presunção de legalidade dos atos administrativos e no art. 159 do CPP.

A Sexta Turma do STJ, por unanimidade, concedeu a ordem de *habeas corpus* para declarar a nulidade das provas obtidas pelo acesso ao celular, por entender ser necessária a autorização judicial. O voto condutor do acórdão (proferido pelo relator Min. Nefi Cordeiro) tem por fundamentos principais a Lei n. 9.472/97 (Lei Geral de Telecomunicações - LGT) e a Lei n. 12.965/14 (Marco Civil da Internet - MCI), que positivam, respectivamente, o direito do usuário de telecomunicações à inviolabilidade e segredo de sua comunicação salvo nas exceções constitucionais (LGT, art. 3º, V) e o direito do usuário de *internet* à inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial (MCI, art. 7º, III). Ressalta-se ainda no voto que para acesso a conversas armazenadas em correio eletrônico (e-mail) há jurisprudência consolidada quanto à necessidade de ordem judicial prévia para quebra do sigilo, orientação que deve ser estendida ao acesso a conversas armazenadas em celular.

Os votos-vista proferidos no caso, por sua vez, amparam-se no direito comparado para dar suporte à conclusão quanto à necessidade de autorização judicial. No voto proferido pelo Min. Rogerio Schietti, registra-se que a controvérsia se insere no âmbito do assim chamado "direito probatório de terceira geração", em que é necessário aferir a licitude de provas altamente invasivas propiciadas pelo avanço tecnológico, que permite alcançar conhecimentos e resultados inatingíveis pelos meios de obtenção de prova convencionais. Tais provas incluiriam: "a) as buscas superintrusivas, b) as observações virtuais e c) a organização de grandes volumes

de informações, sendo obviamente as primeiras colocadas no topo da mitigação de direitos fundamentais".[3]

Assim, em relação a tal problemática, assenta-se a relevância do precedente *Riley v. California* (573 U.S. ___, 2014), no qual a Suprema Corte dos EUA assentou ser indispensável mandado judicial para acesso a dados de celular, mesmo em caso de prisão, ante o elevado número de dados privados insertos em *smartphone*, em regra invioláveis com base na proteção à privacidade constante da Quarta Emenda à Constituição estadunidense.

Dessa forma, o Min. Schietti registra a necessidade de se superar o entendimento firmado pelo STF em 2012 no HC 91.867/PA (Segunda Turma, Rel. Min. Gilmar Mendes, DJe 20.09.12) – no sentido da desnecessidade de mandado judicial prévio para acesso aos dados de celular – em razão do avanço tecnológico.

Com efeito, o caso enfrentado pelo STF no HC 91.867/PA havia ocorrido em 2004, época em que ainda não existiam *smartphones*, de modo que o acesso aos dados de celular se limitou ao registro das ligações telefônicas e à agenda de contatos do celular. Ante tal substrato fático, a Corte Suprema observou que o acesso a tais dados do celular não se equipara à interceptação telefônica (que propicia acesso ao *conteúdo* das conversas em fluxo, em tempo real), ao passo que não se diferencia substancialmente do exame de objetos apreendidos com o suspeito (por exemplo, em pouco se distinguiria da leitura de uma agenda física de contatos telefônicos ou papéis e documentos com números de telefone anotados, todos passíveis de apreensão). Assim, o STF assenta a desnecessidade de autorização judicial prévia para o acesso a dados de celular.

3. Sobre o tema, ver KNIJNIK, Danilo. *A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI.* Revista da Escola da Magistratura do TRF da 4ª Região, vol. 1, n. 4, 2014, p. 77-96.

O contexto fático do caso enfrentado pelo STF, contudo, é radicalmente alterado com o advento e a difusão dos *smartphones*, que armazenam dados e conversas com muito mais informações privadas do que qualquer coisa material portada pelo suspeito. Daí o reconhecimento da necessidade de se superar o precedente do STF e se firmar a necessidade de autorização judicial para o acesso ao celular, em razão do elevado grau de invasividade da medida, não equiparável a uma simples apreensão de objetos.

Por fim, o voto-vista da Min. Maria Thereza de Assis Moura se assenta no confronto entre a "cláusula geral de resguardo da intimidade" constante do art. 5º, X, da Constituição da República de 1988 (CR/88) e o "direito à segurança pública" previsto no art. 144 da mesma Constituição.

Para enfrentar tal colisão, observa-se no voto que a Suprema Corte do Canadá (*R. v. Fearon*, 2014 SCC 77, [2014] S.C.R. 621) entendeu pela licitude do acesso aos dados de celular de indivíduo preso em flagrante, desde que preenchidos quatro requisitos cumulativos: (1) licitude da prisão; (2) incidentalidade do acesso aos dados em relação à prisão, demonstrada pela instrumentalidade do ato em relação à proteção dos policiais, do suspeito ou de terceiros, à preservação de provas ou à descoberta de provas que possa ser significativamente prejudicada; (3) restrição da natureza e extensão da medida a tais propósitos instrumentais; (4) registro detalhado dos dados examinados e da forma como se deu tal exame (propósito, extensão, tempo de acesso).

De outro lado, pondera-se que o Pleno do Tribunal Constitucional da Espanha (*Sentencia 115/2013*, de 9 de maio de 2013 – BOE núm. 133, de 4 de junho de 2013) decidiu caso similar em que entendeu que uma invasão substancial à privacidade (mais extensa do que mero exame da agenda de contatos do celular) demandaria parâmetro "especialmente rigoroso"

para verificação da proporcionalidade da medida. Assim, em relação ao caso concreto, a Min. Maria Thereza assenta a ilegalidade do acesso ao celular em razão da ausência de qualquer elemento que pudesse justificar a *urgência* para o acesso imediato aos dados sem prévio mandado judicial.

Após esse paradigmático julgado, o entendimento foi reiterado por ambas as Turmas que compõem a Terceira Seção (Quinta e Sexta Turmas)[4] e outros casos similares foram enfrentados pela mesma Corte Superior de Justiça.

4. Cf. HC 418.180/RN (Sexta Turma, Rel. Min. Rogerio Schietti Cruz, DJe 21.11.18) e RHC 67.379/RN (Quinta Turma, Rel. Min. Ribeiro Dantas, DJe 09.11.16)

No RHC 75.800/PR, referente à assim denominada Operação Lava Jato, a Quinta Turma do STJ reconheceu ser suficiente para o acesso aos dados insertos no celular a expedição de mandado judicial de busca e apreensão do próprio aparelho, "sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal" (Quinta Turma, Rel. Min. Felix Fischer, DJe 26.09.2016). Já no HC 433.930/ES e no AgRg no AREsp 1249886/ES (Quinta Turma, Rel. Min. Reynaldo Soares da Fonseca, DJe 29.06.18 e DJe 01.06.18, respectivamente), o STJ reiterou essa importante distinção restritiva (*restrictive distinguishing*), ao firmar que, se houver expedição de mandado judicial e busca e apreensão, é lícito o acesso aos dados inseridos no celular.

Para tanto, o STJ reafirmou a tese de que a proteção à comunicação de dados estatuída pelo art. 5º, XII, da CR/88 (regulamentado pela Lei n. 9.296/96, que trata da interceptação telefônica e telemática) não se confunde com a proteção aos dados em si[5], que se submetem então a regime jurídico diverso – daí a desnecessidade de ordem judicial autônoma para acesso aos dados de

5. Sobre o tema, cf. FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, p. 439–459, 1993.

celular ou computador já apreendido por ordem judicial (cf. RE 418.416/SC, Rel. Min. Sepúlveda Pertence, DJ 19.12.06).

Noutro giro, também em distinção restritiva, no RHC 86.076/MT (Rel. Acd. Min. Rogerio Schietti Cruz, DJe 12.12.17) firmou-se a tese de que "[n]ão há ilegalidade na perícia de aparelho de telefonia celular pela polícia, sem prévia autorização judicial, na hipótese em que seu proprietário – a vítima – foi morto, tendo o referido telefone sido entregue à autoridade policial por sua esposa". Neste caso, o Tribunal observou que diante da morte da vítima do crime (de homicídio) e do consentimento da sua esposa, não havia privacidade ou sigilo a obstar o acesso aos dados constantes do seu celular, para esclarecer o próprio delito.

Por fim, em 2018, o STJ firmou a orientação de ser nula a obtenção de prova por espelhamento do WhatsApp via Código QR para acesso paralelo às conversas travadas pelo celular do suspeito em computador da polícia (WhatsApp Web) pela autoridade policial, mesmo que amparada em mandado judicial prévio e específico (RHC 99.735/SC, Sexta Turma, Rel. Min. Laurita Vaz, DJe 12.12.18). No interessante caso concreto, a autoridade policial requereu autorização judicial para apreensão, espelhamento e monitoramento das conversas travadas no WhatsApp pelo suspeito de liderar uma organização criminosa. Após obter o mandado, a polícia promoveu a condução coercitiva do suspeito à delegacia, apreendeu seu celular por poucos minutos, efetuou o espelhamento em computador da delegacia e devolveu o aparelho ao suspeito.

A conclusão pela nulidade da prova foi assentada na impossibilidade de equiparação do espelhamento de WhatsApp à interceptação telefônica (tese suscitada pelo Ministério Público no caso), em razão de três principais diferenças.

Em primeiro lugar, observou-se que na interceptação a polícia só pode efetuar o monitoramento (observação passiva) de conversas, ao passo que no espelhamento há possibilidade

de inserção ou exclusão de mensagens (manipulação ativa) pela polícia, sem que haja possibilidade de controle dessa atuação em razão da criptografia ponta-a-ponta (*end to end*) que caracteriza o aplicativo. Observa-se no voto condutor que essa impossibilidade de controle da atuação policial acaba por gerar uma presunção *absoluta* (e não meramente relativa) de legitimidade dos atos policiais, pois é impossível à defesa a produção de prova em contrário, com demonstração de eventual atuação ilegítima do aparato policial.

Em segundo lugar, assenta-se que na interceptação há acesso delimitado a conversas posteriores à decretação da medida (*ex nunc*), por prazo determinado (quinze dias, prorrogáveis por decisão judicial fundamentada), ao passo que no espelhamento o acesso é amplo e irrestrito a toda e qualquer conversa anterior à decretação da medida (*ex tunc*).

Por fim, em terceiro lugar, ressalta-se que na interceptação é desnecessária diligência simultânea ou prévia de busca pessoal ou domiciliar e subsequente apreensão do aparelho, medidas que, no entanto, se revelam indispensáveis à efetivação do espelhamento.

Assim, diante de tais diferenças, o STJ fixou o entendimento de ser o espelhamento uma prova atípica e híbrida, que demanda regulamentação legal para possibilitar limitação e controle da atuação policial e impedir eventual abuso do poder de investigação.

03. RACIONALIZAÇÃO JURÍDICA DOS MEIOS DE OBTENÇÃO DE PROVA NO ESTADO DE DIREITO: CAMINHOS POSSÍVEIS

A tradição jurídica brasileira, vinculada ao sistema de *civil law*, tem por característica a regulamentação dos meios de obtenção de prova por meio de normativos específicos, que tipificam um meio de obtenção de prova e, sucessivamente, contornam-lhe as hipóteses de cabimento, os requisitos de validade e os procedimentos e limites de execução. Assim, como exemplos, pode-se mencionar a busca e a apreensão, regidas pelos arts. 240 a 250 do CPP, a interceptação telefônica e telemática, regida pela Lei n. 9.296/96 (ante o comando expresso do art. 5º, XII, da CR/88), o acesso a registros, dados cadastrais, documentos e informações, regido pela Lei n. 9.613/98 quanto à lavagem de ativos, pela Lei n. 12.850/13 quanto às organizações criminosas e pelo art. 13-A do CPP (incluído pela Lei n. 13.344/16) quanto ao tráfico de pessoas, o acesso a sinais e informações de estações rádio base, regido pelo art. 13-B do CPP, também quanto ao tráfico de pessoas (incluído pela Lei n. 13.344/16), a colaboração premiada, a ação controlada, a infiltração de agentes, todas regidas pela Lei n. 12.850/13 quanto às organizações criminosas, entre outros. Esse modelo contrasta com o modelo estadunidense, que estabelece limites para os meios de obtenção de prova especialmente a partir da cláusula geral constante da Quarta Emenda à Constituição, que protege a privacidade individual.

Contudo, a evolução tecnológica impede a normatização precisa de todo e qualquer meio de obtenção de prova. Quebras de sigilo e acesso a dados armazenados em computador, em correio eletrônico ou aparelhos celulares são exemplos de meios de obtenção de prova cuja regulamentação não foi exaurida por meio de lei, mas que ostentam extrema relevância para a investigação penal. Em tal contexto, não é adequado inviabilizar a atividade de persecução penal ao simplesmente cominar de nulo qualquer meio de obtenção de prova ainda não regulamentado em lei específica. Ao revés, é preciso examinar, diante das novas tecnologias existentes, quais critérios, procedimentos e limites devem ser impostos de forma a compatibilizá-las às diretrizes do Estado de Direito. As-

sim, na ausência de lei específica, o desafio de estabelecer tais requisitos de validade recai sobre o Poder Judiciário e sobre os demais atores do processo penal, inclusive e sobretudo na fase de investigação preliminar.

Nesse cenário, é importante reconhecer que a regulamentação legal específica de cada meio de obtenção de prova tem um efeito positivo: a segurança jurídica quanto aos contornos precisos de cada um, definidos de acordo com as suas peculiaridades. Por outro lado, há um efeito colateral negativo propiciado por tal modelo: o esquecimento das razões comuns que justificam e fundamentam a regulamentação de todos os meios de obtenção de prova.

Com efeito, a delimitação das hipóteses de cabimento, dos requisitos de validade, dos procedimentos e limites de cada meio de obtenção de prova não se reduz a mero formalismo ou burocracia autojustificada – ou, ao menos, não deveria se reduzir. A razão de ser de toda regulamentação de todo e qualquer meio de obtenção de prova deve remontar, repise-se, ao Estado de Direito e à correlata noção do devido processo legal[6]: os requisitos e procedimentos legais devem ser compreendidos como condições de validade que evitam a privação arbitrária dos direitos dos cidadãos pela atuação do Estado-penal e que assim conferem instrumentalidade constitucional ao processo, compreendido como meio de garantia dos direitos e liberdades fundamentais.

6. Sobre a evolução da garantia do devido processo legal, especialmente no direito estadunidense, ver ISRAEL et al., 2012.

A compreensão das razões subjacentes aos procedimentos e garantias processuais penais se opõe, por conseguinte, a leituras legalistas e formalistas dos requisitos e procedimentos legais, sem plena compreensão da função e da finalidade por eles cumpridas. Assim, diante do surgimento de novos meios de obtenção de prova ainda desprovidos de regulamentação

/ SOMENTE PELO PRÉVIO CONHECIMENTO DOS FUNDAMENTOS DAS AÇÕES POLICIAIS É QUE ELAS PODERÃO SER CONTROLADAS PELOS PRÓPRIOS CIDADÃOS /

legal específica, a identificação de procedimentos e limites mínimos para a validade de tais meios deve ter por substrato exatamente a *razões* que ensejam a regulamentação dos meios de obtenção de prova no bojo do devido processo legal.

Uma vez firmadas tais premissas, é possível constatar que o estabelecimento prévio de procedimentos e limites para o uso de meios tecnológicos de obtenção de prova tem, no mínimo, uma razão material e uma razão processual. Com efeito, a limitação do poderio estatal de investigação é indispensável não só à proteção à privacidade individual, mas também à viabilização do controle da legitimidade da atuação das agências de investigação penal. Assim, a fixação de limites à atuação probatória pelo aparato policial decorre não apenas de uma razão *material*, qual seja, o direito à privacidade – do qual deriva a proteção jurídica à *legítima expectativa* de não intervenção estatal na esfera privada (cf. *Katz v. United States*, 389 U.S. 347, 1967) –, mas também de uma razão *processual*, a saber, a necessidade de se estabelecer mecanismos procedimentais de fiscalização e controle da idoneidade dos atos praticados na investigação penal, de modo a evitar quebras na cadeia probatória, manipulação de fontes de prova, entre outros vícios que comprometam o direito à prova e ao contraditório. São razões intimamente conectadas ao *devido processo legal*, compreendido em suas dimensões substancial e procedimental.

Os precedentes recentes do STJ acima sumariados transitam entre essas duas preocupações, de ordem material e processual, e colaboram para atribuir um mínimo de racionalidade à atividade de validação jurídica dos meios de obtenção de provas utilizados na atividade de persecução penal, ainda que se trate de meios inovadores e tecnológicos ainda não regulamentados por lei específica. Vale dizer, em tais julgados, o STJ ultrapassa uma leitura meramente formalista dos procedimentos legais ao identificar as razões pelas quais devem ser impostos ao uso de meios atípicos de obtenção de prova.

Assim, no RHC 51.531/RO, nota-se que a exigência de autorização judicial prévia impede o uso generalizado do acesso aos dados constantes de aparelho celular e assim consagra importante proteção ao direito à privacidade, notadamente ao garantir a inviolabilidade aos dados e conversas de caráter privado que, em regra, o indivíduo espera manter a salvo de terceiros. De outro lado, no RHC 99.735/SC, observa-se que a vedação ao uso do espelhamento de conversas via WhatsApp Web, ainda que autorizada judicialmente, obsta o uso de um meio de obtenção de prova desprovido de mecanismos de fiscalização e controle de sua própria licitude, de modo a obstaculizar o uso abusivo dos poderes de investigação sem possibilidade de rechaço a tal abuso.

Tal esforço de racionalização da atividade probatória, contudo, ainda não se mostra consolidado e arraigado na jurisprudência brasileira. A rigor, a construção do discurso jurídico relativo à validade de tais meios tecnológicos de obtenção de prova não raro passa ao largo das razões materiais e processuais que fundam a necessidade de imposição de procedimentos e limites mínimos que assegurem a idoneidade e a legitimidade da atividade investigatória em um Estado de Direito.

Nesse sentido, na pesquisa conduzida por Antonialli *et al* (2019), foram analisadas as razões de decidir de 49 (quarenta e nove) acórdãos de tribunais de justiça estaduais a respeito da legalidade do acesso policial a dados armazenados em celular. Em 37 (trinta e sete) deles, o acesso havia ocorrido após prisão em flagrante delito (mesma situação fática subjacente ao RHC 51.531/RO). E, em 27 de tais 37 casos (73%), os tribunais entenderam pela licitude do acesso, a despeito da falta de mandado judicial prévio. Nos outros 12 (doze) acórdãos, o acesso aos dados ocorreu no bojo de uma abordagem policial, ainda sem

elementos para prisão em flagrante delito. Em 6 de tais 12 casos (50%), os tribunais entenderam pela licitude do acesso.

O que chama a atenção, contudo, não é apenas o percentual expressivo de casos em que a orientação firmada contrasta com aquela firmada pelo STJ, mas sim alguns dos fundamentos reiteradamente utilizados para subsidiar tal orientação.

Nos casos de acessos ao celular de presos em flagrante delito, em 23 casos a licitude da prova foi amparada na aplicação de dispositivos legais do Código de Processo Penal atinentes à busca pessoal e à apreensão (CPP, arts. 6º, II e III, 240, § 2º, 244). Assim, o acesso a dados armazenados em celular ser considerado uma mera apreensão ou, ainda, uma mera *extensão* de uma busca pessoal.

A esse respeito, vale notar que o CPP, no artigo 240 e seguintes, regulamenta duas espécies de busca: a busca domiciliar e a busca pessoal. A busca domiciliar é aquela realizada na casa, objeto de proteção constitucional como asilo inviolável do indivíduo (CR/88, art. 5º, XI). A busca pessoal, por sua vez, é definida de modo residual como a revista realizada "na própria pessoa ou na esfera de custódia de que o acompanha" (MISSAGGIA, 2002, p. 202), o que abrange o corpo, as roupas e os pertences do indivíduo, aí incluído eventual veículo automotor (que não se destine à habitação).

Em relação à busca pessoal, há corrente doutrinária que admite o uso de meios radioscópicos ou mecânicos para inspeção de cavidades do corpo humano (cf. NUCCI, 2012, p. 558; LIMA, M., 2014a, p. 112). Contudo, em oposição, André Luiz Nicollitt e Carlos Ribeiro Wehrs (2015) salientam que neste caso ocorre verdadeira "intervenção corporal", ato de caráter mais invasivo que uma busca pessoal, em razão de penetrar "ainda que minimamente, no corpo humano vivo" ou ser potencialmente capaz "de produzir uma influência sobre ele, influência esta em sua funcionalidade". Assim, a intervenção corporal não se confunde com a mera revista feita na parte exterior do corpo e, portanto, não se submete ao mesmo "regime da busca pessoal" (NICOLITT; WEHRS, 2015, p. 51-53). Por esse viés, constata-se que o exame radioscópico (que permite visualizar o interior do corpo) e a inspeção das cavidades do corpo ("revista íntima", por meio manual ou mecânico) são intervenção corporais e não meras buscas pessoais.

Essa reflexão quanto à distinção entre busca pessoal e intervenção corporal com base no grau de invasividade da medida pode ser aproveitada, portanto, para o debate atinente ao acesso a dados armazenados em celulares.

A aplicação direta dos arts. 6º, II e III, 240, § 2º, e 244 do CPP ao acesso a dados constantes de celular implica uma equiparação entre coisas materiais (passíveis de "busca e apreensão") e entre dados (passíveis de "acesso"). Assim, trata-se o acesso a dados de celulares como consectários de uma busca e apreensão como qualquer outra. Tal orientação, contudo, tem por efeito deletério a flexibilização da privacidade individual. Isso porque a apreensão de coisas materiais encontradas no local de um crime (CPP, art. 6º) ou de objetos que o agente traga consigo após uma busca pessoal (CPP, art. 244) tem um grau de invasividade sensivelmente inferior ao acesso a dados em *smartphones* com alta capacidade de armazenagem, conforme abordado pelo STJ no RHC 51.531/RO. A elevada quantidade de dados e conversas e a elevada expectativa de privacidade sobre eles demanda controle mais rígido de tal meio de obtenção de prova, não equiparável à mera busca e apreensão.

Nesse sentido, é interessante ponderar que, em relação à perspectiva material (afetação ao direito à privacidade), o acesso a dados armazenados em celular mais se assemelha a uma interceptação telefônica do que a uma busca e apreensão, por ter elevado grau de invasividade. Daí a necessidade

de se exigir os requisitos correspondentes: a reserva de jurisdição (mandado judicial prévio) e a subsidiariedade em relação a outros meios de obtenção de prova menos invasivos, ambos consagrados na Lei n. 9.296/96.

A exigência de tais requisitos da interceptação telefônica para o acesso a dados armazenados em celular não parte da premissa de serem ambos institutos equivalentes. De fato, a interceptação da comunicação (fluxo de dados) não se confunde com o acesso aos dados em si, e a interceptação tem um caráter temporalmente delimitado e prospectivo (*ex nunc*), caracteres nos quais se distingue do acesso aos dados armazenados em celular (temporalmente ilimitada e retrospectiva). O que se reconhece é, apenas, a existência de um caractere comum a ambas – o elevado grau de invasividade das duas medidas, superior ao de uma busca pessoal -, o qual consiste exatamente na razão material que ampara a exigência legal de tais requisitos à interceptação telefônica (a proteção à privacidade pessoal) e que assim justifica a extensão da sua aplicabilidade também ao acesso a dados armazenados em celular.

De outro lado, ainda na pesquisa de Antonialli *et al.* (2019), identifica-se que em 8 (oito) casos de acesso a celular de presos em flagrante, a licitude de tal meio de obtenção de prova foi afirmada a partir de um juízo de ponderação de direitos e garantias constitucionais, invocado de forma complementar a outros fundamentos, e suscitado de duas formas: pela afirmação de que os direitos e garantias constitucionais não são absolutos, complementada, ou não, pela ponderação entre o direito ao sigilo das comunicações e o direito à segurança/ordem pública (em que o último prevalece sobre o primeiro).

Tal fundamento, contudo, conduz à neutralização de todo e qualquer critério racional de limitação à atividade de obtenção da prova, uma vez que os objetivos da persecução penal, atrelados aos interesses de toda a sociedade (prevenção/repressão à criminalidade em geral, preservação da segurança pública, manutenção da ordem...), sempre podem ser erigidos de forma genérica como prevalecentes em face dos direitos individuais de suspeitos e acusados.

A esse respeito, Danilo Knijnik (2014) aponta que, desde o fracasso histórico do sistema de provas tarifadas, o direito probatório é por natureza refratário ao discurso jurídico. Assim, o atual sistema da persuasão racional do órgão julgador oscila entre uma corrente maximalista (que encara a valoração probatória como ato subjetivo e perceptivo do julgador, amparada na sua liberdade para a atividade judicante) e uma corrente minimalista (que destaca as limitações lógicas da atividade judicante e impõe critérios racionais e objetivos para a formação da convicção judicial).

Embora a reflexão de Kniknik tenha por objeto a atividade de valoração da prova (já obtida e introduzida no processo), e não de obtenção da prova, dicotomia similar pode ser verificada quanto a esta última atividade (ora em análise). Com efeito, é possível, de um lado, adotar uma posição maximalista quanto à validade de meios de obtenção de prova a partir da presunção de legalidade dos atos administrativos e da possibilidade de ponderação dos direitos individuais perante os objetivos da persecução penal. De outro lado, é possível adotar uma posição minimalista, a partir da imposição de critérios e limites racionais aos meios de obtenção de prova, considerados os direitos individuais de defesa perante o poderio estatal e a necessária controlabilidade dos atos estatais, pilares da noção de devido processo legal.

Uma vez fixada tal dicotomia, é possível entrever que, nos precedentes mais recentes do Superior Tribunal de Justiça, este tem tentado fixar critérios e limites racionais aos novos meios de obtenção de prova proporcionados pelo desenvolvimento tecnológico. Assim, a mera ausência de regulamentação legal não é considerada por si só um óbice ao uso de meios

de obtenção de prova tecnológicos atípicos. Por outro lado, os limites erigidos ao uso de tais meios têm assento constitucional: os direitos individuais de ordem material (notadamente o direito à privacidade) e os procedimentos que conformam o próprio devido processo legal (notadamente considerados em sua relevância para a controlabilidade da atividade probatória estatal, ínsita aos direitos à prova e ao contraditório).

Nesse sentido, vale notar que, nos precedentes de direito comparado utilizados no RHC 51.531/RO, até mesmo as exceções admitidas aos limites construídos também se amparam em critérios racionalmente admissíveis. Assim, no voto-vista prolatado pela Ministra Maria Thereza, marcado pela menção a precedente da Suprema Corte do Canadá (*R. v. Fearon*, 2014 SCC 77, [2014] S.C.R. 621), destaca-se que o mandado judicial prévio pode ser dispensado em situações de *urgência*: nas quais o lapso temporal necessário à obtenção do mandado possa resultar em perigo de dano ou ineficácia da medida. Assim, constrói-se uma exceção delimitada e racionalmente fundamentada, a ser justificada em cada caso concreto a partir de circunstâncias objetivamente verificáveis (o que torna a própria configuração da exceção passível de controle e refutação), o que em muito difere da ponderação abstrata e genérica entre direitos individuais e segurança pública, em uma linha de argumentação em que esta pode, sempre e sempre, prevalecer sobre aqueles, numa formatação muito mais próxima à de um Estado de Polícia do que à de um Estado de Direito.

04. CONCLUSÃO

Diante da evolução tecnológica e do seu impacto sobre os meios de investigação, é indispensável compreender que as condições de validade impostas à atividade probatória, a exemplo da reserva de jurisdição e de mecanismos de fiscalização e controle da atuação policial, não são meros óbices formalistas autojustificados em si mesmos à investigação, mas sim limites mínimos conectados a razões materiais e processuais ínsitas ao próprio Estado de Direito. A vedação à intervenção estatal arbitrária na esfera privada e a necessária controlabilidade dos poderes estatais, pilares da garantia do devido processo legal em suas dimensões substancial e formal. Portanto, os requisitos e procedimentos exigíveis para a validade jurídica da investigação se legitimam na medida em que evitam a generalização de meios invasivos de obtenção de prova (em atenção aos direitos individuais, especialmente à privacidade e à liberdade) e que garantem a controlabilidade do emprego de tais meios (em atenção à vedação ao uso arbitrário do poder estatal e aos direitos à prova e ao contraditório), o que assim legitima o próprio processo como instrumento de garantia dos direitos e liberdades do cidadão em face do Estado.

Contudo, tais funções e finalidades ínsitas ao devido processo legal são comumente olvidadas nas decisões judiciais prolatadas em matéria de direito probatório. Alguns meios de obtenção de prova cuja realização escapa ainda a qualquer exame de racionalidade jurídica. Assim, ainda se tem notícia do uso generalizado e exploratório de meios invasivos de obtenção de prova (a exemplo de buscas domiciliares coletivas em bairros inteiros, ou abordagens policiais e buscas pessoais promovidas sem indícios objetivos de conduta criminosa[7]), ou da flexibilização do uso de tais meios invasivos a partir de fundamentos genéricos que não resultam em exceções pontuais ao procedimento legal, mas sim em verdadeira neutralização aos próprios direitos fundamentais afetados

7. Em outros trabalhos, já apontamos como a busca pessoal, embora seja meio de obtenção de prova restritivo da privacidade e da liberdade ambulatorial individuais, é realizada cotidiana e rotineiramente pelas agências policiais sem respaldo no permissivo legal respectivo (CPP, art. 244), o que tem sido admitido pelas agências judiciais (cf. WANDERLEY, 2017a e 2017b).

(a exemplo da genérica ponderação entre os direitos individuais de suspeitos e acusados em prol da eficiência da persecução penal na consecução de seus objetivos gerais, como a repressão ao crime ou a garantia da segurança pública).

Nesse cenário, os precedentes mais recentes do STJ aqui mencionados constituem um importante avanço em direção à racionalização dos meios de obtenção de prova, a partir de razões materiais e processuais intimamente conectadas ao Estado de Direito – e não a partir de uma leitura legalista e formalista da legislação processual penal. Tais razões, contudo, ainda podem ter sua aplicabilidade expandida para inúmeras outras situações em que o exercício da atividade de investigação carece de critérios e limites racionais indispensáveis à tutela dos direitos individuais e à vedação ao abuso do poder estatal.

05. REFERÊNCIAS

ANTONIALLI, Dennys Marcelo *et al*. Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. *Revista Brasileira de Ciências Criminais*, v. 154, 2019.

BOBBIO, Norberto. *O futuro da democracia: uma defesa das regras do jogo*. São Paulo: Paz e Terra, 1986.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, p. 439–459, 1993.

HAYEK, Friedrich. *The Constitution of Liberty*. Chengcheng: China Social Sciences Publishing House, 1978.

HAYEK, Friedrich. *The road to serfdom*. London: The Institute of Economic Affairs, 2005.

ISRAEL, Jerold H. *et al*. *Proceso penal y Constitución de los Estados Unidos de Norteamérica. Casos destacados Del Tribunal Supremo y texto introductorio*. Valencia: Tirant lo Blanch, 2012.

KNIJNIK, Danilo. *A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do século XXI.* Revista da Escola da Magistratura do TRF da 4ª Região, vol. 1, n. 4, 2014

LIMA, Marcellus Polastri. *A tutela cautelar no processo penal*. 3ª ed. São Paulo: Atlas, 2014.

MISSAGGIA, Clademir. Da busca e da apreensão no processo penal brasileiro. *Revista do Ministério Público (Porto Alegre)*, v. 48, p. 199–246, 2002.

NICOLITT, André Luiz; WEHRS, Carlos Ribeiro. *Intervenções corporais no processo penal e a nova identificação criminal (Lei 12.654/2012)*. São Paulo: Revista dos Tribunais, 2015.

NUCCI, Guilherme de Souza. *Código de Processo Penal comentado*. 11ª ed. São Paulo: Revista dos Tribunais, 2012.

WANDERLEY, Gisela Aguiar. *A busca pessoal no direito brasileiro: medida processual probatória ou medida de polícia preventiva?* Revista Brasileira de Direito Processual Penal, v. 3, n. 3, 2017a.

WANDERLEY, Gisela Aguiar. *Entre a lei processual e a praxe policial: características e consequências da desconcentração e do descontrole da busca pessoal*. Revista Brasileira de Ciências Criminais, v. 128, 2017b.

07.

ACESSO A DISPOSITIVOS ELETRÔNICOS E A DEVIDA INVESTIGAÇÃO LEGAL

Rafael F. Marcondes de Moraes

01. INTRODUÇÃO

No presente ensaio, pretende-se elaborar um breve estudo sobre o acesso a dispositivos eletrônicos, em especial a aparelhos de telefonia móvel celular, diante do atual panorama doutrinário e jurisprudencial assim como a sua correlata repercussão no âmbito da atividade de polícia judiciária.

A abordagem da temática será desenvolvida à luz das disposições contidas na Lei Federal 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, bem como das interpretações dela decorrentes e das demais previsões legais pertinentes.

02. DIRETRIZES E FUNDAMENTOS CONSTITUCIONAIS

O acesso aos dados e documentos contidos em dispositivos eletrônicos, tais como telefones celulares multifuncionais (*smartphones*), computadores portáteis (*notebooks*, *tablets* etc.) e outros aparelhos similares envolve debates sobre a intensidade de afetação e de proteção de tais medidas na privacidade de cada cidadão, direito individual constitucionalmente consagrado no inciso X, do artigo 5º, da Carta Magna de 1988, que prevê a inviolabilidade da intimidade, da vida privada, da honra e a da imagem das pessoas.

Não se olvida que, se por um lado a Constituição Federal tutela a privacidade, por outro indica vetores para que essa proteção seja sopesada, sobretudo o direito individual e coletivo à segurança, consagrado no *caput* do artigo 5º da Lei Maior, que também eleva a segurança como direito social em seu artigo 6º e veicula ainda a segurança pública como dever do Estado e direito e responsabilidade de todos em seu artigo 144, disposições com inegável ressonância na exegese e na aplicação da legislação processual penal.

03. DEVIDA INVESTIGAÇÃO LEGAL, SIGILO E RESERVA DE JURISDIÇÃO

De um modo geral, a discussão ora enfrentada abrange a compreensão sobre o sigilo, vale dizer, acerca do grau de restrição à publicidade das informações armazenadas em equipamentos eletrônicos, acompanhado do paralelo grau de proteção a ser conferido que, em síntese, implicam considerar ou não a matéria sob o manto da absoluta reserva jurisdicional.

Nessa senda, destaca-se a relevância da incidência das garantias processuais penais integrantes do "princípio-síntese" do devido processo legal[1] já no plano do inquérito policial, derivação intitulada "devida investigação legal"[2] ou "devida investigação criminal"[3], tratando-se do momento persecutório em que, como regra, reclama-se o acesso aos dispositivos em comento para viabilizar a apuração dos fatos delitivos.

A aludida aplicação das garantias que defluem do devido processo é imprescindível na fase policial do processo criminal e o desrespeito às suas premissas inviabiliza ou macula a promoção da ação penal em juízo.

Com efeito, a reserva jurisdicional retrata um dos princípios configuradores da devida investigação legal, acompanhada das demais garantias como a motivação, a proibição de provas ilícitas, a legalidade, a presunção de não culpabilidade, a não autoincriminação, o contraditório e a defesa, que podem e devem ser aplicados desde o limiar da atuação estatal para a higidez da persecução penal.

A utilização massiva do telefone celular, como principal instrumento de acesso à internet, popularizou a telefonia

1. BADARÓ, Gustavo Henrique Righi Ivahy. *Processo penal*. Rio de Janeiro: Elsevier, 2014, p. 39-40.

2. BALDAN, Édson Luís. Devida investigação legal como derivação do devido processo legal e como garantia fundamental do imputado. In: KHALED JR., Salah (coord.). *Sistema penal e poder punitivo*: estudos em homenagem ao prof. Aury Lopes Jr. Florianópolis: Empório do Direito, 2015, p.165.

3. COELHO, Emerson Ghirardelli. *Investigação criminal constitucional*. Belo Horizonte: Del Rey, 2017, p. 47-48.

móvel inteligente, com os seus modelos de *smartphones* e variedade de aplicativos, transformou tais aparelhos em grandes depositários de informações e, por consequência, os acessos não autorizados em atos invasivos da privacidade, ensejando uma revisão quanto aos limites jurídicos dessa prática investigativa.[4]

A verificação dos telefones celulares nas abordagens de cidadãos por policiais tornou-se postura corriqueira, na medida em que os aparelhos figuram como um dos principais objetos de delitos patrimoniais, notadamente furtos e roubos, incluindo latrocínios. Os registros policiais adotaram o cadastro do número de IMEI[5] para auxiliar na recuperação de equipamentos subtraídos e a confirmação da identificação e de eventual procedência ilícita perpassa pela conferência dessa numeração, que pode estar ostentada no compartimento da bateria, em outro ponto na estrutura física do aparelho ou também ser obtida por intermédio da digitação da sequência "*#06#" no campo para ligações em cada telefone celular.

Cumpre lembrar que, se for necessário desbloquear a tela do telefone celular para confirmar a numeração IMEI, a ação importará conduta ativa do sujeito abordado para fornecer ou inserir a respectiva senha e ele poderá invocar a garantia da não autoincriminação para se abster de realizá-la, desencadeando a apreensão do aparelho diante de suspeita de origem espúria, sem prejuízo da responsabilização criminal pela subtração ou pela receptação do aparelho, de acordo com as circunstâncias apuradas em cada caso.

4. MACHADO, Leonardo Marcondes. Buscas em celulares sem ordem judicial: atalhos investigativos e nulidades. *Consultor Jurídico*, São Paulo, 26 mar. 2019. Disponível em: https://bit.ly/1C9hzNh. Acesso em: 29.04.2019.

5. IMEI consiste na sigla em inglês para *International Mobile Equipment Identity*, que em português significa "Identificação Internacional de Equipamento Móvel". Trata-se de uma numeração única, composta por quinze caracteres, que identifica cada aparelho de telefone celular.

04. RESERVA DE JURISDIÇÃO ABSOLUTA E RELATIVA

Fala-se em "reserva de jurisdição absoluta" quando o legislador constitucional impõe que a primeira palavra sobre determinada matéria seja do Poder Judiciário, que será o responsável pela moderação de medidas, em regra após requerimento da acusação ou da defesa, ou ainda via representação da instituição de polícia judiciária incumbida da perscrutação dos eventos que demandam essa intervenção judicial. Trata-se da visão tradicional da reserva jurisdicional, ao atribuir ao Juiz de Direito a primeira e última palavra sobre determinados atos estatais.[6]

Lado outro, há matérias em que a Carta Magna confere margem ao legislador para optar que uma autoridade administrativa determine uma medida, com posterior controle pelo Poder Judiciário, hipótese que tem sido designada "reserva de jurisdição relativa"[7], e nesse contexto se encontra boa parte da discussão sobre a exigência ou não de prévia ordem judicial para o acesso ao conteúdo de dispositivos eletrônicos.

Vale lembrar que, de um modo geral, o acesso independentemente de autorização judicial tem como supedâneo legal genérico a diligência arrolada no artigo 6º, inciso III, do Código de Processo Penal, que estabelece à Autoridade Policial, ao tomar conhecimento de infração penal "colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias", somada à previsão da Lei 12.830/2013, que dispõe sobre a investigação criminal conduzida pelo Delegado de Polícia, e no § 2º, de seu artigo 2º, estipula a requisição direta de exames peri-

6. CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição*. Coimbra: Almedina, 2003, p. 584.

7. BARBOSA, Ruchester Marreiros. Justa causa constitucionalmente embrionária e a reserva de jurisdição. In: HOFFMANN, Henrique et al. *Polícia judiciária no Estado de Direito*. Rio de Janeiro: Lumen Juris, 2017, p. 75-83; BRENE, Cleyson. Ativismo policial: o papel garantista do delegado de polícia. Salvador: JusPodivm, 2018, p. 149-155.

ciais, de informações, de documentos e de dados que interessem à apuração dos fatos.

Por sua vez, a reserva jurisdicional absoluta, com exigência de prévia modulação pelo Poder Judiciário, pode constar diretamente no texto constitucional ou em eventuais interpretações de seus dispositivos, sem prejuízo da disciplina pelo ordenamento infraconstitucional.

05. DOCUMENTOS E DADOS

O Código de Processo Penal (Decreto-lei 3.689/1941), no capítulo IX, de seu título VII, que cuida da prova, considera documentos "quaisquer escritos, instrumentos ou papéis, públicos ou particulares", na extração literal do seu artigo 232.

Outra referência complementar reside na Lei Federal 12.527/2011, conhecida como "Lei de Acesso a Informações", que em seu artigo 4º, inciso II, define documento como a "unidade de registro de informações, qualquer que seja o suporte ou formato", de maneira a atualizar e expandir a expressão para as plataformas digitais ou outros suportes que a evolução tecnológica viabilize.

Ademais, na mesma Lei 12.527/2011 é possível obter, a partir de seu artigo 4º, inciso I, a definição de informação como "dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato".

Para os fins deste ensaio, tanto os dados, como matéria-prima bruta da informação, quanto os documentos, serão tomados em suas acepções mais genéricas, de modo a contemplarem os arquivos digitais nos variados formatos como textos, planilhas, imagens, áudios, vídeos e quaisquer outros que possam integrar o conteúdo armazenado em dispositivos eletrônicos.

A seu turno, o acesso a documentos físicos dependerá do local onde se encontram, de maneira que órgãos públicos como regra não se sujeitam a reserva jurisdicional e documentos neles contidos podem ser requisitados diretamente pelas instituições de polícia judiciária, enquanto imóveis particulares poderão demandar eventual representação por busca e apreensão, sobretudo à luz da garantia constitucional da inviolabilidade do domicílio (CF, art. 5º, XI).

Já para documentos armazenados em dispositivos eletrônicos, o cenário é distinto, em especial após o advento da mencionada Lei 12.965/2014 (Marco Civil da *Internet*), adiante comentado.

06. ACESSO A DOCUMENTOS E DADOS ARMAZENADOS EM DISPOSITIVOS ELETRÔNICOS

Como adiantado, um dos aspectos de maior discussão hodierna consiste no acesso aos documentos e dados armazenados em dispositivos eletrônicos e sobretudo em aparelhos de telefonia móvel celular apreendidos pelas instituições de polícia judiciária, no sentido de constituir ou não matéria sob reserva de jurisdição absoluta.

Até 2014, a posição jurisprudencial, encabeçada pelo Supremo Tribunal Federal no então paradigmático HC 91.867-PA[8], era no sentido de que o aludido acesso não demandaria prévia autorização judicial, conforme se extrai do trecho do acórdão ora colacionado:

8. STF, HC nº 91.867-PA, 2ª Turma, Relator Min. Gilmar Mendes, j. 24/04/2012.

HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA.

[. . .]

< 02 > Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corréu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. 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. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha

/ NO ESTADO DEMOCRÁTICO DE DIREITO NÃO HÁ COMO CONSIDERAR O VÍCIO NO INQUÉRITO POLICIAL MERA IRREGULARIDADE /

/ LEVANDO EM CONSIDERAÇÃO O GRAU DE INVASÃO DA PRIVACIDADE, O ACESSO DESBUROCRATIZADO PODE ENSEJAR ABUSOS /

> investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação. 2.4 À guisa de mera argumentação, mesmo que se pudesse reputar a prova produzida como ilícita e as demais, ilícitas por derivação, nos termos da teoria dos frutos da árvore venenosa (fruit of the poisonous tree), é certo que, ainda assim, melhor sorte não assistiria à defesa. É que, na hipótese, não há que se falar em prova ilícita por derivação. Nos termos da teoria da descoberta inevitável, construída pela Suprema Corte norte-americana no caso Nix x Williams (1984), o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado. Bases desse entendimento que parecem ter encontrado guarida no ordenamento jurídico pátrio com o advento da Lei 11.690/2008, que deu nova redação ao art. 157 do CPP, em especial o seu § 2º.

Por esse entendimento, a proteção do inciso XII, do artigo 5º da Constituição Federal abarcaria a comunicação dos dados, porém não os dados em si e o depósito registral deles contidos nos dispositivos eletrônicos, característica cada vez mais comum nos aparelhos de telefonia móvel com múltiplas funcionalidades (*smartphones)*, equipados com aplicativos de comunicação que permitem a troca e o armazenamento de mensagens e arquivos de imagem, de áudio e de vídeo.

Entretanto, com o advento da Lei Federal 12.965/2014, o conhecido "Marco Civil da *Internet*", que estabeleceu princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no Brasil, o debate foi redirecionado, mormente diante da literalidade do artigo 7º, inciso III, do referido diploma, que reivindica autorização judicial para o acesso às "comunicações privadas armazenadas" e assim dispõe:

> O acesso à *internet* é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> [. . .]
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Conquanto a redação do citado dispositivo mencione "comunicações privadas armazenadas" e nem todos os dados e documentos contidos em um aparelho eletrônico sejam, necessariamente, provenientes de uma "comunicação privada", a nova disciplina conferida pela Lei 12.965/2014 ocasionou uma alteração na orientação jurisprudencial, que começou a considerar o acesso ao conteúdo de tais dispositivos objeto de reserva jurisdicional, com destaque para o Superior Tribunal de Justiça, que a partir de 2016 passou a anular decisões lastreadas na obtenção de dados armazenados em equipamentos eletrônicos sem autorização prévia do Poder Judiciário, como se observa na decisão no âmbito do HC nº 51.531-RO[9], da 6ª Turma, com ementa ora reproduzida:

9. STJ, HC nº 51.531-RO, 6ª Turma, Relator Min. Nefi Cordeiro, j. 19/04/2016.

> PENAL. PROCESSUAL PENAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. TRÁFICO DE DROGAS. NULIDADE DA PROVA. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL PARA A PERÍCIA NO CELULAR. CONSTRANGIMENTO ILEGAL EVIDENCIADO.
>
> < 01 > 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.
>
> < 02 > Recurso ordinário em habeas corpus provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos (grifamos).

A 5ª Turma do Superior Tribunal de Justiça, em decisão de 2017, também passou a seguir direção similar, consoante HC nº 75.055-DF[10], com a seguinte ementa:

10. STJ, HC nº 75.055-DF, 5ª Turma, Relator Min. Ribeiro Dantas, j. 21/03/2017.

> PROCESSUAL PENAL. RECURSO EM HABEAS CORPUS. TRÁFICO DE DROGAS. INTERCEPTAÇÃO TELEFÔNICA. ACESSO DE MENSAGENS DE TEXTO VIA WHATSAPP. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL. GARANTIAS CONSTITUCIONAIS. ART. 5º, X E XII, DA CF. ART. 7º DA LEI N. 12.965/2014. NULIDADE. OCORRÊNCIA. CONSTRANGIMENTO ILEGAL CONFIGURADO. RECURSO EM HABEAS CORPUS PROVIDO.
>
> < 01 > A Constituição Federal de 1988 prevê como garantias ao cidadão a inviolabilidade da intimidade, do sigilo de correspondência, dados e comunicações telefônicas, salvo ordem judicial.
>
> < 02 > A Lei n. 12.965/2014, conhecida como Marco Civil da Internet, em seu art. 7º, assegura aos usuários os direitos para o uso da internet no Brasil, entre eles, o da inviolabilidade da intimidade e da vida privada, do sigilo do fluxo de suas comunicações pela internet, bem como de suas comunicações privadas armazenadas.
>
> < 03 > A quebra do sigilo do correio eletrônico somente pode ser decretada, elidindo a proteção ao direito, diante dos requisitos próprios de cautelaridade que a justifiquem idoneamente, desaguando em um quadro

de imprescindibilidade da providência. (HC 315.220/RS, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 15/09/2015, DJe 09/10/2015).

< 04 > Com o avanço tecnológico, o aparelho celular deixou de ser apenas um instrumento de comunicação interpessoal. Hoje, é possível ter acesso a diversas funções, entre elas, a verificação de mensagens escritas ou audível, de correspondência eletrônica, e de outros aplicativos que possibilitam a comunicação por meio de troca de dados de forma similar à telefonia convencional.

< 05 > Por se encontrar em situação similar às conversas mantidas por e-mail, cujo acesso é exigido prévia ordem judicial, a obtenção de conversas mantidas pelo programa whatsapp, sem a devida autorização judicial, revela-se ilegal.

< 06 > Recurso em habeas corpus provido para declarar nula as provas obtidas no celular do recorrente sem autorização judicial, determinando que seja desentranhado, envelopado, lacrado e entregue ao denunciado do material decorrente da medida (grifamos).

Contudo, o próprio Superior Tribunal de Justiça tem revelado em alguns julgados importantes ressalvas, em especial na decisão da 6ª Turma exarada no HC nº 388.008-AP[11], de agosto de 2017, no sentido de legitimar o acesso direto e extrajudicial aos dados armazenados em aparelho de telefonia celular quando a demora na obtenção de uma prévia ordem judicial puder acarretar "prejuízos à investigação" ou "especialmente à vítima do delito":

11. STJ, HC nº 388.008-AP, 6ª Turma, Relatora Min. Maria Thereza de Assis Moura, j. 03/08/2017.

PROCESSO PENAL. NULIDADE. PROVA ILÍCITA. LAUDO PERICIAL ELABORADO EM APARELHO CELULAR SEM AUTORIZAÇÃO JUDICIAL. PESQUISA DE REGISTROS DE CHAMADAS, CONTEÚDO DE AGENDA, MENSAGENS DE TEXTO SMS, ETC. VIOLAÇÃO DO SIGILO DE DADOS. ART. 157 DO CPP.

< 01 > É inequivocamente nula a obtenção de dados existentes em aparelhos de telefonia celular ou em outros meios de armazenamento de dados, sem autorização judicial, ressalvada, apenas, excepcionalmente, a colheita da prova através do acesso imediato aos dados do aparelho celular, nos casos em que a demora na obtenção de um mandado judicial puder trazer prejuízos concretos à investigação ou especialmente à vítima do delito.

< 02 > É nulo o laudo pericial elaborado por requisição direta da autoridade policial no curso da investigação, sem autorização judicial, com obtenção de registros de chamadas depois da realização de ampla invasão aos canais de registros pessoais, tais como, agendas, mensagens de sms, etc, em verdadeira devassa de dados privados.

< 03 > Ordem concedida para anular o acórdão da apelação e permitir que outro seja proferido, uma vez retirado dos autos o laudo pericial 57/2007 (grifamos).

Atualmente o debate se encontra no Supremo Tribunal Federal, na pendência da decisão do Agravo em Recurso Extraordinário (ARE) nº 1.042.075-RJ[12], que em novembro de 2017 reconheceu a existência de repercussão geral da matéria constitucional suscitada e cujo julgamento foi incluído no calendário da Corte para o dia 07/08/2019.

12. STJ, HC nº 388.008-AP, 6ª Turma, Relatora Min. Maria Thereza de Assis Moura, j. 03/08/2017.

De fato, a prevalecer a orientação intermediária identificada em julgados do Superior Tribunal de Justiça, que admite exceções, para o acesso direto ao conteúdo de equipamentos eletrônicos apreendidos, o desafio será precisar parâmetros ou hipóteses a serem consideradas urgentes a ponto de acarretar prejuízos à investigação ou especialmente à vítima do delito.

07. PRISÃO EM FLAGRANTE, INVESTIGAÇÃO CRIMINAL E ACESSO A DISPOSITIVOS ELETRÔNICOS

A decretação da prisão em flagrante delito, como espécie do gênero decisão de indiciamento, demanda não apenas o estado de flagrância delitiva, seu requisito temporal, retratado em uma das modalidades dos incisos do artigo 302 do Código de Processo Penal, mas também a fundada suspeita, seu requisito probatório consubstanciado na justa causa (*fumus commissi delicti*), do § 1º, do artigo 304, do CPP, como suporte indiciário a autorizar o encarceramento extrajudicial fiel aos postulados da Carta Magna.[13]

13. MORAES, Rafael Francisco Marcondes de. Prisão em flagrante delito constitucional. Salvador: JusPodivm, 2018. p. 160-168.

Na perspectiva ora ventilada, o emprego do raciocínio da referida diferenciação entre reserva absoluta e reserva relativa de jurisdição, a primeira tida como a tradicional reserva jurisdicional com prévio controle judicial, incumbindo ao Juiz a primeira e última palavra acerca de determinados atos estatais, e a segunda a afastar o monopólio judicial da palavra inicial e mantendo derradeira contenção pelo Magistrado, autorizaria a adoção de medidas preliminares pelo Delegado de Polícia (Estado-investigação), sujeitas à posterior aferição do Poder Judiciário, como ocorreria no acesso direto aos dados armazenados em equipamentos eletrônicos apreendidos em situação flagrancial delitiva e prejudicial à apuração fática ou à pessoa ofendida.

A título de exemplo, cita-se caso concreto ocorrido no interior do Estado de São Paulo, em que um indivíduo foi preso em flagrante por delito de estupro tentado em concurso com o crime de armazenamento de imagens pornográficas de adolescente[14], conduta que tem sido denominada "sextorsão", neologismo derivado da aglutinação dos vocábulos "sexo" e "extorsão", ou ainda de "estupro virtual" (na realidade estupro cometido por meio virtual ou eletrônico), consubstanciada, em síntese, na coação de uma pessoa à prática sexual ou pornográfica, em troca da preservação em sigilo de imagem ou vídeo da vítima em nudez total ou parcial (conhecida pela expressão inglesa *nudes*), sob a promessa de mal injusto representado pela publicação e divulgação do material íntimo em ambiente virtual.

14. Processo nº 0001090-02.2017.8.26.0599, da 2ª Vara da Comarca de Capivari, vinculado ao Inquérito Policial nº 174/2017, da Delegacia de Polícia de Def. da Mulher.

Na ocasião, o suspeito, além de constranger a vítima com ela se comunicando via aplicativo de seu aparelho de telefonia móvel, no próprio dispositivo mantinha armazenadas as fotos que denotavam a materialidade da prática espúria, ação permanente que revelava a flagrância delitiva, nos termos do tipo penal do artigo 241-B do Estatuto da Criança e do Adolescente (Lei Federal nº 8.069/1990). Ante a comentada

tese da reserva relativa de jurisdição, estaria autorizado ao Delegado de Polícia o acesso a referidos dados contidos no aparelho telefônico, que exprimem o corpo do delito, com ulterior controle e avaliação judicial, que no citado caso homologou a custódia flagrancial decretada pela Autoridade de Polícia Judiciária.

Nesse sentido conclui Marcos Alexandre Coelho Zilli[15]:

> A apreensão de smartphones em contexto de prisão em flagrante adiciona um novo ingrediente a uma já complexa equação. A visibilidade e a imediatidade da prática ilícita autorizam o Estado, por seus agentes, a adotar medidas que restabeleçam a ordem pública e o império da lei penal. A restrição da liberdade, na forma de prisão em flagrante, é, portanto, uma reação legítima do Estado que assumiu o monopólio do exercício da jurisdição penal. A urgência dessa resposta prescinde de prévia ordem judicial, cujo controle é realizado a posteriori. A prisão em flagrante traz implícita a restrição de outros direitos fundamentais. A busca pessoal, por exemplo, é indispensável para o resguardo de quem executa a prisão, de terceiros e do próprio preso. A invasão domiciliar, por sua vez, é necessária não só para fazer cessar a prática ilícita, mas também para resguardar a integridade de eventual vítima. Traz implícita, ainda, a autorização para a busca de elementos probatórios que componham o corpo do delito (grifamos).

15. ZILLI, Marcos Alexandre Coelho. A prisão em flagrante e o acesso de dados em dispositivos móveis: nem utopia, nem distopia. Apenas a racionalidade. In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys Marcelo (Org.). Direitos fundamentais e processo penal na era digital: doutrina e prática em debate. São Paulo: InternetLab, 2018, p. 95-96.

Frisa-se que, como regra, ausente a urgência do estado flagrancial delitivo, a tendência será a exigência de autorização judicial para o acesso de dados e documentos contidos em dispositivos eletrônicos, embora ainda não exista consenso na jurisprudência e na doutrina.[16]

De toda sorte, sobre a aludida diretriz jurisprudencial a partir do mencionado artigo 7º, inciso III, do "Marco Civil da *Internet*", assim pondera Eduardo Luiz Santos Cabette:[17]

> 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. (...). Atualmente, o celular deixou de ser apenas um instrumento de conversação pela voz à longa distância, permitindo, diante do avanço tecnológico, o acesso de múltiplas funções, incluindo, no caso, a verificação da correspondência eletrônica, de mensagens e de outros aplicativos que possibilitam a comunicação por meio de troca de dados de forma similar à telefonia convencional.

16. ANTONIALLI, Dennys; ABREU, Jacqueline de Souza; MASSARO, Heloisa; LUCIANO, Maria. Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. Revista Brasileira de Ciências Criminais, vol. 154, ano 27, p. 177-214, abr. 2019.

17. CABETTE, Eduardo Luiz Santos. Viva-voz e prova ilícita: decisão do STJ. Boletim Instituto Brasileiro de Ciências Criminais (IBCCRIM), ano 25, nº 297, Agosto/2017, ISSN 1676-3661, p. 11-12.

18. MORAES, Rafael Francisco Marcondes de; PIMENTEL JR., Jaime. Polícia judiciária e a atuação da defesa na investigação criminal. Salvador: JusPodivm, 2018, p. 198.

Para tais hipóteses e outras maculadas por vícios na investigação criminal, a natureza da nulidade, relativa ou absoluta, pode comprometer a formação do conhecimento processual penal e desvirtuá-lo para graves injustiças diante de ilações deturpadas provenientes da ilicitude. No Estado Democrático de Direito não há como considerar o vício no inquérito policial mera irregularidade, na medida em que, em acentuada parcela dos casos, o ato eivado será imprestável e prejudicial ao justo processo.[18]

Nesse cenário, na prática da atividade de polícia judiciária, tem sido adotado como protocolo a representação para a concessão de ordem judicial de acesso a dispositivos eletrônicos cumulada, quando necessário, com representações por outras medidas cautelares como busca domiciliar ou prisões provisórias, notadamente em casos como investigações de delitos contra a dignidade sexual de vulneráveis, que envolvam material pornográfico digital com crianças ou adolescentes e outras modalidades criminosas em que o conteúdo de equipamentos eletrônicos consubstancia importante campo para a regular apuração dos fatos.[19]

Contudo, outro aspecto que reforça as polêmicas e conflitos de posicionamentos consiste na aplicação de normas de limitação à derivação da prova ilícita, como a "descoberta inevitável", que o Código de Processo Penal brasileiro conceitua equivocadamente como "fonte independente" ao dispor, no § 2º, de seu artigo 157, que seria "aquela que, por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto de prova". Isso porque tal conceito diz respeito ao que a doutrina aponta como sendo a teoria da "descoberta inevitável", originária dos Estados Unidos da América. Nesse sentido Renato Brasileiro de Lima assevera que "apesar de o dispositivo fazer menção à fonte independente, parece ter havido um equívoco por parte do legislador, pois, ao empregar o verbo no condicional, o conceito aí fornecido (seria capaz de conduzir ao fato objeto de prova) refere-se ao da limitação da descoberta inevitável"[20]. Na mesma linha, Denilson Feitoza afirma que "a fonte independente foi definida, no Brasil, nos termos do que se entende como descoberta inevitável".[21]

Destarte, a teoria da "descoberta inevitável", também designada "exceção da fonte hipotética independente"[22] é aquela que considera lícita a prova que deriva de outra prova originalmente ilegal pelo fato de que seria produzida inevitavelmente. Ou seja, sua descoberta seria inevitável, de maneira que ela independe da prova originalmente viciada.[23] Referida lógica, ao menos em abstrato, é passível de ser sustentada para o acesso preliminar ao conteúdo de dispositivos eletrônicos apreendidos visto que, pela dinâmica habitual, haverá subsequente e provável ordem judicial e os dados armazenados serão acessados de qualquer maneira.

Ainda dentro da temática proposta, oportuno acrescentar que o Superior Tribunal de Justiça reputou ilegal, mesmo diante de autorização judicial específica, o emprego da técnica de espelhamento, via aplicativo *Whatsapp Web*, para o acesso das conversas (pretéritas, atuais e futuras) do sujeito investigado.[24] O Tribunal entendeu que esse tipo de medida não se confunde com a interceptação das comunicações telefônicas ou com o acesso às conversas já realizadas e armazenadas no telefone celular e assim não encontra respaldo na ordem jurídica pátria, motivo pelo qual não poderia ser autorizada pelo Poder Judiciário, conforme ementa abaixo do julgamento do RHC nº 99.735-SC[25]:

19. Trata-se do protocolo adotado como regra, por exemplo, na Delegacia de Polícia de Repressão à Pedofilia, do Departamento Estadual de Homicídios e de Proteção à Pessoa (DHPP), da Polícia Civil do Estado de São Paulo.

20. LIMA, Renato Brasileiro de. Curso de processo penal. São Paulo: Editora Impetus, 2013, p. 880.

21. FEITOZA, Denilson. Reforma do processo penal. Rio de Janeiro: Impetus, 2008, p.199.

22. LIMA, Renato Brasileiro de. Curso de processo penal. São Paulo: Editora Impetus, 2013, p. 880.

23. MORAES, Rafael Francisco Marcondes de, PIMENTEL JR., Jaime. Polícia judiciária e a atuação da defesa na investigação criminal. Salvador: JusPodivm, 2018, p. 200-202.

24. MACHADO, Leonardo Marcondes. Buscas em celulares sem ordem judicial: atalhos investigativos e nulidades. Consultor Jurídico, São Paulo, 26 mar. 2019.
Disponível em: https://bit.ly/2LBNnuj. Acesso em: 29.04.2019.

25. STJ, RHC nº 99.735-SC, 6ª Turma, Relatora Min. Laurita Vaz, j. 27/11/2018.

RECURSO ORDINÁRIO EM HABEAS CORPUS. PENAL E PROCESSO PENAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO AO TRÁFICO. AUTORIZAÇÃO JUDICIAL DE ESPELHAMENTO, VIA WHATSAPP WEB, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. ANALOGIA COM O INSTITUTO DA INTERCEPTAÇÃO TELEFÔNICA. IMPOSSIBILIDADE. PRESENÇA DE DISPARIDADES RELEVANTES. ILEGALIDADE DA MEDIDA. RECONHECIMENTO DA NULIDADE DA DECISÃO JUDICIAL E DOS ATOS E PROVAS DEPENDENTES. PRESENÇA DE OUTRAS ILEGALIDADES. LIMITAÇÃO AO DIREITO DE PRIVACIDADE DETERMINADA SEM INDÍCIOS RAZOÁVEIS DE AUTORIA E MATERIALIDADE. DETERMINAÇÃO ANTERIOR DE ARQUIVAMENTO DO INQUÉRITO POLICIAL. FIXAÇÃO DIRETA DE PRAZO DE 60 (SESSENTA) DIAS, COM PRORROGAÇÃO POR IGUAL PERÍODO. CONSTRANGIMENTO ILEGAL EVIDENCIADO. RECURSO PROVIDO.

08. CONSIDERAÇÕES FINAIS

Foram abordados aspectos envolvendo o acesso aos dados armazenados em dispositivos eletrônicos, sobretudo a partir da exegese oriunda do advento da Lei 12.965/2014 (Marco Civil da *Internet*), a reclamar prévia ordem judicial, indicando reserva jurisdicional absoluta da matéria, sem olvidar do necessário diálogo e da disciplina promovida por outros diplomas legais.

Destarte, o ponto nevrálgico e que enfrenta maiores divergências consiste na falta de consenso doutrinário e jurisprudencial quanto ao referido acesso sem autorização judicial, sobretudo em situações de urgência, que possam acarretar prejuízo às investigações ou à vítima do fato delitivo.

Não se ignora que, levando em consideração o grau de invasão da privacidade e intimidade, ainda que pertinente para a persecução penal, o acesso desburocratizado pode ensejar abusos.

Espera-se que o Supremo Tribunal Federal, no julgamento do destacado Agravo em Recurso Extraordinário (ARE) nº 1.042.075-RJ, agendado para agosto de 2019 e com repercussão geral reconhecida, consiga dirimir a atual insegurança jurídica que orbita em torno do assunto.

As ponderações lançadas revelam a necessidade de permanente estudo sobre a temática, tendo em vista a sua relevância para o tratamento justo aos direitos fundamentais, sem prejuízo da conciliação com a busca de qualidade na consecução da Justiça Criminal.

09. REFERÊNCIAS

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza; MASSARO, Heloisa; LUCIANO, Maria. Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. *Revista Brasileira de Ciências Criminais,* vol. 154, ano 27, p. 177-214, abr. 2019.

BADARÓ, Gustavo Henrique Righi Ivahy. *Processo penal*. Rio de Janeiro: Elsevier, 2014.

BALDAN, Édson Luís. Devida investigação legal como derivação do devido processo legal e como garantia fundamental do imputado. In: KHALED JR., Salah (coord.). *Sistema penal e poder punitivo:* estudos em homenagem ao prof. Aury Lopes Jr. Florianópolis: Empório do Direito, 2015, p.155-182.

BARBOSA, Ruchester Marreiros. Justa causa constitucionalmente embrionária e a reserva de jurisdição. In: HOFFMANN, Henrique *et al*. *Polícia judiciária no Estado de Direito*. Rio de Janeiro: Lumen Juris, 2017, p. 75-83.

BRENE, Cleyson. *Ativismo policial*: o papel garantista do delegado de polícia. Salvador: JusPodivm, 2018.

CABETTE, Eduardo Luiz Santos. Viva-voz e prova ilícita: decisão do STJ. *Boletim Instituto Brasileiro de Ciências Criminais (IBCCRIM)*, ano 25, nº 297, agosto/2017, ISSN 1676-3661, p. 11-12.

CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição*. Coimbra: Almedina, 2003.

CASTRO, Henrique Hoffmann Monteiro de. Requisição de dados pelo delegado de polícia. In: CASTRO, Henrique Hoffmann Monteiro de; et al. *Investigação criminal pela polícia judiciária*. Rio de Janeiro: Lumen Juris, 2016, p. 97-110.

COELHO, Emerson Ghirardelli. *Investigação criminal constitucional*. Belo Horizonte: Del Rey, 2017.

FEITOZA, Denilson. *Reforma do processo penal*. Rio de Janeiro: Impetus, 2008.

LIMA. Renato Brasileiro de. *Curso de processo penal*. São Paulo: Editora Impetus, 2013.

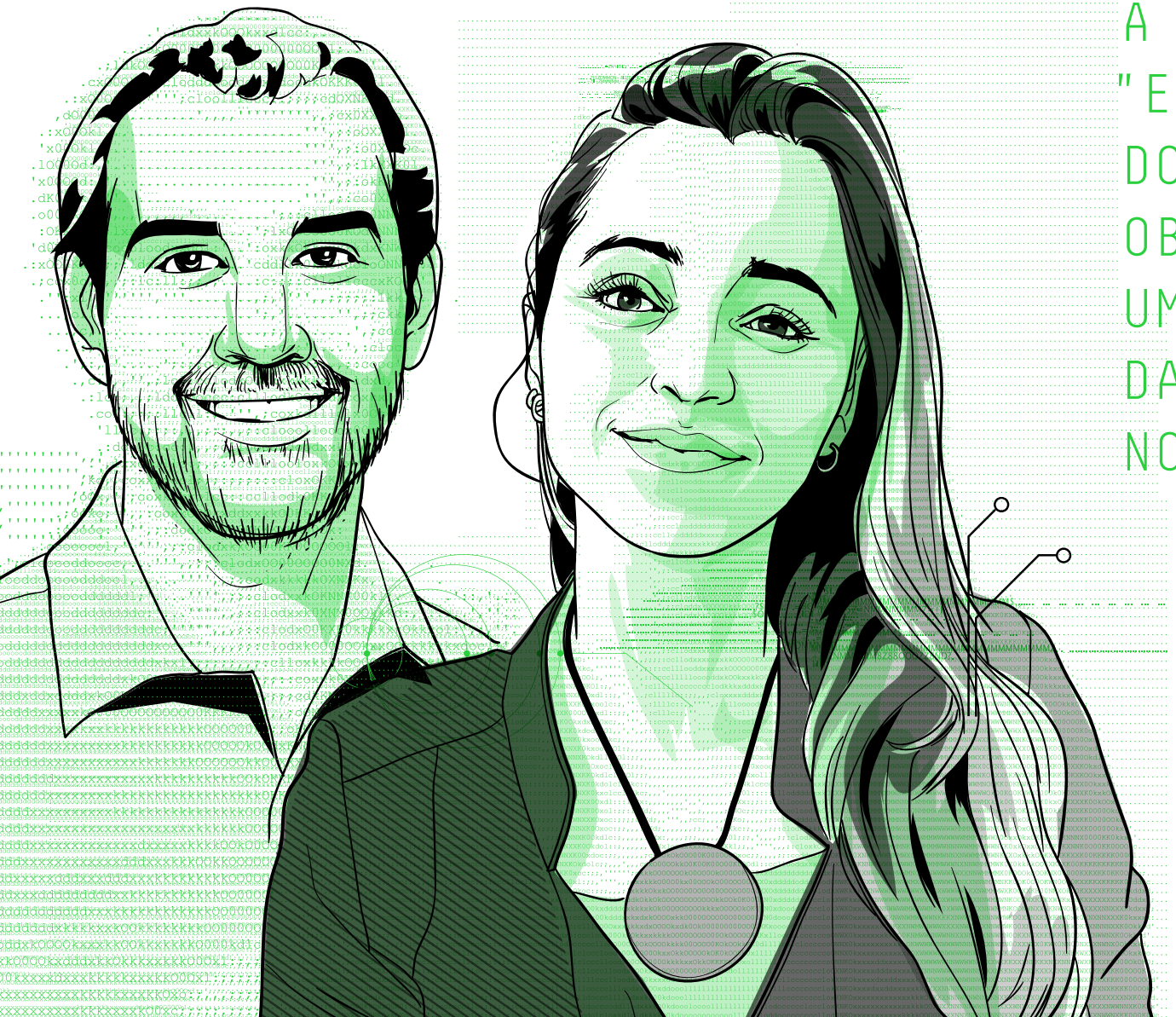
MACHADO, Leonardo Marcondes. Buscas em celulares sem ordem judicial: atalhos investigativos e nulidades. *Consultor Jurídico*, São Paulo, 26 mar. 2019. Disponível em: <www.conjur.com.br>. Acesso em: 29 abr.2019.

MORAES, Rafael Francisco Marcondes de; PIMENTEL JR., Jaime. *Polícia judiciária e a atuação da defesa na investigação criminal*. Salvador: JusPodivm, 2018.

MORAES, Rafael Francisco Marcondes de. *Prisão em flagrante delito constitucional*. Salvador: JusPodivm, 2018.

ZILLI, Marcos Alexandre Coelho. A prisão em flagrante e o acesso de dados em dispositivos móveis: nem utopia, nem distopia. Apenas a racionalidade. In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys Marcelo (Org.). *Direitos fundamentais e processo penal na era digital:* doutrina e prática em debate. São Paulo: InternetLab, 2018, p. 64-99.

08.



A TÉCNICA DE "ESPELHAMENTO" DO WHATSAPP PARA OBTENÇÃO DE PROVAS: UMA RESENHA DA DECISÃO DO STJ NO HC 99.735-SC

Dennys Antonialli
Nathalie Fragoso

01. INTRODUÇÃO

O desenvolvimento de novas tecnologias e o consequente incremento das capacidades e estratégias de obtenção de dados e informações têm influenciado significativamente a forma como se promove o conhecimento dos fatos no processo penal.[1] Com a popularização de aplicativos de troca de mensagens instantâneas, como WhatsApp e Telegram, diferentes questões a respeito dos direitos à privacidade e ao sigilo das comunicações são inauguradas ou revistas na doutrina processual penal. Se, de um lado, a criptografia de ponta-a-ponta é essencial para garantir a segurança e integridade das comunicações privadas, de outro, ela impõe novos obstáculos para o acesso ao seu conteúdo das comunicações por parte das autoridades de investigação.

1. SANTORO, Antonio E. R.; TAVARES, Natália L. F.; GOMES, Jefferson C. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 3, n. 2, p. 607.

As tensões geradas pelo descumprimento de ordens judiciais exigindo a entrega do conteúdo - ou a interceptação - de comunicações trocadas nesses aplicativos, que culminaram, inclusive, em ordens de bloqueio do WhatsApp no Brasil e suscitaram o ajuizamento da ADPF 403[2] e da ADI 5527[3] no Supremo Tribunal Federal, vem sendo respondidas com novas técnicas investigação para superar essa dificuldade de acesso. Nesse contexto, a efetividade de garantias processuais, como o devido processo e o contraditório, depende, em larga medida, da discussão a respeito do funcionamento e implementação dessas técnicas e das especificidades em relação às formas tradicionais de investigação que já estão disciplinadas no ordenamento jurídico brasileiro. O acompanhamento da jurisprudência e a identificação da forma como os tribunais lidam com os dados e informações obtidos a partir da utilização dessas novas técnicas é, nesse sentido, uma importante tarefa na análise da acomodação de tais inovações pelo direito e das balizas eventualmente estabelecidas em seu emprego e implementação.

2. Cf. BARROS, Paula Pécora de, "ADPF 403 no STF: bloqueios do WhatsApp são constitucionais?", disponível em https://bit.ly/2XT10KS

3. Cf. MANSUR, Felipe, "ADI 5527 e bloqueios: um problema na redação da lei ou sua interpretação? Disponível em https://bit.ly/2iQvRSu

Recuperamos aqui, com esse objetivo, os fundamentos do acórdão, relatado pela Ministra Laurita Vaz, no Recurso Ordinário em Habeas Corpus nº 99.735 - SC (2018/0153349-8), que teve por objeto a técnica de "espelhamento" de mensagens do Whatsapp.[4]

4. STJ. Recurso em Habeas Corpus nº 99.735 - SC (2018/0153349-8), Rel. Min. Laurita Vaz. 6a Turma, j. 27.11.2018. Disponível em: https://bit.ly/2KWZKlb.

02. O RECURSO EM HABEAS CORPUS Nº 99.735 - SC

Julgado em 27 de novembro de 2018, o recurso em habeas corpus impetrado desafia a decisão judicial que autorizou o acesso a comunicações trocadas por meio do WhatsApp, mediante apreensão do aparelho celular e posterior "espelhamento", via QR Code, na modalidade WhatsApp Web. O procedimento compreendeu a abordagem do indivíduo, a apreensão do seu aparelho celular, a sua utilização para acesso à conta de WhatsApp e autorização do respectivo emparelhamento com o computador da autoridade policial. Ao final, o aparelho celular foi devolvido sem qualquer notificação a respeito da operação.

Dessa maneira, foi possível obter acesso ao conteúdo das mensagens e dados armazenados de todas as conversas registradas no WhatsApp do investigado, bem como o acompanhamento dos - e a potencial intervenção sobre - diálogos a partir de então travados.

A decisão da Sexta Turma do Superior Tribunal de Justiça, relatada pela Ministra Laurita Vaz, conclui pela ilegalidade da medida e foi assim ementada:

> RECURSO ORDINÁRIO EM HABEAS CORPUS. PENAL E PROCESSO PENAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO AO TRÁFICO. AUTORIZAÇÃO JUDICIAL DE ESPELHAMENTO, VIA WHATSAPP WEB, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. ANALOGIA COM O INSTITUTO DA INTERCEPTAÇÃO TELEFÔNICA. IMPOSSIBILIDADE. PRESENÇA DE DISPARIDADES RELEVANTES. ILEGALIDADE DA MEDIDA. RECONHECIMENTO DA NULIDADE DA DECISÃO JUDICIAL E DOS ATOS E PROVAS DEPENDENTES. PRESENÇA DE OUTRAS ILEGALIDADES. LIMITAÇÃO AO DIREITO DE PRIVACIDADE DETERMINADA SEM INDÍCIOS RAZOÁVEIS DE AUTORIA E MATERIALIDADE. DETERMINAÇÃO ANTERIOR DE ARQUIVAMENTO DO INQUÉRITO POLICIAL. FIXAÇÃO DIRETA DE PRAZO DE 60 (SESSENTA) DIAS, COM PRORROGAÇÃO POR IGUAL PERÍODO. CONSTRANGIMENTO ILEGAL EVIDENCIADO. RECURSO PROVIDO.
>
> < 01 > Hipótese em que, após coleta de dados do aplicativo WhatsApp, realizada pela Autoridade Policial mediante apreensão judicialmente autorizada de celular e subsequente espelhamento das mensagens recebidas e enviadas, os Recorrentes tiveram decretadas contra si prisão preventiva, em razão da suposta prática dos crimes previstos nos arts. 33 e 35 da Lei n.o 11.343/2006.
>
> < 02 > O espelhamento das mensagens do WhatsApp ocorre em sítio eletrônico disponibilizado pela própria empresa, denominado WhatsApp Web. Na referida plataforma, é gerado um tipo específico de código de barras, conhecido como Código QR (Quick Response), o qual só pode ser lido pelo celular do usuário que pretende usufruir do serviço. Daí a necessidade de apreensão, ainda que por breve período de tempo, do aparelho telefônico que se pretende monitorar.
>
> < 03 > Para além de permitir o acesso ilimitado a todas as conversas passadas, presentes e futuras, a ferramenta WhatsApp Web foi desenvolvida com o objetivo de possibilitar ao usuário a realização de todos os atos de comunicação a que teria acesso no próprio celular. O emparelhamento entre celular e computador autoriza o usuário, se por algum motivo assim desejar, a conversar dentro do aplicativo do celular e, simultaneamente, no navegador da internet, ocasião em que as conversas são automaticamente atualizadas na plataforma que não esteja sendo utilizada.
>
> < 04 > Tanto no aplicativo, quanto no navegador, é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato. Eventual exclusão de mensagem enviada (na opção "Apagar somente para Mim") ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal, tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários.
>
> < 05 > Cumpre assinalar, portanto, que o caso dos autos difere da situação, com legalidade amplamente reconhecida pelo Superior Tribunal de Justiça, em que, a

exemplo de conversas mantidas por e-mail, ocorre autorização judicial para a obtenção, sem espelhamento, de conversas já registradas no aplicativo WhatsApp, com o propósito de periciar seu conteúdo.

< 06 > É impossível, tal como sugerido no acórdão impugnado, proceder a uma analogia entre o instituto da interceptação telefônica (art. 1.o, da Lei n.o 9.296/1996) e a medida que foi tomada no presente caso.

< 07 > Primeiro: ao contrário da interceptação telefônica, no âmbito da qual o investigador de polícia atua como mero observador de conversas empreendidas por terceiros, no espelhamento via WhatsApp Web o investigador de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder, conferido pela própria plataforma online, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura.

< 08 > O fato de eventual exclusão de mensagens enviadas (na modalidade "Apagar para mim") ou recebidas (em qualquer caso) não deixar absolutamente nenhum vestígio nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia end-to-end, não ficarem armazenadas em nenhum servidor, constituem fundamentos suficientes para a conclusão de que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica.

< 09 > Segundo: ao contrário da interceptação telefônica, que tem como objeto a escuta de conversas realizadas apenas depois da autorização judicial (ex nunc), o espelhamento via Código QR viabiliza ao investigador de polícia acesso amplo e irrestrito a toda e qualquer comunicação realizada antes da mencionada autorização, operando efeitos retroativos (ex tunc).

< 10 > Terceiro: ao contrário da interceptação telefônica, que é operacionalizada sem a necessidade simultânea de busca pessoal ou domiciliar para apreensão de aparelho telefônico, o espelhamento via Código QR depende da abordagem do indivíduo ou do vasculhamento de sua residência, com apreensão de seu aparelho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da Autoridade Policial, à realização da medida constritiva, ou mesmo, porventura – embora não haja nos autos notícia de que isso tenha ocorrido no caso concreto –, acompanhada de afirmação falsa de que nada foi feito.

< 11 > Hipótese concreta dos autos que revela, ainda, outras três ilegalidades: (a) sem que se apontasse nenhum fato novo na decisão, a medida foi autorizada quatro meses após ter sido determinado o arquivamento dos autos; (b) ausência de indícios razoáveis da autoria ou participação em infração penal a respaldar a limitação do direito de privacidade; e (c) ilegalidade na fixação direta do prazo de 60 (sessenta) dias, com prorrogação por igual período.

< 12 > Recurso provido, a fim de declarar a nulidade da decisão judicial que autorizou o espelhamento do WhatsApp via Código QR, bem como das provas e dos atos que dela diretamente dependam ou sejam consequência, ressalvadas eventuais fontes independentes,

revogando, por conseguinte, a prisão preventiva dos Recorrentes, se por outro motivo não estiverem presos.

03. FUNDAMENTOS DA DECISÃO

Para analisar as questões suscitadas, o voto da Ministra relatora, Laurita Vaz, seguido unanimemente pelos demais ministros da Sexta Turma do STJ, acerca-se, primeiro, das características que configuram a técnica de "espelhamento" de uma conta de WhatsApp, especialmente quanto à forma de implementação e à extensão do acesso conferido aos atores envolvidos na investigação.

Em uma breve descrição, a técnica de "espelhamento" de uma conta de WhatsApp consiste na exploração de uma modalidade de utilização do serviço oferecida pelo próprio provedor da aplicação: WhatsApp Web. A modalidade foi desenvolvida para permitir o uso de uma conta de WhatsApp a partir de um navegador de internet. Para habilitar sua utilização, a plataforma estabeleceu um procedimento de segurança, consistente na geração de um Código QR (Quick Response) que deve ser lido pelo aplicativo instalado no celular do usuário, como forma de autenticação da conta.

O acesso assim estabelecido - que, aliás, pode se perpetuar indeterminadamente, até que seja deliberadamente interrompido-, além de alcançar a observação de todas as conversas, permite o uso simultâneo do aplicativo, o envio e a exclusão de mensagens enviadas ou recebidas pelo usuário. Eventuais inserções ou exclusões de mensagens não deixam, ademais, vestígios no aplicativo, no computador emparelhado e, como não há armazenamento pelo provedor, não podem ser posteriormente identificados.

Diante destes elementos, entre as razões de decidir, está, primeiro e principalmente, o afastamento de uma relação de analogia entre o espelhamento e a interceptação telefônica.

Interessa notar, no entanto, que essa não é a tese adotada na manifestação do Ministério Público, nem no acórdão recorrido. Aquela, aliás, argui que, "diferentemente da interceptação telefônica, não há previsão legal limitando o prazo, admitindo-se a apreensão das mensagens arquivadas em bancos de dados". Equipara o espelhamento, portanto, à apreensão de mensagens armazenadas em bancos de dados. Já o acórdão recorrido, não fala em analogia, mas subsunção e considera tratar-se de uma interceptação telemática:

> " (...) assertiva segundo a qual o monitoramento das mensagens não possui previsão legal esbarra na redação do art. 1º, caput e parágrafo único, da Lei 9.296/1996, que dispõem: 'Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.' Como se vê, bem cuidou o legislador, atento aos vertiginosos aprimoramentos tecnológicos que perpassam a modernidade, de conferir ao citado dispositivo legal conformação textual permeável a tais mudanças, de modo que por este foi abarcada não apenas a transmissão da voz humana por aparelhos de comunicação à distância, como também aquela realizada por outros meios, entre eles a escrita. É que a tensão constitutiva entre a necessária observância de direitos e garantias fundamentais, de um lado, e a efetividade da pretensão punitiva, de outro, anima de modo perene a persecução penal e, assim, jamais pode ser resolvida com caráter definitivo e unilateral em favor de um desses polos."[5]

De acordo com os termos do acórdão do STJ, o espelhamento via WhatsApp Web, diferentemente da interceptação, extrapola a mera observação - aliás possível em relação a todos os contatos do investigado - e permite a participação, isto é, a manipulação do conteúdo das conversas registradas e em andamento através do aplicativo. Ao permitir a interação por meio da plataforma online, são possibilitados o envio de novas mensagens aos contatos do investigado e a sua respectiva exclusão no dispositivo, sem vestígios. É nesse contexto, a propósito, que a relatora aborda a presunção - dita relativa - de legitimidade que caracterizaria os atos de funcionários públicos. Por suas características, o espelhamento a converteria em absoluta, ao tornar a contestação por parte do investigado impossível.

5. Cf. TRIBUNAL DE JUSTIÇA DE SANTA CATARINA. Habeas Corpus n. 4011613-76.2018.8.24.0000, de Navegantes. Rel. Des. Luiz Cesar Schweitzer, Quinta Câmara Criminal, j. 7.06.2018.

Embora tal presunção seja ela mesma objeto de controvérsia, o prejuízo relativo imposto ao exercício do contraditório na produção da prova posto pelo meio de obtenção é aqui o objeto de atenção. Isso porque, em um contexto, como o brasileiro, em que a prova testemunhal é fundamental para o desfecho do processo e em que os atores do sistema de justiça criminal reconhecem que o testemunho policial é, com frequência, o lastro único de condenações criminais, a enunciação de uma presunção, ainda que relativa, de legitimidade, compromete uma outra presunção, a de inocência.[6] A presunção em favor da credibilidade dos testemunhos e da regularidade da conduta dos agentes policiais mitiga o contraditório, ao dificultar o questionamento da credibilidade das fontes e da confiabilidade das evidências, e podem constituir obstáculo na identificação de irregularidades e

6. Cf. BRASIL. Avanços científicos em psicologia do testemunho aplicados ao reconhecimento pessoal e aos depoimentos forenses. Brasília: Ministério da Justiça/Ipea, 2015a, p. 64.

na prevenção de condenações injustas.[7] Nesse sentido, justamente porque incumbidos do uso da força, da imposição de restrições sumárias à liberdade e da seleção dos sujeitos que serão submetidos ao controle penal, é que é devido um rígido controle das evidências fornecidas por policiais em juízo.[8]

7. Cf. THOMPSON, S. G. Judicial gatekeeping of police-generated witness testimony. The Journal of Criminal Law and Criminology, v. 102, n. 2, p. 329–395, 2018.

8. Cf. DORFMAN, D. N. Proving the lie: litigating police credibility. Pace Law Faculty Publications. v. 26, n. 455, p. 1–50, 1999.

Outro elemento de diferenciação da interceptação telefônica está na abrangência temporal do objeto da "escuta": o espelhamento via WhatsApp Web viabiliza ao investigador o acesso amplo e irrestrito a todas as comunicações travadas com quaisquer interlocutores, inclusive aquelas anteriores à respectiva autorização, produzindo assim efeitos retroativos. Segundo a relatora, tratar-se-ia de um tipo híbrido – e não previsto em lei - de obtenção de prova consistente, a um só tempo, em interceptação telefônica e em quebra de sigilo de *e-mail*. Finalmente, ao contrário da interceptação telefônica, a técnica de espelhamento depende da abordagem do indivíduo e da realização de buscas, da apreensão do aparelho telefônico e da devolução desacompanhada de qualquer menção à realização da medida.

As outras três razões apontadas pela ministra consistem *(i)* na inexistência de fato novo na decisão que autorizou o espelhamento, após seis meses da determinação do arquivamento dos autos em razão da inexistência de indícios de autoria e materialidade delitiva, em desacordo com a orientação do Superior Tribunal de Justiça[9]; *(ii)* no desrespeito à exigência (art. 2.º, inciso I, da Lei n.º 9.296/1996) de "indícios razoáveis da autoria ou participação em infração penal" para justificar a limitação do direito de privacidade consistente na interceptação; e *(iii)* na extrapolação do prazo de 15

9. STJ. Recurso em Habeas Corpus 41.933/SP. Rel. Ministro Felix Fischer, Quinta Turma, j. 11.06.2015

dias para a execução da medida "em manifesta contrariedade e negativa de vigência ao artigo 5º da Lei n.º 9.296/1996". As duas últimas hipóteses consideram, ainda que por conjectura, pertinente a analogia com a interceptação telefônica.

Ao final, foi declarada a nulidade da autorização de espelhamento do WhatsApp, das provas e dos atos dela dependentes e revogados os decretos de prisão preventiva dos recorrentes.

04. OBSTÁCULOS AO CONTRADITÓRIO: A TÉCNICA DE ESPELHAMENTO E O CONTROLE DA INTEGRIDADE DAS PROVAS

Na argumentação encampada pela ministra, merece atenção, em primeiro lugar, o esforço no sentido de compreender e diferenciar o meio de obtenção de provas utilizado das formas tradicionais de obtenção de elementos informativos, já minimamente regulamentadas. No caso das interceptações, vale lembrar que a Lei no 9.296/1996 estabeleceu os requisitos necessários para a sua autorização, quais sejam (i) a configuração de indícios razoáveis da autoria ou participação em infração penal; (ii) a inexistência de outros meios de prova; e (iii) o envolvimento em crimes de maior gravidade e definiu um limite temporal para realização da medida. Já no caso de acesso a comunicações armazenadas por um intermediário, o Marco Civil da Internet (Lei no 12.695/14) determina a necessidade de "ordem judicial" (art. 7º, III) nas hipóteses e na forma que a lei estabelecer (art. 10, § 2º), sem, entretanto, explicitar requisitos substantivos de padrão probatório. No caso de acesso a comunicações armazenadas em aplicativos como WhatsApp, tribunais têm inclusive admitido a devassa de aparelhos sem ordem judicial.[10]

10. Cf. ANTONIALLI, Dennys; et al. Acesso de autoridades policiais a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. Revista Brasileira de Ciências Criminais, vol. 154, ano 27, p. 177-214, 2019

/ O ESPELHAMENTO EXTRAPOLA A MERA OBSERVAÇÃO E PERMITE A MANIPULAÇÃO DO CONTEÚDO DAS CONVERSAS /

Dito issso, seria, no mínimo, impreciso comparar os dados armazenados nos dispositivos do usuário de WhatsApp, como mensagens, áudios, imagens, documentos, a uma ligação telefônica. Sendo assim, a técnica de espelhamento não encontra respaldo na Lei das Interceptações. Além disso há complexas e inúmeras dificuldades de verificação das fontes de prova nesses casos.[11]

Para analisar este ponto em específico, cabe retomar a noção de cadeia de custódia. Embora mais frequentemente associada ao manejo de vestígios médico-legais ou de amostras submetidas a exames toxicológicos, a cadeia de custódia também diz respeito, sobretudo atualmente, à extração de dados. Definida na Portaria nº 82, de 16 de julho de 2014, da Secretaria Nacional de Segurança Pública, como o conjunto de "procedimentos utilizados para manter e documentar a história cronológica do vestígio", "rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte",[12] a cadeia de custódia estabelece a necessidade de documentação da coleta, do manuseio e da análise; de registro dos agentes incumbidos desses processos; além da observância de procedimentos capazes de preservar a integridade da prova e garantir a sua rastreabilidade[13].

Especialmente em se tratando de meios de obtenção de prova empregados na fase pré-processual, sem o conhecimento do investigado e, portanto, sem o contraditório pleno, a idoneidade do processo tende a ficar comprometida sem a sua observância.[14]

Afinal, para que a defesa tenha condições de exercer o contraditório, ainda que diferido, são cruciais a compreensão e a capacidade de fiscalizar a origem e verificar a integridade, confiabilidade e originalidade dos elementos trazidos aos autos.[15] A esse respeito, Geraldo Prado destaca ainda que a cadeia de custódia, ao preservar esta oportunidade, isto é, ao concretizar o princípio da "mesmidade" e garantir a integral identidade entre a prova valorada e a colhida, preserva também o "valor epistêmico do conteúdo probatório".[16] Outro princípio, assim observado, seria o da "desconfiança". Deste, em contraste com as presunções que fragilizam os direitos do acusado ou réu, decorre a necessidade de acreditação dos elementos trazidos aos autos, isto é, de teste e demonstração, ao invés de regularidade presumida.

Assim é que, na decisão, a ilicitude da prova obtida através da técnica de espelhamento deriva no reconhecimento de que não seria possível a recuperação ou rastreio de todos os atos da operação, com a respectiva e necessária verificação da existência de eventual manipulação ou adulteração de seu conteúdo. Ainda que não mencionada, é dos propósitos da cadeia de custódia que se trata, ao controlar, por exemplo, a fidedignidade dos elementos e, no processo de sua obtenção, transporte, análise, sua suscetibilidade à manipulação.

Cabe aqui o destaque de que são abordados traços inerentes ao espelhamento, como meio de obtenção, e não a inexistente disciplina legal, o desrespeito às regras postas ou a

11. Cf. SANTORO, Antonio Eduardo Ramires; et al. O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. Revista Brasileira de Direito Processual Penal, volume 3, n. 02, 2017

12. Conceito veiculado na Portaria nº 82, de 16 de julho de 2014, Secretaria Nacional de Segurança Pública. Disponível em: https://bit.ly/2R8SRjo

13. LOPES, M.; GABRIEL, Maria Madalena; BARETA, G. M. S.. CADEIA DE CUSTÓDIA: UMA ABORDAGEM PRELIMINAR. Visão Acadêmica, [S.l.], jun. 2006. ISSN 1518-8361. Disponível em: https://bit.ly/2NvYfgd. Acesso em: 02.07.2019.

14. SILVA, R. S. M. A interceptação das comunicações telemáticas no processo penal. Dissertação. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014.

15. SILVA, R. S. M. A interceptação das comunicações telemáticas no processo penal. Dissertação. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014.

16. PRADO, Geraldo. Ainda sobre a "quebra da cadeia de custódia das provas". Boletim IBCCRIM, São Paulo, ano 22, nº 262, p. 16-17, set./2014.

deficiência da ordem judicial na indicação de balizas. Ainda assim, são pertinentes considerações acerca da reserva legal endossada no voto da relatora, já que a cadeia de custódia se perfaz num "procedimento regrado e formalizado", para o "exercício do controle epistêmico".[17]

Amostra das novidades da era da digital[18], o espelhamento é uma forma de investigação profundamente invasiva e potencialmente comprometedora da paridade de armas, da presunção de inocência, do devido processo legal, da ampla defesa e do contraditório no processo penal (art. 5º, LIV, LV e LVII, CF). Diferenciando-a, inicialmente, da interceptação – a captação de comunicações contemporâneas, enquanto ocorrem - e excluindo-a, assim, da incidência da Lei nº 9.296/1996, a decisão reforça pontualmente a necessidade de previsão legal como fundamento de medidas constritivas do direito à privacidade.[19]

Embora o processo penal brasileiro não conheça um sistema taxativo de meios de prova, sendo admitidas, segundo a doutrina majoritária, provas não previstas em lei,[20] a reserva legal, decorrente do art. 5º, XII, da Constituição Federal e do que vem sendo reafirmado em cortes internacionais como elemento de um julgamento justo[21], é importante providência na aposição de balizas que reforcem garantias diante do desenvolvimento tecnológico. Noutro contexto, cabe lembrar, a carência de previsão legal levou o Supremo Tribunal Federal a declarar a inadmissibilidade das interceptações telefônicas anteriores à Lei nº 9.296/1996.[22] Uma vez regulamentada, em razão da intrusividade da medida, a interceptação foi destinada, ao menos em tese, ao uso em casos extraordinários, condicionada à indisponibilidade de outros meios e à adoção de cautelas para garantia da intimidade e a liberdade.

Não acreditamos ser este, no entanto, o caso do espelhamento, pelas razões abordadas na própria decisão, isto é, a frustração das premissas para a adequada instrução probatória decorre de atributos da tecnologia. Provas inverificáveis não se harmonizam com quaisquer garantias processuais. A consideração, no entanto, merece perpetuar-se diante do desafio imposto pelo crescente e, sempre atualizado, uso das tecnologias de comunicação e informação na persecução penal.

O produto deste equacionamento, ao final, guarda íntima relação com significado e os limites que a paridade de armas, presunção de inocência, devido processo legal, ampla defesa e contraditório (art. 5º, LIV, LV e LVII, CF) lograrão impor à persecução na era digital.

17. LOPES JUNIOR, Aury; ROSA, Alexandre Morais da. A importância da cadeia de custódia para preservar a prova penal. Disponível em: https://bit.ly/2KXITMd.

18. COSTA ANDRADE, Manuel. "Bruscamente no verão passado", a reforma do Código de Processo Penal: observações críticas sobre uma lei que podia e devia ter sido diferente. Coimbra, 2009, p. 21.

19. "Não há, todavia, ao menos por agora, previsão legal de um tal meio de obtenção de prova híbrido". Cf. STJ Recurso em Habeas Corpus nº 99.735 - SC (2018/0153349-8). Rel. Min. Laurita Vaz, 6a Turma, j.27.11.2018. Disponível em: https://bit.ly/2KWZKlb.

20. BADARÓ, Gustavo. Processo Penal. Rio de Janeiro: Campos, Elsevier, 2012, p. 273.

21. Cf. CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros vs. Brasil, sentença de 6 de julho de 2009.

22. STF, HC 72588/PB, rel. Min. Maurício Correa, Pleno, j. 12.06.1996.

ESTE LIVRO FOI COMPOSTO COM AS FAMÍLIAS TIPOGRÁFICAS *DECIMA MONO* E *FF META*. PARA O MIOLO FOI UTILIZADO O PAPEL OPALINA E PARA A CAPA O PAPEL DUO DESIGN 300G/M². O PROJETO GRÁFICO É DE AUTORIA DO *ESTÚDIO CLARABOIA* E AS ILUSTRAÇÕES SÃO DA *PINGADO SOCIEDADE ILUSTRATIVA*. FORAM IMPRESSAS 300 CÓPIAS PELA GRÁFICA CINELÂNDIA EM JULHO DE 2019.

INTERNETLAB
pesquisa em direito e tecnologia