Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 29.11.2018
Aprovado em: 13.12.2018

Revista Brasileira de Direitos e Garantias Fundamentais

A INVIOLABILIDADE DOS DADOS PESSOAIS E O CONTROLE JUDICIAL DA PROVA ELETRÔNICA ILÍCITA

Tarcísio Teixeira*
Américo Ribeiro Magro*

Resumo: O trabalho analisa a inviolabilidade, especialmente penal, dos dados pessoais informáticos, decorrente de garantias fundamentais do processo. Principia analisando o conteúdo e o âmbito de proteção da inadmissibilidade das provas ilícitas, correlacionando-a com outras garantias e direitos de índole constitucional, como o direito à privacidade e a liberdade de comunicação. Após, qualifica os dados pessoais de comunicação sob a perspectiva técnica e legislativa, conforme a novel Lei nº 13.709/2018. Finaliza destacando o controle judicial prévio e motivado dos meios de prova eletrônicos. Utiliza-se o método dedutivo e comparativo, com base em pesquisa de legislação, doutrina e jurisprudência, nacional e comparada.

Palavras-chave: Dados pessoais. Provas ilícitas. Comunicações. Reserva judicial. Lei nº 13.709/2018.

THE INVIOLABILITY OF PERSONAL DATA AND THE JUDICIAL CONTROL OF THE UNLAWFUL ELECTRONIC PROOF

Abstract: The work analyzes the inviolability, especially criminal, of personal computer data, which derives from fundamental guarantees of the process. It begins analyzing the content and scope of protection against unlawful evidence, correlating it with other constitutional guarantees and rights, such as the right to privacy and the freedom of communication. After, it qualifies the personal data of communication from technical and legislative perspectiva, according to novel Law nº 13709/2018. It ends by highlighting prior and motivated judicial control of electronic evidence. It employs the deductive and comparative methods, based on research of the legislation, doctrine and jurisprudence, national and foreign.

Key words: Personal data. Unlawful evidence. Communications. Judicial reserve. Law nº 13.709/2018.

1 INTRODUÇÃO

* Doutor e Mestre em Direito Comercial pela Faculdade de Direito do Largo São Francisco (USP). Professor Adjunto de graduação e mestrado da Universidade Estadual de Londrina (UEL). E-mail: contato@tarcisioteixeira.com.br.
* Advogado. Mestrando em Direito Negocial pela Universidade Estadual de Londrina (UEL). Especialista em Interesses Difusos e Coletivos pelo Centro Universitário "Antônio Eufrásio de Toledo" de Presidente Prudente. Especialista em Direito Eleitoral pela Universidade de Santa Cruz do Sul (UNISC). E-mail: americomagro@hotmail.com.

Com advento da internet e das inúmeras tecnologias baseadas na rede mundial de computadores, a sociedade experimentou avanços e experiências sem precedentes, notadamente com a ruptura dos limites concretos das comunicações e do exponencial desenvolvimento de sistemas informáticos que guardam inúmeras informações de impossível armazenamento num espaço físico. Qual tem demonstrado a experiência teórica e prática, tais avanços não se limitam à facilitação da vida cotidiana, mas resultam numa vasta gama de questões, crises e casos que clamam à disciplina e solução do Direito, embora desafiem sua capacidade de transformação.

É no âmbito de tão instigante debate que se insere este artigo, o qual analisa, especialmente no âmbito do processo penal, a (i)licitude da prova coletada a partir da apreensão, intercepção e quebra de sigilo de dados pessoais armazenados em dispositivos informáticos, especialmente os móveis, a exemplo de smartphones e congêneres.

A relevância do tema decorre da própria popularização de tais tecnologias, de uso corrente e comezinho do cidadão médio, bem como da crescente relevância das provas digitais – o que corresponde à necessidade de incremento de seu controle.

Assim é que inicialmente o trabalho analisa o conceito de prova ilícita e a garantia de sua inadmissibilidade por imposição constitucional, delimitando também o seu âmbito de proteção e correlação com outros direitos também fundamentais. Após, explorou-se, especificamente, o núcleo conceitual da garantia de inviolabilidade da intimidade e da vida privada (art. 5º, X, CFRB), bem como da inviolabilidade das comunicações – talhando, quanto a esta última, a diferença entre a proteção das comunicações em si da tutela dos dados de comunicações.

Em seguida, com suporte na Lei nº 13.709/2018, novel lei nacional de proteção dos dados pessoais, bem como na experiência internacional sobre o tema – notadamente os regulamentos da União Europeia sobre o mesmo tema –, explorou-se os conceitos e caracteres de dados pessoais e seu tratamento. Por fim, tratou-se do controle judicial da prova produzida a par da devassa de dispositivos eletrônicos e/ou decorrente da interceptação de dados produzidos em programas informáticos, demonstrando a necessidade de autorização prévia sob pena de sua total inadmissibilidade, assim como demais provas que dela decorram.

Para alcançar os resultados almejados foi utilizado o método dedutivo, com base em análise de legislação, doutrina e jurisprudência; partindo de premissas genéricas, desde a

conceituação de dados informáticos, inadmissibilidade da prova ilícita e garantia da privacidade digital, para desaguar em premissas específicas, notadamente no que tange ao controle da prova digital no âmbito do processo penal, as quais encaminharam às conclusões da pesquisa.

2 DA PROVA ILÍCITA E SUA INADMISSIBILIDADE

Fruto de longa maturação da história do constitucionalismo moderno, a vedação ao uso da prova ilícita para fins processuais encontra assento expresso na Constituição da República, cujo art. 5º, LVI expressamente impõe que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos".

A ilicitude da prova, em especial sob escopo do processo penal, pode decorrer de três ordens: porque contrária a um juízo abstrato de moralidade ou de impossível produção; porque carente de previsão legal (*in lato sensu*) e incompatível com os princípios do processo moderno; ou porque seu meio de produção é simplesmente ilícito, sendo a ilicitude transmitida por derivação.

Como é de suceder com o rigor da conceituação jurídica, a definição de prova ilícita não se confunde com o de prova *ilegítima*, malgrado ambas compartilhem o traço de serem, topologicamente, espécies do gênero maior de prova *ilegal*. Nessa ordem, tomando a prova ilegal como a obtida com violação de normas legais ou de princípios gerais do ordenamento, resta que "[...] quando a proibição for colocada por uma lei processual, a prova será *ilegítima* (ou ilegitimamente produzida); quando, pelo contrário, a proibição for de natureza material, a prova será *ilicitamente* obtida" (Grinover et al, 1995, p. 115).

No entanto, em que pese a diferenciação, o teor do texto constitucional deixa claro que o tratamento jurídico conferido às provas ilícitas e às provas ilegítimas é uno, a saber: são indistintamente inadmissíveis. Referida disciplina segue tendência do direito comparado quanto à tutela dos direitos e garantias individuais no processo – em toada análoga é, por exemplo, o art. 32 da Constituição da República Portuguesa, cujo art. 32, 8 expressamente estatui que "são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade

física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações" [3].

De todo modo, a inadmissibilidade é reforçada com maior enlevo pelo legislador infraconstitucional, na medida em que o art. 156 do Código de Processo Penal reputa inadmissíveis tanto as provas ilícitas – "assim entendidas as obtidas em violação a normas constitucionais ou legais" –, bem como as que daquelas derivem, "salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras" (§ 1º).

Vê-se, portanto, que a vedação do emprego da prova ilícita no processo penal é categoricamente restritiva, não se admitindo sequer seu ingresso nos autos processuais. Como explica Vicente Greco Filho (2012, p. 285):

> O art. 5º, LVI, da Constituição da República considera inadmissíveis os meios de prova obtidos por meio ilícito. Tal disposição é resultante da opção do texto constitucional pela corrente mais rigorosa a respeito da ilicitude do meio de prova, em virtude da ilicitude da origem ou da obtenção. Outras correntes doutrinárias e jurisprudenciais admitiam a produção da prova obtida nessas condições ou a admitiam em termos, somente na hipótese de o bem jurídico alcançado com a prova ser de maior valor que o bem jurídico sacrificado pela ilicitude da obtenção. Esta última posição era a acolhida pelas decisões judiciais, inclusive do Supremo Tribunal Federal, que sempre fazia uma análise do peso dos valores jurídicos envolvidos. O texto constitucional parece, contudo, jamais admitir qualquer prova cuja obtenção tenha sido ilícita.

A garantia inadmissibilidade da prova ilícita representa autêntica limitação dos poderes instrutórios do juiz – os quais, mesmo no processo penal, no qual são sabidamente mais amplos do que na esfera civil. Aliás, não somente a atividade jurisdicional, mas sobretudo todo o aparato do estado está talhado por níveis de limitação de seu poder soberano – os quais são também de ordem processual, como bem observa Luís Roberto Barroso (2015, p. 29/30):

> Em um Estado constitucional existem três ordens de limitação do poder. Em primeiro lugar, as limitações *materiais*: há valores básicos e direitos fundamentais que hão de ser sempre preservados, como a dignidade da pessoa humana, a justiça, a solidariedade e os direitos à liberdade de religião, de expressão, de associação. Em segundo lugar, há uma específica estrutura orgânica *exigível*: as funções de legislar, administrar e julgar devem ser atribuídas a órgãos distintos e independentes, mas

[3] No entanto, a Carta nacional é ainda mais firme do que sua equivalente lusa: ao impor a nulidade da prova ilícita, o constituinte português condiciona que a prova nula seja assim declarada pelo juiz; ao contrário, o constituinte brasileiro optou por sequer admitir o ingresso da prova no processo, sob pena de seu desentranhamento.

> que, ao mesmo tempo, se controlem reciprocamente (*checks and balances*). Por fim, há as limitações *processuais*: os órgãos do poder devem agir não apenas com fundamento na lei, mas também observando o devido processo legal, que congrega regras tanto de caráter procedimental (contraditório, ampla defesa, inviolabilidade do domicílio, vedação de provas obtidas por meios ilícitos) como de natureza substantiva (racionalidade, razoabilidade-proporcionalidade, inteligibilidade).

Portanto, não se cogita de condenação ou restrição a direito que, em processo judicial, decorram baseadas de provas ilícitas; as quais, porque produto da inevitável transgressão do ordenamento positivo, são juridicamente ineficazes.

2.1 O ÂMBITO DE PROTEÇÃO DA INADMISSIBILIDADE DA PROVA ILÍCITA

A garantia (evidentemente fundamental) de inadmissibilidade da prova ilícita se conecta logicamente a outros direitos e garantias fundamentais, a exemplo dos direitos à intimidade e à privacidade (art. 5º, X, CRFB), à inviolabilidade do domicílio (art. 5º, XI) e ao sigilo profissional e de fonte (CF, art. 5º, XIII e XIV), bem como ao sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII) – todos devidamente protegidos pela característica de intangibilidade legislativa (art. 60, § 4º) [4].

No entanto, dado que as liberdades públicas não podem ser tidas por absolutas, é sabidamente admitida a restrição à inviolabilidade dos direitos e garantias individuais para fins de produção de prova, especificamente quando a mesma preceder de adequada determinação judicial motivada e observar a forma prescrita em lei.

Constata-se, assim, o necessário controle judicial da prova, na medida em que o magistrado, presidente da instrução penal, é quem detém a reserva para autorizar a produção probatória pretendida pelas partes – e, mesmo no inquérito, sabe-se exercer autêntica função de controle, ainda que à míngua de contraditório. No entanto, em ruptura ao modelo processual penal anterior, de matriz inquisitorial, a ordem constitucional vigente e seu sistema de garantias individuais não mais admite ao juiz assumir a iniciativa acusatória, sobretudo pela via de ordenação de provas de ofício [5].

[4] Outrossim, é por decorrência natural que a obtenção de prova sem observância das normas do ordenamento positivo deságua em ofensa ao princípio do devido processo legal e à básica garantia de não autoincriminação, os quais, além de previsão normativa expressa (art. 5º, LXIII, CFRB e art. 186, parágrafo único, CPP), gozam também de proteção internacional, a par dos arts. 14, 3, g do Pacto Internacional sobre Direitos Civis e Políticos (Decreto nº 592/1992) e 8º, 2, g da Convenção Americana sobre Direitos Humanos (Decreto nº 678/1992).

[5] Faculdade ainda (e infelizmente) prevista, dentre outros, no art. 156, I do vigente CPP, mas que se revela eivada de clara inconstitucionalidade.

Daí que a cláusula de reserva jurisdicional na produção da prova é especialmente talhada para o controle das restrições às inviolabilidades e não para os interesses da investigação e do processo criminal; sempre na assunção, pelo juiz, de postura imparcial, naturalmente exigível a par da paridade de armas, do contraditório e da ampla defesa. É o que demonstra Eugênio Pacelli (2013, p. 334/335), que tratando especificamente da investigação assim leciona:

> O juiz, quando defere uma prisão cautelar, quando defere uma intercepção telefônica ou a quebra de uma inviolabilidade pessoal, não está, nem nesse momento, protegendo os interesses da investigação criminal. Na verdade, como garantidor que é das liberdades públicas, ele estará exercendo o controle constitucional das restrições às inviolabilidades, nos limites da Constituição da República e do devido processo legal. É por isso que se instituem as chamadas cláusulas da reserva da jurisdição, segundo as quais somente ao juiz se defere o tangenciamento de direitos e garantias individuais, como ocorre, por exemplo, em relação à inviolabilidade do domicílio (mandado de busca e apreensão), da liberdade individual (prisão cautelar), do direito à intimidade e à privacidade (interceptação telefônica e ambiental, etc.).

Como dito, várias são as feições de direitos fundamentais que convergem à inadmissibilidade da prova ilícita; no entanto, para os fins deste estudo convém concentrar em duas categorias explícitas que especialmente tocam no objeto dissertado: a inviolabilidade da intimidade e da vida privada (art. 5º, X) e a inviolabilidade das comunicações telegráficas, telefônicas e de dados (art. 5º, XII).

2.1.1 Da inviolabilidade da intimidade e da vida privada

Ao garantir que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (art. 5º, X) a Constituição da República conferiu elevada proteção a elementos que, embora devam ser conceituados separadamente, relacionam-se em conexão descendente.

Assim explica Lucrecio Rebollo Delgado (2000, p. 54):

> O conceito de vida privada é muito amplo, genérico e engloba tudo aquilo que não é ou não queremos que seja de conhecimento geral. Dentro dele, existe um núcleo que protegemos com mais zelo, com maior força porque o entendemos como essencial na configuração de nossa pessoa. A este último denominamos Intimidade. [...] A vida privada é o genericamente reservado, sendo a Intimidade o radicalmente vedado e o mais pessoal (tradução livre).

Sem embargo de tal distinção conceitual, é certo que privacidade e intimidade são atributos que se confundem, sobremaneira "agravado" ao fato de que, além da lei civil não

estabelecer qualquer distinção entre si [6], a Constituição lhes defere a mesma proteção e sentido. Assim é que, em termos de praticidade, convém seja adotado a locução *direito à privacidade*, em sentido amplo, que assim "[...] abarca todas as manifestações da esfera íntima, privada e da personalidade que o art. 5º, inc. X da Constituição Federal consagrou: direito à intimidade, à vida privada, à honra e à imagem das pessoas" (TEIXEIRA, 2014, p. 71).

É patente – pelo espírito destes novos tempos – que o direito à privacidade encontra hoje relevante (senão a mais relevante) acepção em termos de sua expressão e gozo no meio ambiente virtual. Não por menos, o Marco Civil da Internet (Lei nº 12.965/2014) expressamente contempla sua proteção como princípio da disciplina do uso da internet no País (art. 3º, II), condicionando que "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet" (art. 8º).

A preocupação do legislador tem razão de ser. Com efeito "com a alta capacidade de sistemas e dispositivos informáticos de processarem e registrarem conexões e acessos, há um grave risco para a privacidade, a intimidade, a honra e a imagem das pessoas" (GONÇALVES, 2017, p. 66).

Vê-se, portanto, que a proteção constitucional do direito à privacidade encontra contemporaneamente um novo horizonte a desafiar sua aplicabilidade, isto é, a internet, que fez nascer uma nova dimensão para exercício, bem como para violação, desta e demais liberdades públicas contempladas na Carta de 1988. É o que adverte Tarcísio Teixeira (2014, p. 75):

> [...] Com a chegada da internet, a privacidade pode ter encontrado uma grande vilã nessa avançada rede de comunicação. Acontece que, na internet, a privacidade por ser violada com facilidade em decorrência da indiscriminada captação de dados, muitos comercializados a partir da formação de perfis dos usuários, abrindo possibilidades de envio de inúmeras mensagens não solicitadas, sem levar em conta outras questões jurídicas relacionadas e os prejuízos causados aos usuários, pessoas físicas ou jurídicas.

Como sucede com as demais liberdades individuais, o direito à privacidade não ostenta força absoluta em qualquer caso, mas cede sua esfera de proteção quando confrontado com ordem judicial que determine sua "devassa autorizada" para fins de produção probatória

[6] O Código Civil Brasileiro confunde ambos os conceitos e só trata expressamente de um deles, a "vida privada", como bem demonstra seu art. 21: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

– sobretudo em processo penal, cuja instrução hoje também abarca meios de prova outrora desconhecidos, a exemplo dos dados armazenados em smartphones, computadores e outros dispositivos eletrônicos que permitem a imediata comunicação.

Neste particular é que tal garantia se conecta umbilicalmente ao sigilo da correspondência e das comunicações, eis que, como delimita Tercio Sampaio Ferraz (1999, p. 447), "[...] o direito à privacidade não é propriamente um gênero *do*, mas tem a ver *com* o direito à inviolabilidade do domicílio (estar-só), da correspondência (segredo), etc.". Tal demarcação, entre objeto do direito e faculdade de agir, é assim detalhada pelo autor (idem):

> [...] Pontes de Miranda (p. 360) vê na inviolabilidade da correspondência e do segredo profissional um direito fundamental de 'negação", um a liberdade de "negação": liberdade de não emitir pensamento exceto para u m número reduzido (segredo da correspondência circular, dos avisos reservados aos empregados, etc.) ou exceto para u m (cartas particulares). Com o direito subjetivo fundamental aqui também há de se distinguir entre o objeto e o conteúdo. O objeto, o bem protegido, é, no dizer de Pontes, a liberdade de 'negação' de comunicação do pensamento. O conteúdo, a faculdade específica atribuída ao sujeito, é a faculdade de resistir ao devassamento, isto é, de manter o sigilo (da informação materializada na correspondência, na telegrafia, na comunicação de dados, na telefonia). A distinção é importante. Sigilo não é o bem protegido, não é o objeto do direito fundamental. Diz respeito à faculdade de agir (manter sigilo, resistir ao devassamento), conteúdo estrutural do direito.

Dada tal conexão é que é imperativo tratar das comunicações e dados cuja inviolabilidade é também tutelada pelo texto constitucional, como faz a seguir.

2.1.2 Da inviolabilidade das comunicações telegráficas, telefônicas e de dados

O art. 5º, XII da Constituição Federal é expresso tanto na proteção, quanto na possibilidade de mitigação da inviolabilidade de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas.

Especificamente quanto ao sigilo das comunicações telefônicas, o constituinte foi expresso (art. 5º, XII, *in fine*) ao admitir sua mitigação com objetivo de prova em processo penal, conquanto seja realizada na forma da lei própria (no caso, a Lei nº 9.296/1996, editada sob *interpositivo legislatoris*) e autorizada, justificadamente, pelo Poder Judiciário.

Com efeito, como em todos os demais casos de restrição autorizada ao sigilo, a forma prescrita em lei e o controle jurisdicional são indispensáveis à liceidade e eficácia da prova resultante da devassa (v.g., escuta). Qual explica Manoel Gonçalves Ferreira Filho (2012, p. 227) a inviolabilidade constitucional

> Abre, todavia, exceção quanto às comunicações telefônicas. Estas podem sofrer restrição em sua inviolabilidade com objetivos de investigação criminal ou instrução processual penal. A restrição tem sido defendida pela doutrina e adotada em alguns sistemas jurídicos em face dos crimes de sequestro e de narcotráfico, em especial, cuja investigação não pode desprezar a escuta telefônica, muitas vezes único meio para a solução de tais crimes. Ainda assim a escuta somente poderá realizar-se por ordem judicial, nas hipóteses e na forma previstas em lei. A regra, portanto, continua sendo a inviolabilidade das comunicações por quaisquer meios. Isto se reforça pela disposição constitucional que proíbe apresentação de 'provas obtidas por meios ilícitos" (art. 5º, LVI)'.

Sem embargo, deve ficar claro que a restrição da inviolabilidade sob autorização do Judiciário não está adstrita às comunicações telefônicas; mas, além de se estender também ao sigilo de correspondência e às comunicações telegráficas, pode-se se cogitar que alcance ainda outros veículos e formas de interação linguística não expressamente positivados. Assim o conclui Paulo Gustavo Gonet Branco (2012, p. 382):

> A leitura do preceito pode levar à conclusão de que apenas nos casos de comunicações telefônicas seria possível que o Poder Público quebrasse o sigilo e que seria impossível abrir ao seu conhecimento os dados constantes de correspondência postal, telegráfica ou de comunicações telemáticas. Sabe-se, porém, que A restrição de direitos fundamentais pode ocorrer mesmo sem autorização expressa do constituinte, sempre que se fizer necessária a concretização do princípio da concordância prática entre ditames constitucionais. Não havendo direitos absolutos, também o sigilo de correspondência e o de comunicações telegráficas são passíveis de ser restringidos em casos recomendados pelo princípio da proporcionalidade.

Não há como desprezar o avanço tecnológico experimentado desde o advento da Lei Maior, sentido em especial com o desenvolvimento de novos meios e formas de comunicação entre particulares, sobremaneira incentivado com a expansão do uso da internet e dos sistemas cujo funcionamento baseia ou decorre da própria rede. Daí advém as recentes discussões quanto à interceptação e/ou invasão a sistemas de troca de mensagens simultâneas entre usuários, como fóruns de bate-papo, aplicativos de mensagens e aplicações congêneres.

Tal como a tecnologia de comunicações desenvolve progressivamente, assim também floresceram, todavia em ritmo menor, as ferramentas de investigação e prova em processo penal. A esse título se pode destacar, dentre outros, os novos métodos de *ação controlada* sobre aplicações baseadas na internet, a exemplo da vigilância cibernética em tempo real de mensagens trocadas e postadas em fóruns de debate dedicados a objetivos

criminosos (v.g., redes de pedofilia baseadas na "Deep Web" [7]) ou mesmo a infiltração de agentes da persecução penal em comunidades virtuais dedicadas a intentos ilícitos, mediante técnicas de engenharia social [8] e com apoio de softwares especialmente desenvolvidos para a investigação policial (v.g., *Child Protection System*).

No entanto, como é avaliado adiante, em que pese admitida a restrição do direito fundamental à inviolabilidade das comunicações, a garantia de sigilo a que a alude o art. 5º, XII da Constituição Federal alcança apenas as comunicações de dados, mas não os dados em si mesmos.

3 QUALIFICAÇÃO E INVIOLABILIDADE DOS DADOS PESSOAIS

Antes de ingressar na análise da proteção jurídica dos dados pessoais, convém sejam delimitados os contornos do que se pode convencionar de um conceito normativo de tais informações, à luz da legislação nacional e da experiência internacional sobre o tema.

3.1 CONCEITO NORMATIVO DE DADOS INFORMÁTICOS PESSOAIS

Exemplo típico da conduta do legislador negativo, até há pouco o Ordenamento brasileiro não contava com disciplina legal expressa a respeito dos dados informáticos pessoais, legando aos Tribunais e à literatura jurídica a tarefa de perquirir seu conteúdo normativo e possível proteção.

Para sanar tal deficiência é que adveio a Lei nº 13.709/2018, alcunhada Lei Geral de Proteção de Dados Pessoais, a finalmente dispor sobre o tratamento de dados pessoais, inclusive nos meios digitais – o tema de vital pertinência não só porque curial à competitividade comercial do País, mas também por conferir balizamentos objetivos ao exercício da liberdade e privacidade no ambiente informático [9].

O art. 5º da novel lei introduz um conceito geral de *dado pessoal* (inciso I) – assim entendido como "informação relacionada à pessoa natural identificada ou identificável" - bem

[7] Conceito dado às partes da rede mundial de computadores cujo conteúdo não está indexado por motores de busca/buscadores (v.g., Google, Bing e afins).
[8] Habilidade de manipular pessoas para pessoas para obter informações necessárias.
[9] Note-se que o Brasil já contava com normas e regulamentos setoriais que disciplinam direta ou indiretamente a exploração e proteção dos dados pessoais; todavia, carecia de uma lei geral que conferisse alguma ordem metodológica a tal arcabouço normativo.

como, em específico, duas espécies subjacentes: os *dados sensíveis* (inciso II) e os *dados anonimizados* (inciso III). Veja-se:

> Art. 5º Para os fins desta Lei, considera-se:
> I – dado pessoal: informação relacionada à pessoa natural identificada ou identificável;
> II – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural;
> III – dados anonimizados: dados pessoais relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Note-se que a lei expressamente excepciona sua disciplina quanto ao tratamento de dados pessoais "realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais" (art. 4º, III). Sem embargo, considerando que o legislador, *ipsis litteris*, excepcionou da esfera penal apenas o que tange ao tratamento dos dados, é de se concluir que as definições legais acima referidas podem sim ser aproveitadas para a discussão penal.

Sem prejuízo deste conceito legislativo, é oportuno colacionar a definição adotada pelo *General Data Protection Regulation* (GDPR) – o festejado regulamento da União Europeia que introduziu inúmeras provisões relativas à privacidade e proteção de dados sobre o território da comunidade e do Espaço Econômico Europeu – cujo art. 4º, I adota o seguinte conceito de dado pessoal e seu titular:

> *For the purposes of this Regulation:*
> *(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* [10];

É de justificar a pertinência do conceito alienígena à notória complexidade de sua construção (em comparação ao menos com a Lei nº 13.709/18); o que pode ser creditado, dentre outros, à reconhecida experiência legislativa da UE a respeito do tema, notadamente

[10] "Para efeitos deste Regulamento: (1) 'dado pessoal' significa qualquer informação relativa uma pessoa natural identificada ou identificável ('titular de dados'); uma pessoa identificável é uma pessoa natural que pode ser identificada, direta ou indiretamente, em especial por referência a um identificador como um nome, um número de identificação, dado de localização, um identificador online ou por um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social desta pessoa natural" (tradução livre).

desde a Diretiva 95/46/EC, que aplicava ao bloco europeu orientações relativas à proteção individual em termos de processamento de dados pessoais.

3.2 A INVIOLABILIDADE DOS DADOS PESSOAIS X INVIOLABILIDADE DAS COMUNICAÇÕES DE DADOS

É preciso demarcar a diferença entre *comunicações de dados* – expressamente protegidas pelo sigilo constitucional do art. 5º, XII – dos *dados informáticos* em si.

Como adiantado no item anterior, dado se refere a toda informação processada ou armazenada por um computador e expressada na forma de documentos de texto, clipes de áudio, programas de software e congêneres, guardados em arquivos/ficheiros e pastas contidos em seu disco rígido (hard disk - HD).

Com rigor técnico, Ralph M. Stair e George W. Reynolds (2010, p. 05/06) assim constroem a relação entre dados e informação:

> *Data consists of raw facts, such as an employee number, total hours worked in a week, inventory part numbers, or sales orders. [...] When facts are arranged in a meaningful manner, they become information. Information is a collection of facts organized so that they have additional value beyond the value of the individual facts. [...] Turning data into information is a process, or a set of logically related tasks performed to achieve a defined outcome. The process of defining relationships among data to create useful information requires knowledge. Knowledge is the awareness and understanding of a set of information and the ways that information can be made useful to support a specific task or reach a decision* [11].

Isto compreendido, qual seria, então, o conteúdo normativo da expressão *comunicações de dados* expressa pela Lei Maior? O Supremo Tribunal Federal já teve múltiplas ocasiões de pesar a matéria, tendo firmado entendimento, desde o julgamento do Recurso Extraordinário nº 418.416/SC, sob relatoria do então Ministro Sepúlveda Pertence, que "[...] a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador" (STF, 2006, on-line).

[11] "Dados consistem em fatos brutos, como um número de funcionário, o total de horas trabalhadas em uma semana, números de peça num estoque ou pedidos de vendas. [...] Quando os fatos são organizados de maneira significativa, eles se tornam informações. Informação é uma coleção de fatos organizados para que eles tenham valor adicional além do valor dos fatos individuais. [...] Transformar dados em informação é um processo, ou um conjunto de tarefas logicamente relacionadas executadas para alcançar um resultado definido. O processo de definir relacionamentos entre dados para criar informações úteis requer conhecimento. Conhecimento é a conscientização e compreensão de um conjunto de informações e as maneiras pelas quais as informações podem ser úteis para apoiar uma tarefa específica ou chegar a uma decisão" (tradução livre).

Exemplo didático deste posicionamento da Corte foi o verificado por ocasião do Habeas Corpus nº 91.867, sob relatoria do Ministro Gilmar Mendes, de cuja ementa se extrai o seguinte aresto de interesse (STF, 2012, on-line):

> 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. Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do art. 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.

Resta, portanto, que, conforme jurisprudência vigente do Supremo Tribunal Federal, "a utilização de dados constantes de computador não configura violação ao disposto no art. 5º, XII, no que concerne à proteção de comunicação de dados, desde que a apreensão se faça com base em ordem judicial adequada" (MENDES et al, 2014, p. 384).

Assim, os *dados estáticos*, armazenados em computador ou dispositivo congênere que não sejam objeto de apreensão, interceptação ou monitoramento em troca de mensagens, ou outra forma instantânea de comunicação entre usuários em tempo real, não goza da proteção fundamental da inviolabilidade das comunicações. No entanto, isto não quer dizer que os *dados de computador*, sobretudo os *dados pessoais*, sejam carentes da tutela da Constituição.

Com efeito, o fundamento de tal proteção só será objeto de mera mudança topológica no rol de direitos fundamentais: ao invés de tutelados à luz do art. 5º, XII, os *dados pessoais* acham-se expressamente albergados sob a proteção do direito à privacidade (*lato sensu*) igualmente positivado pelo Constituinte de 1988, com traço de fundamentalidade, no art. 5º, X de nossa Lei Maior.

Acresce-se, ainda, à salvaguarda constitucional, a disciplina normativa do Marco Civil da Internet, que, além de consagrar a proteção dos dados pessoais como princípio norteador do uso da rede (art. 3º, III), também reconhece aos usuários brasileiros vasta gama de direitos sobre seus dados pessoais, dentre os quais a inviolabilidade e sigilo do fluxo tanto de suas comunicações pela internet (art. 7º, II), quanto de suas comunicações privadas armazenadas (inciso III).

Resta, destarte, que os dados pessoais, assim como as comunicações de dados, não se acham disponíveis à livre devassa; forçando-se, como sucede com estes, que sua apropriação

para fins probatórios em processo penal seja precedida de obrigatória, e motivada, autorização judicial, sob pena de inadmissibilidade da prova que a partir deles se pretendia constituir.

É dizer: não se pode admitir que os dados pessoais restassem carentes de qualquer tutela, eis que sua criação e utilização é parte indelével da vivência humana. Nesse sentido é a lição de José Afonso da Silva (2011, p. 208):

> A tutela constitucional visa proteger as pessoas de dois atentados particulares: (a) ao *segredo da via privada*; e (b) à *liberdade da vida privada*. O segredo da vida privada é condição de expansão da personalidade. Para tanto, é indispensável que a pessoa tenha ampla liberdade de realizar sua vida privada, sem perturbação de terceiros. São duas variedades principais de atentados ao *segredo da vida privada*, nota Kayser: a *divulgação*, ou seja, o fato de levar ao conhecimento do público, ou a pelo menos de um número indeterminado de pessoas, os eventos relevantes da via pessoal e familiar; a *investigação*, isto é, a pesquisa de acontecimentos referentes à vida pessoal e familiar; envolve-se aí também a proteção contra a conservação de documento relativo à pessoa, quanto tenha sido obtido por meios ilícitos. O autor ressalta o fato hoje notório que o segredo da via privada é cada vez mais ameaçado por investigações e divulgações ilegítimas por aparelhos registradores de imagem, sons e dados, infinitamente sensíveis aos olhos e ouvidos.

No entanto, a mera autorização judicial não pode ser encarada como chancela automática à liceidade, afastadora de qualquer inadmissibilidade quanto ao emprego de provas digitais. É que o magistrado, além de seu inafastável dever jurídico de motivação – perquirindo quanto à pertinência e eficácia da devassa –, deve proceder também a um juízo de ponderação ("Abwàgung"), isto é, uma avaliação ponderada dos fins antes de ceder à simples pressão do órgão acusador.

4 O CONTROLE JUDICIAL DA PROVA ELETRÔNICA RESULTANTE DA CAPTAÇÃO DE DADOS PESSOAIS

Falando sob o prisma processual penal, José Maria Asencio Mellado (2008, p. 01) conceitua a prova como simplesmente "[...] *aquella actividad de carácter procesal cuya finalidade consiste em lograr la convicción del Juez o Tribunal acerca de la exactitud de las afirmaciones de hecho operadas por las partes em el processo*" [12]. A projeção concreta desta atividade são os *meios de prova*, assim entendidos como "[...] os recursos diretos ou indiretos para alcançar a verdade no processo, ou seja, são os métodos pelos quais as informações sobre os fatos (provas) são introduzidas no processo" (SILVA, 2010, p. 08).

[12] "[...] aquela atividade de natureza processual cuja finalidade consiste em obter a convicção do Juiz ou do Tribunal sobre a exatidão das afirmações de fato operadas pelas partes no processo" (tradução livre).

Como sucede em qualquer esfera processual, o documento – assim entendido como a representação material de um fato – é o meio de prova que, objetivamente, ostenta maior eficácia para fins de convencimento; no entanto, sua manifestação concreta não está limitada à uma projeção física propriamente dita, podendo se cogitar de documento e, pois, prova eletrônica.

Qual observa Tarcísio Teixeira (2014, p. 143), "a cada dia diminui o receio em se admitirem como prova documentos eletrônicos, haja vista sua segurança [...] isso em razão de sua ampla utilização, da legislação e da posição favorável dos tribunais".

Assim também Patrícia Peck Pinheiro (2010, p. 213):

> [...] a documentação em papel está em fase de transição, passando a ser eletrônica, relevante para a produção de provas em Direito. Aos poucos, evoluímos de um suporte limitado, com baixa tecnologia de segurança, para um ambiente independente de suporte, em que é possível replicar originais eletrônicos e de valor original e não de cópia. É de se saber que tudo em meio eletrônico deixa rastro [...].

A própria lei não cria óbice à utilização da prova eletrônica (notadamente documental). Nesse sentido é a Lei nº 11.419/2006, que trata da informatização do processo judicial e cujo art. 11 expressamente reputa como originais, para todos os efeitos legais, "os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário".

O mesmo sucede com a lei processual penal: a par de interpretação conjunta dos arts. 231 e ss. do Código de Processo Penal, vê-se que o legislador preferiu consagrar, quanto à prova documental, fórmula aberta que considera documentos "quaisquer escritos, instrumentos ou papéis, públicos ou particulares" (art. 233); ainda consignando que "à fotografia do documento, devidamente autenticada, se dará o mesmo valor do original" (parágrafo único).

Todavia, tal flexibilização em termos de produção probatória (própria do processo penal e de sua busca pela "verdade real") está limitada por juízos de moralidade, bem como pela defesa da dignidade humana.

Assim é que os dados pessoais de um dado usuário – guardados em dispositivos computacionais caracterizáveis como meio material de prova – podem seguramente ser objeto de intervenção, captura e armazenamento pela autoridade policial para fins probatórios em processo penal. Todavia, estando tais dados incluídos no âmbito de proteção do direito constitucional à privacidade e sua inviolabilidade, qualquer atividade da persecução nesse

sentido deve ser precedida de expresso requerimento/representação e autorização judicial, sob pena de serem consideradas ilícitas todas as provas eventualmente obtidas.

A questão é sobretudo relevante do ponto de vista dos dispositivos móveis, especialmente os aparelhos celulares, que a rigor são objeto de consumo indistinto do cidadão médio. Tais dispositivos armazenam em si múltiplas informações sensíveis de seu titular, como arquivos de fotos, vídeos, clipes de áudio, mensagens, contatos e afins, cujo acesso incontrolado pode representar lesão não apenas à sua privacidade digital, mas também à sua vida íntima e honra pessoal (a depender do conteúdo do arquivo devassado).

Tais dispositivos, sobretudo os smartphones [13], gozam hodiernamente de popularidade tal que não se cogita ao cidadão moderno prescindir de seu uso no dia-a-dia. Essa relação de dependência se afigura tão aguda que no recente julgamento do caso *Timothy Ivory Carpenter v. United States*, a Suprema Corte dos Estados Unidos qualificou tais dispositivos como praticamente "parte da anatomia humana" (USSC, 2018, on-line).

A Corte ainda teve ocasião de traçar o seguinte paralelo entre as múltiplas funções dos smartphones e a possibilidade de que, com elas, seja possível o rastreamento do usuário com precisão próxima a de uma "tornozeleira eletrônica" (idem):

> *[...] While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. [...] Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user. Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable* [14].

Além de permitir o efetivo rastreamento de um dado indivíduo, as próprias funções de um aparelho celular – externadas através de aplicativos móveis (apps), isto é, softwares desenvolvidos para execução em dispositivos *mobile* – invariavelmente envolvem a coleta de dados pessoais do próprio usuário (frequentemente sem o consentimento informado deste),

[13] Nome dado ao aparelho celular com funções típicas de um computador, a rigor composto de tela com toque sensível, acesso a internet e sistema operacional capaz de executar simultaneamente aplicativos próprios.

[14] "Enquanto os indivíduos deixam seus carros regulamente, eles, de outro modo, carregam compulsivamente seus celulares consigo o tempo todo. Um telefone celular segue fielmente seu proprietário além das vias públicas e em residências particulares, consultórios médicos, sedes políticas e outros locais potencialmente reveladores. [...] Assim, quando o governo rastreia a localização de um celular, ele consegue uma vigilância quase perfeita, como se tivesse fixado uma tornozeleira eletrônica no usuário do telefone. Além disso, a qualidade retrospectiva dos dados dá à polícia acesso a uma categoria de informação que de outra forma seria desconhecida" (tradução livre).

com finalidade de personalizar seu funcionamento ou simplesmente traçar padrões de consumo para exploração mercantil.

Esse é o quadro exposto no relatório "*The OECD Privacy Framework*" da Organização para a Cooperação e Desenvolvimento Econômico (2013, p. 82):

> *More recently, mobile computing devices – including "smart" phones – have emerged. Powerful but portable, these devices are a transformative technology, combining geolocational data and Internet connectivity to support a broad new range of services and applications, many of which rely on (or involve) the collection and use of personal information to generate revenue. The mobile market has skyrocketed, with the total number of mobile subscriptions in OECD countries at 1.14 billion in 2007. Game consoles and portable gaming devices are other, more recent ways of accessing the Internet that are becoming popular* [15].

Na esfera penal, a simples apreensão de um aparelho celular potencialmente confere à autoridade policial livre acesso a dados e informações de índole pessoal que permitem a clara incriminação de seu proprietário. A esse título se pode conjecturar de provas como a triangulação de sua rota ou a identificação de locais pelos quais tenha passado, via dados de GPS, a fim de determinar sua possível vinculação com o tempo e local do crime; bem como o acesso ao histórico de chamadas e/ou de mensagens (via torpedos ou aplicativos próprios como *Whatsapp* e *Telegram*) com outros integrantes de um dado grupo criminoso, daí concluindo pela sua integração à empreita ilícita.

Em tais cenários a interpretação mais consentânea com a tutela jurídica da privacidade é a seguinte: os agentes da persecução não podem prescindir de adequado requerimento/representação à autoridade judiciária antes de proceder à extração ou análise de dados do dispositivo (meio de prova material); cabendo-lhes, ao apreender determinado aparelho celular ou outro dispositivo informático, solicitar judicialmente a quebra do sigilo dos lá dados armazenados.

No entanto, considerando a plêiade de arquivos complexos que um mesmo dispositivo pode apresentar, a mesma garantia constitucional da intimidade e da vida privada – cuja natureza de direito fundamental não comporta interpretação restritiva – impõe que por

[15] "Mais recentemente, dispositivos de computação móvel - incluindo telefones "inteligentes" - surgiram. Poderosos, mas portáteis, esses dispositivos são uma tecnologia transformadora, combinando dados de geolocalização e conectividade com a internet para oferecer suporte a uma ampla gama de serviços e aplicativos, muitos dos quais dependem (ou envolvem) da coleta e uso de informações pessoais para gerar receita. O mercado móvel disparou, com o número total de assinaturas móveis nos países da OCDE em 1,14 bilhões em 2007. Consoles de videogame e dispositivos de jogos portáteis são outras formas mais recentes de acessar a Internet que estão se tornando populares" (tradução livre).

ocasião de requerimentos desta ordem sejam fixados os limites objetivos e subjetivos da quebra de sigilo, delimitando as espécies de arquivos que serão objeto da devassa, a finalidade e pertinência da quebra e os responsáveis que se encarregarão da diligência, inclusive peritos.

Tal exigência não constitui mero preciosismo, eis que em âmbito penal os mandados e diligências devem ser obrigatoriamente delimitados, não se tolerando mandados genéricos ou em branco, sob pena de exacerbação da autoridade e ilicitude da prova. Nesse sentido é a disciplina do Código de Processo Penal a respeito da busca e apreensão, cujo art. 243 obriga que o respectivo mandado indique com precisão o local em que se realizará o ato e o nome do respectivo proprietário ou morador; ou, no caso de busca pessoal, o nome da pessoa que terá de sofrê-la ou os sinais que a identifiquem, além do motivo e os fins da diligência.

Igual restrição se aplica às interceptações de comunicações telefônicas, cujo pedido, a par da Lei nº 9.296/1996, deve descrever com clareza a situação objeto da investigação, inclusive com a qualificação dos investigados (art. 2º, parágrafo único), bem como demonstrar que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados (art. 4º).

Isto posto, é natural que o tratamento restritivo conferido às buscas e apreensões e às interceptações telefônicas deve ser igualmente estendido à quebra de sigilo dos dados armazenados em dispositivos informáticos, assim como às conversas simultâneas entabuladas através de aplicativos de mensagens.

De há muito assim se posiciona, acertadamente, o Superior Tribunal de Justiça; tanto, que, a respeito dos dados armazenados em aplicativos de mensagens, firmou entendimento no seguinte sentido:

> [...] Os dados armazenados nos aparelhos celulares decorrentes de envio ou recebimento de dados via mensagens SMS, programas ou aplicativos de troca de mensagens (dentre eles o "WhatsApp"), ou mesmo por correio eletrônico, dizem respeito à intimidade e à vida privada do indivíduo, sendo, portanto, invioláveis, nos termos do art. 5°, X, da Constituição Federal. Assim, somente podem ser acessados e utilizados mediante prévia autorização judicial, nos termos do art. 3° da Lei n. 9.472/97 e do art. 7° da Lei n. 12.965/14 (STJ, 2018, on-line).
>
> [...] 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. Deste modo, ilícita é tanto a devassa de dados, como das conversas de whatsapp obtidos de celular apreendido, porquanto realizada sem ordem judicial (STJ, 2016, on-line).

Não há, portanto, como excluir dos dados pessoais a mesma proteção que se confere (em especial na esfera penal) contra a devassa da vida privada pelos meios típicos até então previstos pelo direito. Trata-se de conclusão inafastável, eis que, mesmo diante da escassa legislação a respeito do tema – vácuo progressivamente superado com o advento de estatutos como o Marco Civil da Internet e a Lei Geral de Proteção de Dados – os bens jurídicos e as liberdades individuais assumem novas feições à medida que se desenvolve tecnológica e socialmente a comunidade social. E sua salvaguarda deve ser naturalmente a mesma.

3 CONSIDERAÇÕES FINAIS

O avanço das tecnologias de informação força a adaptação de institutos jurídicos clássicos a uma nova realidade social que, além de provocar a sagacidade do legislador, desafiam sobretudo a atividade jurisdicional e os limites do silogismo jurídico. Com efeito, ao pretender a atividade de pacificação social no litígio, o juiz contemporâneo não pode mais se limitar a interpretar o Direito, mas é também compelido a interpretar as próprias circunstâncias dos casos concretos.

Tais questões se projetam com maior enlevo no âmbito da privacidade e da liberdade de comunicações, as quais, se de um lado enfrentam novas dimensões e facilidades, por outro são também mais facilmente violadas e aviltadas. É por essa que os dados informáticos, notadamente os de índole pessoal, converteram-se em autêntica *commodity* moderna, eis que através de sua interceptação, análise e manipulação é possível extrair desde padrões de consumo até arquétipos de comportamento (político, social, sexual e afins) de vastas legiões de usuários. Basta ver que temas outrora ignorados como *big data*, *fake news* e *bots* operadores em rede sociais ganharam espaço de destaque tanto no noticiário quanto no Judiciário.

Não se pode ignorar, porém, que afora tais questões correntes – da maior relevância, sem dúvida – as novas tecnologias digitais também merecem reflexão em termos de sua aplicabilidade para fins penais, sobretudo no que tange à produção da chamada prova eletrônica, cada vez mais explorada pelo aparato de persecução do estado. Com efeito, salvo pelo emprego de técnicas alheias ao usuário comum (v.g., navegação por software *Tor* ou via *Virtual Private Netword – VPN*), a utilização de aplicações em internet invariavelmente deixa traços de seu usuário, não se podendo cogitar de uma utilização absolutamente anônima. Por

essa precípua razão, a persecução penal lança mão de softwares e técnicas progressivamente mais complexas para, a partir dos dados coletados de um determinado usuário, contra ele produzir provas que podem ser futuramente aproveitadas em processo penal.

Como citado, pode-se conceber métodos de ação controlada sobre aplicações em internet – notadamente com a vigilância cibernética em redes sociais e fóruns de bate-papo – ou mesmo a simples apreensão de dispositivos informáticos, como computadores pessoais e aparelhos *mobile*; dos quais, após devida quebra, é possível extrair vasta gama de dados pessoais, potencialmente incriminadores num grau de precisão sem precedentes.

A questão é sensível sobretudo do ponto de vista dos aparelhos celulares e *smartphones*, que, tratando-se de objetos de consumo comum, são invariavelmente portados pela massiva maioria da população. Ora, ao apreender um dado aparelho celular, a autoridade policial pode ter livre acesso a dados e informações que permitem a incriminação de seu proprietário, como por exemplo: a triangulação de sua rota ou a identificação de locais pelos quais tenha passado via dados de GPS; acesso ao histórico de chamadas e/ou de mensagens; fotos e vídeos com produtos e objetos do crime, dentre outros.

Tais facilidades devem ser evidentemente analisadas à luz dos direitos fundamentais do processo e das demais liberdade públicas consagradas na Constituição, em especial a vedação do emprego de provas ilícitas. Assim é que se defendeu a imperiosa extensão das garantias processuais ao presente estado de vivência tecnológica, de tal maneira que não se prescindirá do necessário controle judicial da prova eletrônica – provocado, prévio e motivado –, sem o qual esta se inquinará de automática inadmissibilidade.

REFERÊNCIAS

BADARÓ, Gustavo Henrique Righi Ivahy. Ônus da prova no processo penal. São Paulo: Revista dos Tribunais, 2003.

BARRO, Luís Roberto. Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo. 5 ed. São Paulo: Saraiva, 2015.

DELGADO, Lucrecio Rebollo. El derecho fundamental a la Intimidad. Madrid: Dykinson, 2000.

FERRAZ JUNIOR, Tércio Sampaio Ferraz. 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. 447, 1993.

FERREIRA FILHO, Manoel Gonçalves. Curso de Direito Constitucional. 38ª Ed. rev. e atual.. São Paulo: Saraiva, 2012.

GONÇALVES, Victor Hugo Pereira. Marco civil da internet comentado. São Paulo: Atlas, 2017.

GRECO FILHO, Vicente. Manual de Processo Penal. 9ª Ed.. São Paulo: Saraiva, 2012.

GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães. As Nulidades no Processo Penal. São Paulo: RT, 1995.

MELLADO, José Maria Asencio. La prueba prohibida y prueba preconstituida en el proceso penal: fundamentos dogmático-procesales y de derecho comparado para la aplicación de la prueba prohibida en el proceso penal acusatorio. Lince: Instituto Peruano de Criminologia y Ciencias Penales, 2008.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 7ª ed., rev. e atual. São Paulo: Saraiva, 2012.

OECD. Organização para a Cooperação e Desenvolvimento Econômico. The OECD Privacy Framework. Disponível em: <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 06/08/2018.

OLIVEIRA, Eugênio Pacelli de. Curso de Processo Penal. 17ª Ed. rev., atual. e ampl.. São Paulo: Atlas, 2013.

PINHEIRO, Patricia Peck. Direito digital. 5.ed. rev., atual. e ampl. São Paulo: Saraiva, 2013.

SILVA, César Dario Mariano da. Provas ilícitas. 6. ed. São Paulo: Atlas, 2010.

SILVA, José Afonso da. Curso de Direito Constitucional Positivo. Malheiros: São Paulo, 2011.

STAIR, Ralph M.; REYNOLDS, George W. Principles of Information Systems: A Managerial Approach. 9ª Ed.. Boston: Course Technology, 2010.

STF. HABEAS CORPUS: HC nº 91.867/PA. Relator: Ministro Gilmar Mendes. DJ: 24/04/2012. Supremo Tribunal Federal, 2012. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328>. Acesso em: 05/08/2018.

STJ. RECURSO EM HABEAS CORPUS: RHC nº 89.981/MG. Relator: Ministro Reynaldo Soares da Fonseca. DJ: 05/12/2017. Superior Tribunal de Justiça, 2017. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201702509663&dt_publicacao=13/12/2017 >. Acesso em: 07/08/2018.

SUPREMA CORTE DOS ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. Carpenter v. United States – 585 U.S. j. em 22/06/2018. Disponível em: <https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf >. Acesso em 30/07/2018.

TEIXEIRA, Tarcisio. Curso de Direito e Processo Eletrônico: Doutrina, jurisprudência e prática. 2ª Ed. São Paulo: Saraiva, 2014.