BUSCA E APREENSÃO DE DADOS EM TELEFONES CELULARES: NOVOS DESAFIOS DIANTE DOS AVANÇOS TECNOLÓGICOS

Search and seizure of cellphone records: new challenges facing technological advances

Revista Brasileira de Ciências Criminais | vol. 156/2019 | p. 353 - 393 | Jun / 2019
DTR\2019\31674

Ricardo Jacobsen Gloeckner
Pós-Doutor em Direito pela Università Frederico II (2016). Doutor em Direito pela Universidade Federal do Paraná (2010). Coordenador da Especialização em Ciências Penais da Pontifícia Universidade Católica do Rio Grande do Sul. Professor do Programa de Pós-Graduação em Ciências Criminais da Pontifícia Universidade Católica do Rio Grande do Sul. Advogado. ricardogloeckner@hotmail.com

Daniela Dora Eilberg
Mestra em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul (2018). Bacharela em Ciências Jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul (2016). Advogada. daneilaeilberg@gmail.com

Área do Direito: Constitucional; Penal; Processual
Resumo: A busca e apreensão no ordenamento jurídico brasileiro se restringe a um Código de Processo Penal voltado meramente às coisas materiais, evidenciando a inexistência de uma regulação normativa específica que acompanhe a atual dinâmica das relações sociais que implica o alto nível de uso tecnológico em todas as esferas. A ausência da adequação dessa disciplina jurídica diante da evolução tecnológica somada à lacuna jurídica sobre a custódia da prova contribui para a criação de categorias divorciadas de sua natureza jurídica. Nesse sentido, o presente artigo visa a analisar a licitude da busca e a apreensão de dados extraídos de telefones celulares. Para tanto, utilizou-se a pesquisa bibliográfica e a análise jurisprudencial de casos da Suprema Corte dos Estados Unidos, do STF, STJ, do Tribunal de Justiça da União Europeia e as inovações trazidas pelo Tribunal Constitucional Federal alemão. Uma especial atenção é dada aos casos Riley vs. California e Carpenter vs. United States. Entre outras questões, destacam-se as dificuldades em relação à obtenção dos dados eletrônicos que se encontram no telefone celular e a necessidade de maior definição quanto aos limites da busca e do material que poderá ser apreendido.

Palavras-chave: Busca e apreensão – Telefone celular – Dados digitais – Prova ilícita – Autorização judicial
Abstract: The search and seizure in the Brazilian legal system is restricted to a code of criminal procedure focused merely on material things. Furthermore, it is possible to observe the lack of specific normative regulation that would be able to follow the current dynamics of social relations that implies the high level of technological use in all spheres. The absence of adequacy of this legal discipline in the face of the technological developments along with the legal gap on the custody of evidence contributes to the creation of categories divorced from their legal nature. In this sense, this article aims to analyze the lawfulness of the search and the seizure of data extracted from cellular phones. For this purpose, a bibliographic research and case law analyses of the US Supreme Court, STF, STJ, the Court of Justice of the European Union and the innovations brought by the German Federal Constitutional Court. A special attention is directed to the cases Riley v. California and Carpenter v. United States. Among other issues, we highlight the difficulties in obtaining the electronic data found in the cell phone and the need for greater definition regarding the limits of the search and the material that can be arrested.

Keywords: Search and seizure – Cell phone – Digital data – Illegally obtained evidence – Warrant
Sumário:

1.Introdução

O tema da busca e apreensão no Brasil[1] é um daqueles áridos campos do processo penal em que, apesar da mudança constitucional e convencional, permanece confinado a uma doutrina acrítica, tratando das questões normativas a partir da base de codificação italiana de 1930[2]. Isso para não se referir à própria lacuna bibliográfica existente sobre o assunto[3]. Interessante notar que não obstante as diversas reformas que aconteceram no Código de Processo Penal (LGL\1941\8), os artigos 240 e subsequentes, que tratam da busca e apreensão como "medida acautelatória", jamais sofreram qualquer espécie de modificação – seja para contemplar novas hipóteses, requisitos ou pressupostos, seja para tutelar a medida em consonância com a Constituição de 1988 ou mesmo com os tratados internacionais de direitos humanos em que o Brasil configura como signatário.

A própria inserção do tema no Capítulo VII do Código de Processo Penal (LGL\1941\8), tendo como objeto a prova, é um grande equívoco, que contribui enormemente para a manutenção de desalinhos e desacordos constitucionais e convencionais. Dentro de um enquadramento constitucional, os dispositivos que poderiam ser convocados para disciplinar a busca e a apreensão (inequivocamente de institutos processuais distintos, apesar de o Código de Processo Penal (LGL\1941\8) ter tratado os institutos de forma unívoca[4]) são o art. 5º, XI, da Constituição – que regula a inviolabilidade do domicílio –, o art. 5º, X – que dispõe sobre a inviolabilidade da vida privada e da intimidade –, assim como o inciso XII do mesmo artigo – que cuida da inviolabilidade do sigilo de correspondência e das comunicações telegráficas e, ainda, do sigilo de dados, resguardando a Constituição da República o sigilo das comunicações telefônicas, nos moldes da Lei 9.296/96 (LGL\1996\65). Ademais, duas outras normas constitucionais podem ser referenciadas como mecanismos de tutela dos direitos fundamentais concernentes às buscas e apreensões: o respeito ao devido processo legal (art. 5º, LIV) e a inadmissibilidade das provas ilícitas (art. 5º, LVI).

Por seu turno, no que diz respeito à esfera da Convenção Americana de Direitos Humanos[5], a matéria está disciplinada no seu art. 11.2, ao afirmar que

"ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio" e no seu art. 17.1, que, por sua vez, estabelece que "ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio".

Portanto, em consonância com os dispositivos constitucionais e convencionais, há uma clara dimensão de restrição às buscas, cuja natureza jurídica é a de meio de obtenção de prova – o que implica, inevitavelmente, a relativização de direitos fundamentais dos sujeitos que suportam a medida. Contemporaneamente, os institutos da busca e da apreensão são categorias jurídicas insuficientes para regular todos os direitos fundamentais e suas correlatas garantias.

Isso porque, a busca – que relativiza um direito fundamental – evidentemente deve seguir as diretrizes normativas para que seja contemplado o devido processo, sob pena de se ter uma prova obtida por meio ilícito. Ou seja, a obediência às hipóteses normativas como verbi gratia (e.g. requisitos do mandado, horário de cumprimento etc.) demonstra-se imprescindível. A apreensão, contingente em relação à busca, também deve corresponder aos ditames legais, parcamente regulados pelo art. 245, §§ 6º e 7º do CPP (LGL\1941\8), que disciplina a elaboração de auto circunstanciado dos objetos apreendidos.

Além desses dois institutos (busca e apreensão), o direito contemporâneo exige requisitos para a custódia do material apreendido, de modo que ao Estado compete resguardar os elementos encontrados de eventuais contaminações e manipulações, sendo seu dever traçar controles e registros sobre a manipulação do material. Portanto, além das usuais buscas e apreensões, tem-se a necessária cadeia de custódia que perfaz elemento da própria validade da prova encontrada[6]. Assim, o binômio busca e apreensão deve ser, obrigatoriamente – por força de inúmeros dispositivos de ordem constitucional –, reinterpretado como uma relação tricotômica: busca-apreensão-custódia, sendo os dois últimos institutos contingenciais em relação ao primeiro.

Ainda a título de introdução, é forçoso avaliar que, a exemplo de alguns países como os Estados Unidos, diversas formas de busca têm sido eufemisticamente tratadas como institutos diversos. O escândalo do monitoramento de milhões de cidadãos norte-americanos pela NSA, vazados por Eduard Snowden (que demonstravam como o governo americano, a partir de parceiros como Google, Facebook e Apple, entre outros, vigiavam a população) acarretou a regulação pela Quarta Emenda à Constituição norte-americana, tendo em vista que a medida foi juridicamente trabalhada dentro de outros moldes. Esse movimento, consoante demonstra Friedman, é uma tendência a evitar qualquer tensão com o direito dos cidadãos norte-americanos de não sofrer buscas ilegais e injustas[7].

Em realidade, a discussão sobre se uma determinada medida constitui ou não uma busca tem sido objeto de discussão durante muito tempo na Suprema Corte Americana. No caso Olmstead vs. United States[8], o debate recaiu sobre a circunstância de as escutas telefônicas serem ou não um determinado tipo de busca. Mediante uma votação por cinco x quatro, a Suprema Corte interpretou que as escutas telefônicas não estariam restringidas pela Quarta Emenda, uma vez que temia a sua ampliação[9], sob a alegação de que as buscas se dão sempre sobre "coisas materiais". A orientação da Suprema Corte Americana tão somente mudou de direção em Katz I United States[10], que aplicou a Quarta Emenda às "coisas imateriais", definindo a privacidade como âmbito de proteção.

No caso brasileiro, a fim de se subtrair do controle constitucional e convencional, mais especificamente, o fenômeno de "eufemização" das buscas também aparece. Como exemplo, pode-se citar a "identificação genética", tratada como uma hipótese – e, inclusive, regulada pela Lei 12.037/09 (LGL\2009\2151), com as alterações trazidas pela Lei 12.654/12 (LGL\2012\1889), que introduziu tal "identificação genética".

Em Maryland vs. King[11], o exame do caso se deu sobre a razoabilidade da Lei do Estado de Maryland determinar a extração compulsória do material genético de presos por crime violento com a base de dados das investigações ainda em aberto, afirmando-se que se tratava de caso similar à identificação das digitais. Friedman destaca que "a identificação criminal não tem nada a ver com o porquê o Estado de Maryland extraiu e testou o DNA de King"[12], pois o material genético do preso foi utilizado para resolver casos em aberto e isso não é, em hipótese alguma, um caso de identificação criminal, mas de obtenção de prova, ou seja, "as amostras foram coletadas como parte de uma investigação oficial de um crime"[13]. E, assim, trata-se de uma burla aos direitos envolvidos na Quarta Emenda.

Como se pode concluir do caso americano, a mesma orientação parece adotar o sistema brasileiro, ao situar uma busca por material genético como uma hipótese de identificação criminal. Ora, quando se tratar de medida que tenha por escopo a obtenção de prova se está diante de uma busca, seja qual for o nome adotado pelo legislador. A evolução da tecnologia e a ausência de atualização da disciplina jurídica sobre a busca e a apreensão (além da lacuna jurídica sobre a custódia da prova) contribuem para a criação de categorias divorciadas de sua natureza jurídica, como é o caso da identificação criminal. A disciplina da busca, no atual Código de Processo Penal (LGL\1941\8), especialmente, volta-se para coisas materiais (como é o caso da busca pessoal e em lugares), podendo ser conectada à mesma interpretação dada pela Suprema Corte americana no caso

Olmstead. Entretanto, como referido, o avanço da tecnologia demonstra a necessidade de que novas modalidades de meio de obtenção de prova sejam tratadas como casos de busca. Entre eles se pode citar: a) busca genética; b) busca de dados eletrônicos; c) busca de coisas (atualmente é o caso da busca em lugares e buscas pessoais reguladas pelo código de processo penal); d) buscas para a obtenção de metadados (como números de celulares, uso de cartão de crédito, envio de mensagens, data, para quem foram enviadas etc.); e) buscas para a localização via GPS.

O objeto do presente artigo é exclusivamente a análise da busca e da apreensão de dados extraídos de aparelhos de telefonia móvel, que não possuem regulação normativa específica. Ademais, a apreensão do aparelho e dos dados eletrônicos que se encontram no dispositivo oferecem não apenas dificuldades em relação à obtenção dos dados, mas, substancialmente, a necessidade de ainda maior delimitação quanto aos limites da busca e do material que poderá ser apreendido.

2.A busca e apreensão realizada em aparelhos celulares

O avanço dos meios tecnológicos impele o direito para panoramas cada vez mais complexos, nos quais a atuação do Estado na persecução de delitos e os direitos de personalidade dos indivíduos entram em rota de colisão. Nesse cenário, os meios de investigação criminal tendem a se servir de plataformas tecnológicas que possibilitam ampla acessibilidade e conectividade em uma sociedade da informação[14]. A evolução dos aparelhos celulares e a revolução provocada pelo surgimento dos smartphones garantem certamente que antigos julgados e decisões resultem, com o passar dos anos, insuscetíveis de bem apreender os novos fenômenos tecnológicos, requerendo-se, sempre, a reflexão em torno do novo.

O que deve ser imediatamente bem compreendido é que o aparelho celular configura-se, concomitantemente, como um objeto capaz de assegurar a portabilidade[15] de registros e informações de conteúdo pessoal e receptáculo de tecnologias de informação (especialmente aplicativos), que faz o papel de conector entre o usuário e múltiplos veículos de informação e facilitadores. Dessa maneira, ao mesmo tempo que o celular integra aparatos tecnológicos – como câmeras digitais, agendas de contato, calculadoras, gravadores de voz e outros tantos instrumentais –, também acaba por servir como um verdadeiro computador, atuando, então, como uma plataforma tecnológica de integração entre múltiplos canais de comunicação, além de permitir, como dispositivo tecnológico, a utilização de aplicativos de trocas de mensagens (e.g. WhatsApp), de acesso e movimentação de contas bancárias, de aquisição e armazenamento de passagens aéreas, de verificação e utilização de e-mails registrados no dispositivo, de acesso às redes sociais como o Facebook.

Portanto, evidentemente, o aparelho de telefone celular não se presta unicamente à comunicação por telefone, o que lhe rende uma terminologia enganosa. Apesar da nomenclatura "telefone celular", os atuais aparelhos (smartphones) são computadores móveis multifuncionais, capazes de servir, também, como instrumentos para ligações telefônicas. Logo, parece óbvio afirmar-se que a tutela do direito à privacidade que recai sobre os limites estatais na obtenção de informações não pode ser (bem) protegido, unicamente recorrendo-se ao argumento de que a Lei 9.296/96 (LGL\1996\65) não contempla a proteção dos dados digitais contidos no aparelho telefônico. E isso é por demais elementar: um aparelho celular é multifuncional e a Lei 9.296/96 (LGL\1996\65) trata exclusivamente do sigilo telefônico.

Entretanto, o fato de que não há legislação específica sobre o acesso ao conteúdo do celular é diverso da afirmação de que se trata de um conteúdo de acesso "livre" às autoridades públicas. Interpretando-se rigorosamente todos os impactos trazidos pelas tecnologias móveis, a justaposição de inúmeros aplicativos em apenas um dispositivo não apenas reclama a reserva jurisdicional. O acesso aos distintos aplicativos reclama autorizações judiciais precisas: acesso a mensagens trocadas pelo WhatsApp, acesso a dados bancários, acesso a contas de e-mail, tudo isso reclama da autoridade judicial que

examine as distintas formas de afastamento da privacidade. Assim, a rigor, para que a polícia examine dados bancários, telefônicos, contas de e-mail, o aplicativo WhatsApp, tudo deve ser detalhadamente requerido e examinado pelo juízo, sob pena de se estabelecer indevidas quebras não autorizadas a sigilos protegidos pela lei e pela Constituição da República. Aliás, o acesso ao telefone celular, mediante uma autorização genérica, poderia consistir em um "atalho" que facilitaria, mediante apenas um pedido e uma decisão, acesso a múltiplas dimensões da privacidade, considerando que o aparelho celular, como já referido, é, ao mesmo tempo, um facilitador e um mecanismo de armazenamento de informações.

Isso é assim porque duas são as balizas que regulam as atividades exercidas por intermédio dos aparelhos celulares. A primeira delas é a portabilidade. O uso cada vez mais disseminado de aplicativos capazes de gerenciar múltiplas tarefas humanas tem como elemento substancial o fato de que o aparelho celular pode armazenar todos esses utilitários em um só dispositivo. Portanto, em vez de o indivíduo ter um computador, uma câmera digital, uma agenda escrita e outros utilitários individualizados, utiliza um único dispositivo capaz de executar todas essas tarefas com alto grau de rendimento e performance. Assim, a capacidade de portabilidade, grande virtude dos smartphones, não implica renúncia, por parte do sujeito, da inviolabilidade de distintos direitos que podem ser exercidos nas operações acima referidas. Em síntese, portabilidade não se confunde com apreensibilidade dos bens.

Ademais, a portabilidade se tornou possível graças à capacidade de armazenamento e de memória que tais dispositivos são capazes de possuir. Logo, alguém antes da revolução digital jamais teria a possibilidade de ter apreendido consigo tantos documentos e informações como o armazenamento no celular permite. Sem dúvidas, o paralelo com os documentos físicos (objeto da decisão no caso Olmstead e que serviu durante largo tempo para a Suprema Corte americana balizar as suas decisões) é absolutamente inapropriado, pois o conteúdo apreendido em um dispositivo celular seria o equivalente a alguém ter apreendido milhares de fotos, um computador, uma câmera digital, cartão e conta bancária, enfim, uma gama enorme de informações que jamais seriam apreendidos em um único momento estando na posse de um sujeito.

Além da portabilidade, que se constitui como um requisito absolutamente primordial nas relações sociais neste milênio, deve-se perquirir pela segunda questão que impõe uma dinâmica a ser considerada no uso de dispositivos móveis. Trata-se da questão da segurança[16]. Com efeito, a portabilidade acarreta importantes problemas em caso de perda ou mesmo de roubo ou furto do dispositivo móvel. As empresas que desenvolvem os aparelhos têm sofisticado cada vez mais os seus programas utilitários que garantam ao usuário do telefone celular certa segurança. Logo, sistemas de reconhecimento facial e reconhecimento por digitais são exemplos que identificam a preocupação dos usuários desses aparelhos com a segurança. Segurança que garante, a seu tempo, a relevantíssima portabilidade do dispositivo e todas as informações armazenadas. Para se ter ideia da importância das transações realizadas por meio digital, hoje em dia a maneira mais segura de se usar o internet banking é via o telefone celular e o aplicativo de banco[17].

2.1.O direito à privacidade e as novas tecnologias de informação: a insuficiência da regulação contida na Lei 9.296/96

O direito à privacidade não pode ser mais tratado dentro do paradigma clássico do right to be left alone, de acordo com a clássica formulação de Samuel Warren e Louis Brandeis em seu artigo de 1890[18]. O direito à privacidade não pode ser lido e interpretado apenas a partir de uma postura negativista e isolacionista como a do paradigma clássico. Posta em outros termos, a privacidade lida com o indivíduo e as múltiplas possibilidades de controle sobre as informações que lhe dizem respeito. E, como consequência, os diversos desenvolvimentos de uma teoria da privacy, mormente aquelas posteriores ao famoso estudo de Warren e Brandeis acabaram por deslocar a noção de privacidade para os direitos de personalidade. Dessa maneira, o que está em jogo não é – a não ser que

se queira reproduzir um contexto jurídico-social liberal-individualista – um direito à privacidade versus um direito do Estado na persecução do crime. Têm-se como ponto de base as relações dos direitos da personalidade versus as indevidas inserções do Estado no âmbito daqueles complexos multilaterais de relações. Assim, a questão que fica clara é aquela dos limites e alcances dos direitos de personalidade.

Sendo um complexo de relações multilaterais, os direitos de personalidade compreendem: a) a inviolabilidade de domicílio; b) o controle sobre as informações de cunho pessoal; c) a liberdade corporal e de autodeterminação, entrando aqui questões como o aborto e a eutanásia; d) todas as questões envolvendo a vigilância e formas de interrogatório. É assim que a privacidade deixa de lado o status de "ser deixado só" para regular um conjunto de situações jurídicas que indicam escolhas de vida, que devem ser abrigadas contra formas de ingerência estatal e de estigmatização social, tutelando as liberdades tanto políticas quanto existenciais[19]. Assim, a esfera do privado corresponde inequivocamente o conjunto de dados pessoais[20], o que gera um direito à "autodeterminação informativa", sendo, em consequência disso, uma condição da cidadania[21]. Tomando-se o telefone celular como um conector entre diversos utilitários e aplicativos, chega-se facilmente à conclusão de que o dispositivo carrega tantas informações que, no limite, acabam se confundindo como uma extensão informacional da própria pessoa. O acesso ao telefone celular sem autorização judicial representa gravíssima violação aos direitos de personalidade, uma vez que, consoante já referido, esse gadget é um verdadeiro conector das mais variadas tecnologias, o que o torna não apenas uma ferramenta indispensável para muitas pessoas, como também uma extensão dos direitos de personalidade. Assim, com efeito, não se resume à proteção contra a quebra do sigilo veiculada na Lei 9.296/96 (LGL\1996\65), que regula as formas de interceptação telefônica.

Veja-se que se o sigilo telefônico deve ser objeto de autorização judicial, mais afrontoso seria o acesso aos dados contidos no telefone móvel, pois nesses dispositivos estão congregadas as mais amplas e irrestritas ebulições e manifestações do direito à personalidade (cuja segmentação pode ser conferida nos aplicativos para celulares e em seus utilitários). No campo político criminal, em um país com mais telefones celulares do que pessoas[22], a permissão para que a polícia devasse e acesse sem restrições e autorização judicial o conteúdo dos aparelhos móveis equivaleria, no ponto, a esvaziar o direito à privacidade. Mandados de busca e apreensão de computadores, por exemplo, seriam medidas írritas, posto que a polícia poderia ter acesso livre ao computador perfectibilizado no telefone celular. Requerer uma autorização judicial para análise das contas de e-mail seria medida nula, posto que bastaria à polícia invadir o aparelho móvel e verificar as correspondências do suspeito.

Sem exagero, a revolução digital fez com que os telefones celulares fossem verdadeira extensão dos direitos de personalidade dos sujeitos. E, além disso, provocou uma mudança drástica no campo da preservação desses direitos. Tudo pode ser acessado por um único dispositivo portável[23]. Daí por que o telefone celular deve ter a mais ampla e irrestrita forma de proteção contra o acesso a dados por terceiros. Sendo um dispositivo que permite reconstruir onde a pessoa esteve, com quem ela falou, quais os horários, quais os e-mails enviados e recebidos, quais as mensagens trocadas, qual o círculo de conhecidos da pessoa e com quem ela interage (como nas redes sociais), o telefone celular representa uma sensível fragilidade do indivíduo frente à proteção de seus dados. A proteção ao telefone celular representa, hoje, a mais necessária tutela de proteção dos direitos à privacidade. Em outras palavras, franquear o acesso irrestrito aos dados digitais equivaleria a uma abolição completa dos direitos de personalidade no Brasil.

2.2.Alguns precedentes no processo penal brasileiro sobre o acesso a informações contidas em telefones móveis

No recurso ordinário em Habeas Corpus 51.531-RO, julgado em 2016, o Superior Tribunal de Justiça se manifestou sobre a matéria. Tratava-se, na oportunidade, de crime de tráfico de drogas e de associação para o tráfico. A polícia apreendeu o celular

do recorrente, procedeu à devassa dos dados contidos no telefone celular, produzindo prova pericial. Nesse caso, o fundamento precípuo que autorizou a polícia a proceder à coleta das informações contidas no aparelho celular foi o de que o procedimento não estava albergado pela Lei 9.296/96 (LGL\1996\65), argumento utilizado reiteradas vezes em procedimentos criminais no Brasil.

Nesse caso específico, em seu voto, o Ministro Nefi Cordeiro asseverou que o telefone celular deixou de ser um instrumento que se presta unicamente a conversas telefônicas, permitindo o acesso a inúmeras funções[24]. Além disso, a tese proposta pelo Ministro Nefi Cordeiro acerca da ilicitude da prova foi corroborada pelo voto do Ministro Rogério Schietti Cruz, ao sustentar que o precedente exarado pelo Supremo Tribunal Federal no Habeas Corpus 91.867-PA, julgado em 2012, não poderia analisar a verdadeira revolução tecnológica operada pelos smartphones, o que o torna imprestável para servir de arrimo a qualquer julgado que porventura venha a ser realizado sobre a questão da acessibilidade ao conteúdo de telefone celular.

Como se pode notar, há que se ter em mente que o acesso não autorizado aos telefones celulares, com a utilização de informações privadas ali existentes pela polícia, não pode ser tratado como se apenas se estivesse diante de situação análoga à quebra de sigilo telefônico, pois coloca a situação jurídica em estado muito aquém de todas as dimensões do direito à privacidade que acabam por ser colocadas em xeque pelos avanços da tecnologia móvel. Não se trata, como referido nesse caso julgado pelo Superior Tribunal de Justiça, de quebra de sigilo telefônico. Trata-se de violação a todos os direitos de personalidade que se encontram cristalizados no uso do celular como ferramenta de comunicação, não restrita às conversas telefônicas bem como de dispositivo de armazenamento, capaz de guardar em sua memória uma significativa quantidade de informações pessoais como fotos e vídeos.

Outro precedente julgado no Brasil e que trata de matéria similar é o recurso ordinário em Habeas Corpus 89.981-MG e que se coaduna com o caso alhures referido. O recurso tinha como objeto de análise uma denúncia pela prática do crime de furto qualificado e associação criminosa. A autoridade policial teria, em uma abordagem policial e sem autorização judicial, acessado mensagens arquivadas no WhatsApp, violando o conteúdo de intimidade do recorrente. O STJ decidiu no sentido da ilicitude da colheita dos dados contidos no aparelho telefônico dos investigados, sem autorização judicial, bem como das demais derivadas, nos termos do art. 157 do CPP (LGL\1941\8). Nessa perspectiva, fundamentou que teria sido vilipendiada a inviolabilidade da privacidade dos dados armazenados no celular (mensagens de texto arquivados no WhatsApp).

Com efeito, o Ministro Reynaldo Soares da Fonseca proferiu seu voto dando provimento ao recurso ordinário em habeas corpus para reconhecer a ilicitude da colheita dos dados dos aparelhos telefônicos e das demais provas recorrentes, com o seu posterior desentranhamento dos autos. Fundamentou que, apesar de o caso não configurar uma hipótese prevista pela Lei 9.296/1996 (LGL\1996\65) nem pela Lei 12.965/2014 (LGL\2014\3339) – haja vista a diferenciação de quebra do sigilo telefônico por meio de interceptação telefônica (violação da garantia de inviolabilidade de comunicações) – com o acesso indevido a dados de celular apreendido sem autorização judicial, era possível constatar-se a violação à intimidade e à vida privada, nos termos do art. 5º, X, da CF (LGL\1988\3).

Contudo, apesar dessas decisões exaradas pelo STJ, há precedente do Supremo Tribunal Federal[25] em que o acesso aos dados contidos no telefone celular é questionado. Naquela oportunidade, entendeu-se que não haveria qualquer violação à privacidade o acesso da polícia no telefone celular. Três seriam os pontos de apoio da decisão: a) inexistência de direitos fundamentais absolutos; b) ausência de proteção da Lei 9.296/96 (LGL\1996\65); c) a privacidade protege o sigilo da comunicação de dados e não "os dados". No entanto, nenhum desses argumentos é capaz de dar conta da complexidade das questões envolvendo os direitos fundamentais e os direitos de personalidade diante de dispositivos multifuncionais.

Os smartphones, que passaram a integrar os mais diversos tipos de tecnologia, passaram a ser, a rigor, extensões do direito à personalidade de seus proprietários e usuários, capazes de armazenar informações que de nenhuma forma seriam abertas ao público em geral. Funcionam em muitas hipóteses como verdadeiras próteses cibernéticas, bastando para isso verificar-se o funcionamento da memória do celular, que substituiu progressivamente o próprio uso da memória humana no armazenamento de números de conhecidos ou de pessoas de nossas relações sociais. O paralelo traçado na comparação com o sigilo da comunicação telefônica e eventuais documentos físicos é manifestamente inapropriado. No primeiro caso, o dispositivo móvel ultrapassa e muito a esfera da comunicação telefônica. Disso decorre a necessidade de maior proteção relativamente à própria comunicação telefônica.

Por outro lado, comparar os dados digitais com os físicos também se mostra um procedimento inadequado, pois ninguém portaria consigo tamanha documentação. É, como salientado, justamente a portabilidade, capacidade de armazenamento e segurança que garantem aos indivíduos a confiança em terem a sua privacidade protegida. Como assinalou a Suprema Corte Americana em caso que será analisado, autorizar a devassa no aparelho celular hoje representa maior ingerência na privacidade do que uma busca e apreensão no domicílio.

No julgamento do caso Riley vs. California, o juiz Samuel Alito levantou a questão sobre a possibilidade de a polícia examinar fotos e pedaços de papel contendo nomes e números de telefone. Todavia, a Suprema Corte Americana acabou por reconhecer a mais absoluta diversidade da natureza jurídica de ambos os tipos de informação, de maneira que as provas físicas e as digitais são completamente distintas, não se prestando a comparação para fins jurídicos. Ou, ainda, nas palavras da Suprema Corte americana no caso Riley vs. California, "o fato de que alguém dobrou e guardou um extrato bancário no bolso não justifica uma busca em todos os extratos bancários nos últimos cinco anos"[26].

Autorizar a polícia a proceder a uma devassa no celular das pessoas sem autorização judicial equivale hoje a tornar 306 milhões de aparelhos sem qualquer tipo de proteção[27]. É ainda mais grave do que autorizar a polícia a violar o domicílio de todos os nossos habitantes, pois nem mesmo nessa modalidade se poderia encontrar tanta informação reunida como em um dispositivo móvel[28].

Atualmente, em sede do Supremo Tribunal Federal, foi reconhecida a repercussão geral do Recurso Extraordinário com Agravo 1.042.075-RJ, caso[29] que versava justamente acerca da licitude de prova obtida por meio de acesso a dados do telefone celular sem autorização judicial[30]. O julgamento foi agendado para o dia 13 de março de 2019.

3.Bases normativas e jurisprudenciais de direito comparado

Considerando-se, portanto, que a matéria no Brasil é bastante recente, calha trazer à tona alguns dados de direito comparado capazes de contribuir para a discussão a respeito da matéria.

3.1.As inovações na jurisprudência do Tribunal Constitucional Federal alemão

O Tribunal Constitucional Federal alemão compreendeu as mudanças da revolução tecnológica no campo da sociedade de informação em seu corpo jurisprudencial, a contribuir com importante reforma na concepção do direito fundamental. Assim, dentro de sua função inerente à responsabilidade de produção da jurisprudência constitucional e frente aos progressos científico-tecnológicos, o Tribunal realizou um exercício hermenêutico legítimo do Direito para se adaptar às novas circunstâncias da sociedade atual, inovando dentro da esfera do direito constitucional[31].

A sentença referente ao caso Lüth foi a primeira a contribuir nesse processo. Versava sobre o direito fundamental à liberdade de expressão e auxiliou na chamada

"constitucionalização do ordenamento jurídico". O Tribunal consolidou entendimento de que os direitos fundamentais teriam também uma espécie de "dimensão jurídico-objetiva" para todo o ordenamento jurídico. Logo, deveria colaborar com o desenvolvimento dos deveres de proteção e elaboração da prohibición del defecto de protección, qual seja, a proibição do excesso à limitação dos direitos fundamentais desenvolvida no marco do princípio da proporcionalidade[32].

No ano de 1983, o Tribunal alemão proferiu decisão a respeito da proteção do direito geral de personalidade, com base nos arts. 2.1 e 1.1 GG, determinando a possibilidade de o indivíduo decidir sobre a entrega de seus dados pessoais. Nessa perspectiva, o caso alemão configurava situação semelhante ao caso brasileiro sobre os dados digitais do aparelho celular. Essa sentença refletiu uma maior exploração por parte do Tribunal alemão sobre a matéria dos direitos fundamentais, também com base nos arts. 2.1 e 1.1 GG. O direito constitucional foi hermeneuticamente desenvolvido pelo Tribunal, no intuito de adaptar o direito geral da personalidade. Como consequência, concluiu-se pela impossibilidade de proteção da autonomia de liberdade do sujeito dentro da nova sociedade de informação e, em 2008, conceituou-se o chamado "direito fundamental IT" (direito fundamental das tecnologias e da informação e telecomunicação) e se passou a denominar "garantia" do direito fundamental em vez de "proteção" – a fazer referência ao Estado garante e à dimensão jurídico-objetiva da proteção dos direitos fundamentais [33]. A criação desse direito fundamental sem precedentes é oriunda da obrigação estatal de proteção a dignidade das pessoas e o livre desenvolvimento de sua individualidade diante das agressões externas, a incluir a da própria autoridade pública[34]. O caso também estimulou uma mudança na disciplina constitucional, com a previsão do art. 91c GG.

Em conclusão, o exemplo alemão demonstra a importância do exercício hermenêutico do Tribunal constitucional para garantir a supremacia dos direitos fundamentais, atualmente em crise na sociedade contemporânea. Diante dos avanços tecnológicos e da extensão das capacidades de abusos autoritários, o Tribunal reconheceu o seu papel essencial na barragem de situações ilegais e na adoção de medidas de correção e/ou reparação para a proteção dos direitos. Logo, a extensão pormenorizada do direito fundamental à proteção da personalidade desenvolvido no corpo jurisprudencial alemão é uma referência exemplar à posição que deve ser adotada no presente caso pelo ordenamento jurídico brasileiro, haja vista a responsabilidade dos órgãos jurisdicionais em contribuir com a proibição dos excessos às limitações dos direitos fundamentais dentro do marco da proporcionalidade.

3.2.O leading case Riley vs. California

Um dos mais conhecidos casos em que um tribunal superior foi chamado a enfrentar a questão do acesso não autorizado a celular é o julgado Riley vs. California, objeto de análise pela Suprema Corte Americana dos Estados Unidos. Nesse caso, o acusado Riley foi detido pela polícia de San Diego, que constatou estar a sua carteira de motorista vencida. Ao proceder à revista do veículo, a polícia encontrou duas armas. Incontinenti, a polícia revistou e encontrou o celular de Riley, constatando informações relevantes em seu celular, conectando o acusado a uma gangue responsável por um homicídio.

Para que seja bem compreendido o caso, a polícia norte-americana está autorizada a proceder à revista nas pessoas presas em flagrante, tendo em vista a doutrina denominada como SITA (search incident to a lawful arrest), que permite aos policiais procederem à busca no corpo do preso e nas imediações em que a prisão aconteceu, com a finalidade específica de encontrar objetos que possam comprometer a integridade física dos policiais. No caso específico, a doutrina SITA, que havia sido produzida no caso Chimel vs. California, de 1969 (e que corresponde a uma das pequenas exceções norte-americanas à Quarta Emenda, garantindo uma busca sem mandado judicial) havia sido invocada e aplicada tanto pelo juiz de primeiro grau quanto pelo Suprema Corte da California[35].

No caso Chimel vs. California, debateu-se a extensão e a razoabilidade do mandado de busca. Chimel foi preso em sua casa, e os policiais procederam a uma busca completa em sua casa (de três quartos), incluindo a garagem e o sótão. Vejamos o argumento adotado pela Suprema Corte nesse caso:

"Quando uma prisão é realizada é razoável ao agente policial proceder à busca na pessoa detida a fim de remover quaisquer armas que depois possam ser utilizadas para resistir à prisão ou obter uma fuga. Do contrário, a segurança do policial pode ser colocada em risco e a própria prisão frustrada. Ademais, é completamente razoável para o policial que efetuou a prisão proceder à busca de qualquer prova da pessoa do detido, a fim de evitar a sua ocultação ou destruição... Há ampla justificação, assim, para uma busca sobre a pessoa detida e na área "sob o seu controle imediato", significando tal frase a área dentro da qual ele pode obter a posse de uma arma ou a prova sujeita à destruição (Tradução nossa)[36]".

No julgado proferido pela Suprema Corte da California, sustentou-se a doutrina SITA, afirmando-se que os policiais poderiam explorar livremente o celular do detido, utilizando-se de precedente recente (People vs. Díaz), desde que o celular fosse encontrado com o acusado ou nas imediações da prisão (na área de seu alcance, consoante expressão utilizada no caso Chimel vs. California). O caso Riley vs. California é, na verdade, a junção de dois casos: o próprio Riley e o caso United States vs. Wurie[37] . A primeira questão colocada em cena no julgamento dos casos era a de que o acesso ao conteúdo digital do telefone não representava um risco à integridade física dos agentes policiais, de forma que não se poderia estar ao abrigo da doutrina SITA.

Analisando-se as distintas manifestações da Suprema Corte quanto à necessidade de mandados judiciais para obtenção da prova, constata-se claramente uma orientação no sentido de submeter a diligência ao critério da razoabilidade. Assim, o primeiro elemento que deve ser analisado em qualquer busca é a razoabilidade. A proteção estabelecida na Quarta Emenda da Constituição Americana protege os cidadãos contra buscas ilegais. E, portanto, a polícia, em caso de dúvida se precisa ou não de mandado judicial, deve requerê-lo. A razoabilidade como parâmetro da busca já foi produto do precedente Brigham City vs. Stuart, de 2006[38]. Também no precedente Vernonia School Dist. 47J v. Acton, a Suprema Corte havia se manifestado novamente sobre o mandado judicial, dessa vez afirmando que "quando uma busca é realizada pelos oficiais para descobrir provas de um crime... a razoabilidade geralmente determina a obtenção de um mandado judicial" [39]. A importância do mandado judicial é colocada fora de qualquer dúvida, consoante o caso Johnson vs. United States, quando a Corte asseverou que a relevância do mandado está na circunstância dele ser "elaborado por magistrado neutro e imparcial, ao invés de ser decidido por um agente engajado na atividade competitiva de descobrir o crime"[40].

Ainda de acordo com o julgamento proferido pela Suprema Corte, o juiz John Roberts traça importante distinção entre o caso Riley vs. California e as variações da doutrina SITA que foram se produzindo ao largo de anos, especialmente o caso United States vs. Robinson, de 1973. Nesse caso, a doutrina elaborada no caso Chimel foi aplicada em um contexto de prisão realizada por um policial, uma vez que o motorista Robinson estava dirigindo com a sua licença vencida. O policial procedeu a uma busca no corpo de Robinson, encontrando embaixo de seu casaco um objeto que não podia identificar. Ato contínuo, o policial retirou o objeto e constatou que se tratava de uma carteira de cigarro. Dentro da carteira estavam 14 cápsulas de heroína. A discussão em torno desse caso cingiu-se novamente à irrazoabilidade da busca no acusado e a doutrina SITA. A questão levantada pelo juiz John Roberts é a de se tais precedentes poderiam ser aplicados aos telefones celulares.

Tanto os smartphones quanto os celulares de tecnologia menos avançada (como aquele do caso Wurie) eram dispositivos impensáveis no tempo em que a doutrina SITA e suas variantes foram concebidas pela Suprema Corte Americana. Fundamentalmente porque o caso Robinson trata de busca e apreensão de bens físicos, e não de dados digitais

contidos em um dispositivo. Logo, de acordo com o juiz da Suprema Corte, a racionalidade que guiava o caso Robinson é naturalmente inaplicável à busca em celulares. E isso por duas razões: a) a busca por conteúdo digital em celular não oferece risco à integridade física do policial; b) não há perigo de destruição de informações contidas no dispositivo móvel, posto que não se podem equiparar os dados digitais com as provas físicas. Nesse sentido, vale à pena transcrever as palavras do juiz Roberts:

"Os dados digitais armazenados em um telefone celular não podem eles mesmos ser usados para agredir um policial ou para garantir a fuga. Os agentes policiais continuam livres para examinar os aspectos físicos do telefone, para assegurar que ele não será usado como uma arma, isto é, para determinar se há uma lâmina escondida entre o telefone e a sua capa. Uma vez que o policial verificou o telefone e eliminou qualquer ameaça física potencial, os dados do telefone não podem colocar ninguém em risco (Tradução nossa)[41]".

Resta, então, verificar a possibilidade de a busca no celular ser legítima com a finalidade de possível destruição de provas, que aparece como a segunda racionalidade subjacente ao caso Chimel vs. California. De acordo com a lógica aplicada pelo juiz Roberts no caso Riley vs. California, não há nenhum risco de que o sujeito detido pudesse comprometer os dados encontrados no aparelho celular. Bastaria que os próprios policiais fisicamente resguardassem o aparelho até a emissão do mandado judicial.

No caso Riley vs. California discutiu-se sobre a possibilidade de duas ameaças que poderiam colocar em risco as provas digitais: a) a limpeza remota do dispositivo; b) a criptografia. No primeiro caso, para ocorrer a limpeza remota, uma terceira pessoa deveria enviar um sinal via wireless, apagando os dados digitais do telefone ou, ainda, quando o celular está programado para limpar os seus dados quando ingressa em uma determinada área (geofencing). Por seu turno, a criptografia é uma ferramenta de segurança presente nos celulares contemporâneos, para além da senha de acesso. Quando a criptografia entra em cena, acionada pela tentativa de acesso, os dados se tornariam protegidos por uma tecnologia de difícil suplantação. Para evitar a primeira ameaça, bastaria aos agentes policiais desconectar o aparelho da rede wireless ou, ainda, desligar o dispositivo. Para acabar com o perigo da criptografia entrar em ação, bastaria aos policiais deixar o aparelho ligado, colocando-o em uma mochila revestida de alumínio (mochilas de Faraday), cortando qualquer possibilidade de ondas via rádio chegarem ao celular.

Dessa maneira, os dados contidos no celular eram muito diversos do caso Robinson, onde se procedeu à busca na roupa do detido e dentro de uma carteira de cigarro. Neste ponto, o juiz Robert acentua claramente que

"[...] os telefones celulares diferenciam-se, tanto quantitativa quanto qualitativamente dos objetos que poderiam estar com uma pessoa detida. O termo "telefone celular" é enganoso. Muitos destes dispositivos são de fato minicomputadores que também têm a capacidade para ser usados como telefones. Eles poderiam ser facilmente chamados de câmeras, aparelhos de vídeo, agendas, calendários, gravadores, bibliotecas, diários, álbuns, televisões, mapas ou jornais (Tradução nossa)[42]".

Uma das principais características dos celulares contemporâneos é a sua capacidade de armazenamento. Antes desses aparelhos, a busca em uma pessoa traria menores impactos em seu direito de privacidade. É justamente essa capacidade de armazenamento um dos pontos centrais relativos ao caso Riley vs. California. Novamente trazendo à baila as palavras do juiz Roberts, tem-se que:

"[...] a capacidade de armazenamento dos telefones celulares tem diversas consequências inter-relacionadas para a privacidade. Em primeiro lugar, um telefone celular reúne em apenas um lugar distintas formas de informação – um endereço, uma nota, uma prescrição, uma declaração bancária, um vídeo que revela muito mais em combinação que um arquivo isolado. Em segundo lugar, a capacidade do celular permite

que apenas um tipo de informação transmita muito mais do que anteriormente era possível. A soma da vida privada de um indivíduo pode ser reconstruída através de mil fotografias datadas, localizações e descrições. O mesmo não pode ser dito de uma ou duas fotografias de seus entes queridos amassada na carteira. Em terceiro lugar, os dados do celular podem retroagir à data da aquisição do telefone ou mesmo antes. Uma pessoa pode portar consigo um pedaço de papel lembrando-a de ligar para o sr. Jones. Ele não traria consigo um arquivo de todas as suas comunicações com o Sr. Jones dos últimos meses, como seria rotineiramente mantido pelo telefone (Tradução nossa)[43]".

Como vislumbrado corretamente pelo juiz Roberts, antes da era digital, ninguém carregaria ou portaria consigo tanta informação. Contemporaneamente, pessoas que não portam celulares seriam a exceção nos Estados Unidos. De acordo com a pesquisa 2013 Mobile Consumer Habits Study, realizada pela Harris Interactive, três quartos dos usuários de telefone celular alegam estar o tempo todo com o aparelho, enquanto 12% afirmar que usam os celulares até mesmo no chuveiro. Essa é apenas a diferença quantitativa referentemente aos demais tipos de dados. Qualitativamente, o uso do telefone celular pode revelar onde a pessoa esteve (e essa é uma das características primárias de todo telefone celular), reconstruir o seu passo a passo durante largo período, podendo-se determinar, inclusive, se ela ingressou ou não em determinado local, como uma farmácia ou um escritório. Isso sem falar, inclusive, dos aplicativos. Como asseverou a Suprema Corte Americana,

"uma busca em um telefone celular exporia ao governo muito mais do que a mais exaustiva busca em uma casa. Um celular não apenas contém em forma digital arquivos sensíveis previamente encontrados na casa. Ele também contém um amplo rol de informações privadas que jamais seriam encontradas na casa a não ser através do telefone"[44].

A situação se torna ainda mais complexa quando se constata que o uso de telefones celulares também é feito para acessar dados digitais que não se encontram armazenados no próprio aparelho (cloud computing). O acesso de conteúdo armazenado na nuvem trata da capacidade do dispositivo em acessar dados que estão armazenados em servidores remotos. Alguns usuários não conseguem distinguir entre os dados armazenados no celular e aqueles armazenados na nuvem, como bem identificado pelo Brief for Amicus Curiae Electronic Privacy Information Center (Epic). E tais dados estariam fora da margem de proteção da doutrina SITA. Acentuou o juiz Roberts que esse tipo de busca seria como encontrar a chave da casa no bolso do suspeito e argumentar que tal fato autorizaria a busca feita pela polícia.

O entendimento adotado foi no sentido de que a busca dos dados eletrônicos no aparelho celular é muito mais "invasiva" que a busca realizada em uma casa, "porque não apenas expõe 'registros sensíveis' da casa, mas também informações 'jamais encontradas em uma casa'"[45]. O que foi certificado na decisão é a circunstância de que não se está a imunizar o aparelho celular da busca, mas apenas de que ela deve ser precedida de mandado judicial.

Apesar dos grandes avanços percorridos com o presente acórdão para a compreensão da Quarta Emenda na nova era tecnológica, alguns autores apontam problemas na sentença. Kelly Ozurovich, por exemplo, evidencia três falhas[46]: i) a ausência da previsão referente a dispositivos inteligentes além dos telefones celulares, bem como inexistência de diferenciação de telefones celulares com smartphones; ii) a debilidade da orientação a respeito da aplicabilidade da sentença quando se trata da busca dos demais dispositivos tecnológicos, em razão do agrupamento dos casos de Wurie e Riley sem abordar as suas diferenças; e iii) a potencial confusão a respeito da desnecessidade da adesão ao precedente com a distinção dos casos Riley de Robinson. A autora desenvolve no sentido de que a Suprema Corte não considerou as características típicas de um telefone celular comum – como o do caso Wurie – e de outros dispositivos inteligentes comumente utilizados pela sociedade que se assemelham, em termos de ingerência de privacidade, com os smartphones, como iPad e iPods e propõe, como solução, um

entendimento mais amplo com um debate a respeito das tecnologias mais recentes.

3.3.A legislação espanhola

Os legisladores espanhóis buscaram contemplar as mudanças da sociedade contemporânea referentes ao uso corriqueiro das tecnologias de informação na investigação criminal. Nesse sentido, em sua reforma processual, dispuseram acerca da imprescindibilidade de conformar o direito interno à previsão do corpus juris europeu "a partir da regulação das medidas de investigação tecnológica no âmbito dos direitos à intimidade, ao segredo das comunicações e à proteção de dados pessoais garantidos pela Constituição"[47].

O artigo 588, sexies b, da Ley de Enjuiciamento Criminal espanhola trata do acesso à informação sobre os dispositivos eletrônicos apreendidos fora do domicílio do investigado. Naturalmente, em tal caso, compreende-se o telefone celular. De acordo com a legislação espanhola:

"La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización".

Prossegue o documento, no seu art. 588, sexies c, confirmando a necessidade de autorização judicial:

"1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial".

Como se pode notar, tem-se mais um caso de proteção dos dados contidos em dispositivo eletrônico móvel, em que a autorização judicial se faz absolutamente necessária para a validade das fontes de informação armazenadas no telefone.

3.4.A jurisprudência do Tribunal de Justiça da União Europeia e a Diretiva 2016/680 do Parlamento Europeu e do Conselho

No que diz respeito à proteção de dados pessoais na chamada "sociedade de informação", o continente europeu caminhou em direção à consolidação de algumas previsões normativas. Não apenas cabe destacar o art. 16 do Tratado sobre o Funcionamento da União Europeia e o art. 8º da Carta dos Direitos Fundamentais da União Europeia como também alguns diplomas que passaram a influenciar a produção legislativa da região. Entre eles, estão as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais[48]-[49] da OCDE (Organização para a Cooperação e Desenvolvimento Econômico), de 1980; a Convenção 108 da União Europeia (Convenção para a proteção de indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais), de 1981; a Diretiva 95/46/CE do Parlamento Europeu, sobre proteção às pessoas físicas, no que diz respeito ao tratamento de dados e da circulação destes; a Diretiva 2002/58/CE, sobre o tratamento de tais dados de forma eletrônica; os Safe Harvour Privacy Principles, de 2002; e, em 2012, uma reforma de proteção de dados, em 2016, com a previsão do Regulamento 2016/679 do Parlamento Europeu e do Conselho, que revogou a Diretiva 95/46/CE, e foi complementado pela Diretiva 2016/680 (relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detenção ou repressão de infrações penais ou

execução de sanções penais e a livre circulação desses dados), com vigência a partir de maio de 2018.

Uma vez considerado o quadro normativo da região supramencionado, volta-se à produção jurisprudencial do Tribunal de Justiça da União Europeia, o qual veio proferindo interessantes decisões referentes ao acesso à prova digital, quais sejam: i) Promusicae, em matéria cível, de 29 de janeiro de 2008 (C-275/06)[50]; ii) Leading CaseDigital Rights Ireland e Seitlinger e o[51]; iii) Schrems, 06 de outubro de 2015 (C-362/14)[52]; iv) Acórdão Tele2 Sverige (Processo C-203/15)[53], de 21 de dezembro de 2016; e v) Acórdão Ministerio Fiscal[54] (Processo C-207/16), de 2 de outubro de 2018.

No Leading CaseDigital Rights Ireland e Seitlinger e o., de 8 de abril de 2014 (C-293/12 e C-594/12), foi proposta a incompatibilidade da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações com o artigo 52º, n. 1, da Carta dos Direitos Fundamentais da União Europeia,

"na medida em que as restrições ao exercício dos direitos fundamentais que comporta, devido à obrigação de conservação de dados que impõe, não são acompanhadas pelos princípios indispensáveis que devem reger as garantias necessárias para regular o acesso aos referidos dados e a sua exploração".[55]

A decisão se deu tendo como premissa verificar-se a proporcionalidade da ingerência dos artigos 7º e 8º observados, contrapondo a proteção dos dados pessoais na perspectiva do direito fundamental ao respeito pela vida privada e a amplitude e a gravidade da ingerência neste direito. Nessa perspectiva, o TJUE concluiu que a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, é inválida.

A decisão foi no sentido do Acórdão Digital Rights Ireland, ao reiterar que a conservação de todos os dados não está de acordo com os critérios de proporcionalidade, de modo que a legislação nacional em matéria de direito penal deve ser verificada pela Comissão e pelo Tribunal (e.g. art. 15, n. 1, da Diretiva 2002/58/CE). A fundamentação do acórdão proferido envolveu a questão da imprescindibilidade de atentar quanto ao grau de ingerência dos direitos fundamentais dos dados conservados com a pretensão da derrogação da regulamentação nacional que previa a confidencialidade das comunicações eletrônicas. No entanto, a decisão também menciona a possibilidade de ocorrência desse acesso, uma vez configurada a "criminalidade grave". Ainda, a decisão segue o entendimento dos julgados anteriores no que tange ao princípio da proporcionalidade, ao fundamentar que a concessão dos dados conservados pelas prestadoras de serviços de comunicações eletrônicas pode ocorrer "dentro dos limites do estritamente necessário", conforme a previsão vinculativa do direito interno, que deve determinar as condições em que os fornecedores de serviços de comunicações eletrônicas devem conceder o acesso[56]. In verbis:

"119. Assim, e uma vez que um acesso generalizado a todos os dados conservados, independentemente de uma qualquer relação, no mínimo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário, a regulamentação nacional em causa deve basearse em critérios objetivos para definir as circunstâncias e as condições nas quais deve ser concedido às autoridades nacionais competentes o acesso aos dados dos assinantes ou dos utilizadores registados. A este respeito, só poderá, em princípio, ser concedido acesso, em relação com o objetivo da luta contra a criminalidade, aos dados de pessoas suspeitas de terem planeado, de estarem a cometer ou de terem cometido uma infração grave ou ainda de estarem envolvidas de uma maneira ou de outra numa infração deste tipo [...]. Todavia, em situações específicas, como aquelas em que os interesses vitais da segurança nacional,

da defesa ou da segurança pública estejam ameaçados por atividades terroristas, pode também ser concedido acesso aos dados de outras pessoas quando existam elementos objetivos que permitam considerar que esses dados podem, num caso concreto, trazer uma contribuição efetiva para a luta contra essas atividades.

120. Para garantir, na prática, o pleno cumprimento destas condições, é essencial que o acesso das autoridades nacionais competentes aos dados conservados seja, em princípio, salvo em casos de urgência devidamente justificados, sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente, e que a decisão desse órgão jurisdicional ou dessa entidade ocorra na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de detecção ou de ação penal [...]

121. Do mesmo modo, importa que as autoridades nacionais competentes às quais foi concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível comprometer as investigações levadas a cabo por essas autoridades. Com efeito, essa informação é, de facto, necessária para permitir que essas pessoas exerçam, nomeadamente, o direito de recurso, explicitamente previsto no artigo 15º, n. 2, da Diretiva 2002/58, lido em conjugação com o artigo 22º da Diretiva 95/46, em caso de violação dos seus direitos [...]".

O Tribunal de Justiça da União Europeia decidiu da seguinte maneira:

"1) O artigo 15º, n. 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7º, 8º e 11º, bem como do artigo 52º, n. 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica.

2) O artigo 15º, n. 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7º, 8º e 11º bem como do artigo 52º, n. 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União".

Ademais, recentemente, no Acórdão Ministério Fiscal, o Tribunal de Justiça da União Europeia, a respeito do entendimento dos julgados Digital Rights e Tele2 Sveridge, decidiu pela delimitação à imprescindibilidade de autorização judicial para o acesso de metadados dos celulares, tais como o IMEI (Identidade Internacional de Equipamento Móvel), bem como dos "dados de base" (dados do titular da linha telefônica), quando se tratar de investigação criminal e de ação penal. Nessa perspectiva, com base no princípio da proporcionalidade, o Tribunal relativizou tal acesso, afirmando que, em não se tratando de uma ofensa grave à vida privada, os dados pessoais conservados pelos fornecedores de serviços de comunicações eletrônicas podem ser obtidos ainda que a infração penal não configure particularmente grave.

A decisão foi nesse sentido porque o TJUE considerou não ser uma ingerência de direitos fundamentais grave, ao afirmar que não poderiam ser retiradas conclusões qualificadas da vida privada do sujeito e, portanto, não deveria ser limitado o acesso "em matéria de prevenção, de investigação, de detenção e de repressão de infrações penais, à luta contra a criminalidade grave.". Portanto, declarou:

"O artigo 15º, n. 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que o acesso das autoridades públicas aos dados com vista à identificação dos titulares dos cartões SIM ativados num telemóvel roubado, tais como o apelido, o nome próprio e, sendo caso disso, o endereço desses titulares, constitui uma ingerência nos direitos fundamentais destes últimos, consagrados nesses artigos da Carta, que não apresenta uma gravidade tal que esse acesso deva ser limitado, em matéria de prevenção, de investigação, de detenção e de repressão de infrações penais, à luta contra a criminalidade grave".

4. A extensão da necessidade de autorização judicial ao posicionamento geográfico do suspeito: o caso Carpenter United States

Recente e importante caso julgado pela Suprema Corte Americana cuida da obtenção de dados geográficos sobre a localização do aparelho celular. Mais especificamente, trata-se de discussão em torno da possibilidade de aproveitamento do histórico de registros sobre a localização do telefone celular como fonte de prova. O debate da corte estadunidense questionou se haveria a necessidade de ordem judicial para a busca e apreensão de dados e informações sobre a movimentação física de determinada pessoa mediante as redes de telefonia celular.

No intuito de melhor compreensão da matéria, o Juiz Roberts relatou a situação da localização de dispositivos móveis nos EUA:

"Existem 396 milhões de contas de serviços de telefonia celular nos Estados Unidos - para uma nação de 326 milhões de pessoas. Os telefones celulares executam suas amplas e crescentes variedades de funções conectando-se a um conjunto de antenas de rádio chamado Estação Rádio Base (ERB) ou 'cell site'. Embora as ERB's sejam montadas em uma torre, elas também podem ser encontradas em postes de luz, nos mastros, nas torres de igrejas, ou nas laterais dos edifícios. As ERB's normalmente têm várias antenas direcionais que dividem a área coberta em setores. Celulares escaneiam continuamente seu ambiente procurando pelo melhor sinal, que geralmente vem da ERB mais próxima. A maioria dos dispositivos modernos, como os smartphones, acessam as redes de 'wireless' várias vezes por minuto, sempre que o sinal estiver ligado, mesmo que o proprietário não esteja utilizando um dos recursos do telefone. Cada vez que o telefone se conecta a uma ERB, gera um registro com data e hora conhecido como Localização pelo Local da Célula (CSLI). A precisão dessas informações depende do tamanho da área geográfica coberta pela ERB. Quanto maior a concentração de ERB's, menor a área de cobertura. Como o uso de dados de telefones celulares aumentou, as operadoras de telefonia móvel instalaram mais ERBs para lidar com o tráfego. Isso levou a áreas de cobertura cada vez mais compactas, especialmente em áreas urbanas.

As operadoras de telefonia móvel coletam e armazenam o CSLI para seus próprios fins comerciais, incluindo encontrar pontos fracos em sua rede e aplicar cobranças de 'roaming' quando outra operadora direciona os dados por meio de suas ERB's [...]" (Tradução nossa).[57]

Assim, nota-se que existem duas técnicas para a localização de dispositivos móveis celulares utilizadas nos Estados Unidos: a Informação da Localização pelo Local da Célula

(CSLI) – que se dá por meio da intensidade do sinal de transmissão entre o aparelho e a Estação Rádio Base (ERB) ou cell site – e o Sistema de Posicionamento Global (GPS).

O Caso Carpenter vs. Estados Unidos tratava de uma série de roubos praticados contra as lojas Radio Shack e T-Mobile em Michigan e Ohio. Entre os produtos do roubo, alguns celulares haviam sido subtraídos. No ano de 2011, um dos quatro suspeitos presos teria confessado o seu envolvimento nos delitos, identificado 15 cúmplices e fornecido o seu celular para os policiais checarem seu histórico de ligações na data do evento.

O FBI conseguiu apurar cerca de 16 ligações oriundas desse telefone para outros números perto do horário do roubo. Além disso, a polícia verificou que o telefone de Timothy Carpenter havia se comunicado com torres de celular no horário do crime, de modo a concluir que esse acusado se encontraria em local aproximadamente cerca de duas milhas das lojas roubadas e em horário compatível com o delito. Essa situação foi suficiente para se determinar a prisão e a acusação contra Carpenter, que acabou restando condenado a 100 anos de prisão. A sua apelação não foi provida, mantendo-se a condenação sob a fundamentação de que:

"[...] Carpenter não tinha uma expectativa razoável de privacidade acerca das informações de localização coletadas pelo FBI porque ele havia compartilhado essa informação com suas operadoras de telefonia celular. Dado que os usuários de telefones celulares transmitem voluntariamente os dados das ERB's para suas operadoras como 'um meio de estabelecer comunicação', a corte concluiu que os registros provenientes de negócios não têm direito à proteção da Quarta Emenda" (Tradução nossa).[58].

O caso chegou até a Suprema Corte dos Estados Unidos, a fim de questionar "[s]e a apreensão sem autorização e a busca de registros históricos de celulares revelando a localização e os movimentos de um usuário de celular ao longo de 127 dias é permitida pela Quarta Emenda" [59]. Ao discorrer sobre a Quarta Emenda, a Suprema Corte fundamentou algumas de suas diretrizes básicas: i) a garantia da "privacidade de vida" contra o "poder arbitrário"; ii) a necessidade que os legisladores tinham, à época, de "determinar obstáculos no caminho de uma vigilância policial muito permeável"[60].

Nesse sentido, o Tribunal reafirmou o seu entendimento exarado nos casos Kyllo e Riley, no intuito de rejeitar uma "interpretação mecânica" da Quarta Emenda, a fim de garantir a "[...] preservação desse grau de privacidade" e não deixar os sujeitos "à mercê do avanço da tecnologia" – a qual se desenvolveu exponencialmente nos últimos tempos. Ademais, o Juiz Roberts identificou que o caso em tela seria uma intersecção de dois conjuntos de precedentes sobre os quais a Corte já havia decidido: a expectativa de privacidade de uma pessoa sobre sua localização física e a ausência de expectativa legítima de privacidade de sujeito que realizou o voluntário compartilhamento a terceiros (por meio da aplicação da chamada third-party doctrine[61]). Por conseguinte, fundamentou a Corte:

"A questão que enfrentamos hoje é como aplicar a Quarta Emenda a um novo fenômeno: a capacidade de reconstruir os movimentos passados de uma pessoa através do registro de seus sinais de celular. [...] Ao mesmo tempo, o fato de o indivíduo continuamente revelar sua localização para sua operadora de telefonia móvel implica o princípio de terceira parte de Smith e Miller. Mas enquanto a doutrina de terceiros se aplica a números de telefone e registros bancários, não está claro se sua lógica se estende à categoria qualitativamente diferente de registros das ERB's" (Tradução nossa). [62]

Dessa maneira, o Tribunal entendeu que "[...] quando o governo rastreia a localização de um telefone celular, ele alcança uma vigilância quase perfeita, como se tivesse anexado um monitor de tornozelo ao usuário do telefone" [63] e, portanto, tratar-se-ia "[...] de uma reconstrução histórica detalhada da presença física de uma pessoa compilada todos os dias, a cada momento, ao longo de vários anos. Isso implica preocupações com a privacidade muito além daquelas consideradas em Smith e Miller."

[64], a configurar expressa violação do direito à privacidade. Nessa perspectiva, a Corte decidiu, majoritariamente, que, diferentemente dos casos anteriormente retratados, haveria a configuração de uma expectativa de privacidade diante de terceiras partes quando se tratarem de empresas de telefonia celular.

Por maioria, a Suprema Corte entendeu que a polícia precisava obter uma autorização judicial para proceder à busca dos registros geográficos que determinavam a localização do telefone. Tais dados foram obtidos de operadoras de celular e, tendo em vista que não haviam sido fornecidos consensualmente pelo acusado, mas sim mantidos por interesses comerciais pelas empresas, não poderiam ser obtidos pela polícia sem um mandado judicial[65].

Fundamentalmente, a aplicação das consequências desse caso acaba por determinar que as informações sobre ligações telefônicas e aparelhos celulares que se utilizaram da estação de rádio base (ERB's) devem ser precedidas de mandado judicial. O argumento que embasou a fundamentação da decisão majoritária tangenciou a imprescindibilidade de adaptação do Direito – no caso, da Quarta Emenda – diante dos avanços da ciência, no intuito de se evitar o acesso irrestrito de dados de informações de localização física pelo Estado e, portanto, preservar o direito fundamental à privacidade dos sujeitos.

Em suma, esse caso refletiu uma extensão do julgado no caso Riley vs. California, que determinou a impossibilidade de acesso sem autorização judicial ao conteúdo digital do celular. Recentemente, por conta do caso Carpenter vs. United States, a Suprema Corte Americana estendeu ainda mais a proteção de dados, indicando que as informações não podem ser obtidas de terceiros (empresas de telefonia celular) sem uma autorização judicial.

5 Nulla coactio sine lege: a atipicidade da coerção processual ausente mandado

Uma vez compreendidas as considerações supra aludidas concernentes ao direito fundamental à privacidade, nota-se uma importante característica. Em razão da inviolabilidade do direito fundamental, uma justificativa respaldada em lei e devidamente proporcional determinando os seus limites – processuais e materiais – faz-se imprescindível, sob pena de sua limitação configurar meramente uma lesão ou violação a tal direito. Com efeito, ausente previsão expressa acerca da licitude dessa intervenção ao direito fundamental, não há que se falar em compatibilidade da medida de coerção com o Estado Democrático de Direito.

Dessa sorte, Greco desenvolve a indispensabilidade do que conceitua ser o "fundamento legal"[66], qual seja, a norma autorizadora da intervenção do direito fundamental. Nesse sentido, com base na experiência da mudança advinda da Lei Fundamental alemã – a qual diferencia os direitos balizados pela "inviolabilidade" (unverletzlich) da "intocabilidade" da dignidade da pessoa humana e do conteúdo ontológico de um direito fundamental (Wesensgehalt) – o autor aponta a substancialidade da fundamentação legal prévia da intervenção do direito fundamental no direito processual penal, uma vez exigida tal reserva de lei. A propósito, consoante a matéria também se faz interessante observar o pacificado entendimento do Tribunal Constitucional Federal alemão a respeito da proteção da configuração privada da vida (tida, pois, como inviolável) em razão de sua contiguidade à dignidade humana.

Sob a mesma perspectiva, tem-se o que Moraes desenvolveu tangente à tipicidade das intervenções processuais – de sua aplicabilidade e de seu conteúdo referente aos direitos fundamentais –, à tradução do nulla coactio sine lege[67]. Bruzonne já havia alertado que, para ser utilizada uma medida de coerção ou ingerência, é preciso abordar a sua tipicidade processual. O autor apontou a necessidade de avaliar a sua aplicação partir dos passos que verificam sua: i) previsão em lei (nulla coactio sine lege); ii) competência do órgão que a dispõe; iii) necessidade; iv) idoneidade para o seu fim; iv) proporcionalidade, face aos interesses afetados[68]. O fato de não haver previsão sobre a autorização judicial para acessar informações do aparelho celular é o que justamente

embasa a impossibilidade de seu uso.

Dessarte, a tipicidade processual penal, ou seja, a "legalidade processual (constitucional) penal" [69], é exigida dos operadores jurídicos processuais tal e qual a previsão da legalidade para tipificação das condutas ilícitas é exigida no direito material. Isso se configura solidificado constitucionalmente, nos termos do art. 5º, II, da Constituição Federal (LGL\1988\3), que explicita que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". A conclusão pela atipicidade processual do acesso aos dados digitais de aparelho celular apreendido sem autorização judicial, pois configura-se, além de medida a ser evitada, de acordo com o direito comparado, processualmente atípica.

6.Conclusões

A era das novas tecnologias de informação modificou por completo a lógica de todas as dinâmicas sociais. Enquanto os avanços tecnológicos são exponenciais, o Direito peca na manutenção de legislações anacrônicas que demandam, como consequência, o exercício constante pelos magistrados de analogias – por muitas vezes descabidas para situações que não mais configuram da mesma maneira como eram no século passado. O processo penal, portanto, vê-se prontamente afetado, desde a fase de investigação até a execução.

Alguns ordenamentos jurídicos estão direcionando suas reformas processuais e/ou corpo jurisprudencial com atenção às demandas dessa adequação à realidade tecnológica que circunscreve nossa sociedade. A inovadora contribuição do Tribunal Constitucional Federal alemão quanto ao direito fundamental TI, bem como a legislação específica espanhola que dispõe acerca da necessidade de autorização judicial para acesso a dados de celulares são dois importantes exemplos.

No mesmo sentido, o Tribunal de Justiça da União Europeia identifica a urgência de alteração do direito interno e da preservação dos direitos fundamentais. No entanto, quanto ao ponto, é preciso observar a suscetibilidade à relativização da ingerência dos direitos fundamentais que podem ser desdobradas a partir da fundamentação que serve de base ao TJUE, qual seja, o princípio da proporcionalidade. Ainda, faz-se de extrema importância atentar ao corpo jurisprudencial da Suprema Corte dos Estados Unidos, o qual traz à baila imprescindíveis ponderações sobre a busca e apreensão de telefones celulares sem autorização judicial, bem como a obtenção dos metadados, respectivamente nos casos Riley vs. California e Carpenter vs. United States. A principal contribuição de tal corpo jurisprudencial diz respeito ao paralelo traçado entre os dados digitais e os físicos e a demonstração de que a busca e apreensão de um celular representa ingerência da privacidade muito maior do que uma busca e apreensão no domicílio. Isso porque tais aparelhos não mais se configuram como antigamente, mas se apresentam como verdadeiros "minicomputadores", multifuncionais, a disponibilizar informações sobre a vida privada que jamais seriam recolhidas em um lar.

No entanto, no ordenamento jurídico brasileiro, a busca e a apreensão são dois institutos que, apesar da previsão constitucional e convencional acerca da preservação dos direitos fundamentais, demonstram-se insuficientes para a regulação de todos esses direitos e garantias fundamentais interligados, já que permanecem atrelados à doutrina acrítica. Diante da ausência de previsão normativa a respeito do acesso da colheita de dados digitais de telefones celulares, o STF e o STJ vêm discutindo e proferindo entendimentos a respeito, e, tamanha a urgência e atualidade da temática que foi reconhecida a repercussão geral do Recurso Extraordinário com Agravo 1.042.075-RJ, caso que versa justamente acerca da licitude de prova obtida por meio de acesso a dados do telefone celular sem autorização judicial.

A razão pela qual o acesso a dados digitais de telefones celulares sem autorização judicial é manifestamente ilícita é simples e basilar para um devido processo dentro do espectro de um Estado Democrático de Direito: uma vez inexistente previsão expressa

da licitude da intervenção ao direito fundamental, não há compatibilidade da medida de coerção processual com um processo democrático e justo. A medida de coerção ou ingerência exige uma tipicidade processual penal, tal e qual se demanda a previsão da legalidade para tipificação das condutas ilícitas no direito material, conforme se pode interpretar do art. 5º, II, da Constituição Federal (LGL\1988\3). A previsão em lei (nulla coactio sine lege) é um dos principais passos para a identificação de tal tipicidade, o que não se identifica no ordenamento jurídico brasileiro.

Em suma, como referido e evidenciado pela análise doutrinária e jurisprudencial, a busca em telefones móveis, ausente autorização judicial, e consequente colheita de tais dados se evidencia como manifestamente ilícita. Essa proteção se estende aos casos de conteúdo extraído do celular como também aos metadados (e.g. obtenção da localização geográfica do suspeito com base nas ERB's). Portanto, espera-se que o julgamento do Recurso Extraordinário com Agravo 1.042.075-RJ, agendado para o dia 13 de março de 2019, direcione o entendimento do Supremo a uma interpretação que prime pela preservação dos direitos fundamentais, não se olvidando a imperiosa e urgente necessidade de adequação da própria legislação brasileira para responder às complicadas demandas de uma sociedade cuja era é completamente pautada pela tecnologia.

7.Referências

BRUZZONE, Gustavo. La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal. Estudios sobre Justicia Penal – Homenaje al Profesor Julio B. J. Maier. Buenos Aires: Editores del Puerto, 2005.

CASTELLS, Manuel. A sociedade em rede. Rio de Janeiro: Paz e Terra, 2009. v. 1.

DERY III, George M.; MEEHAN, Kevin. A new digital divide? Considering the implications of Riley v. California's warrant mandate for cell phone searches. Univ. of Pennsylvania Journal of Law and Social Change, v. 18.4, 2015.

EDITORIAL ESTADÃO. Brasil já tem mais de um smartphone ativo por habitante, diz estudo da FGV. 19 de abril de 2018. Disponível em: [https://link.estadao.com.br/noticias/geral,brasil-ja-tem-mais-de-um-smartphone-ativo-por-habitante-
Acesso em: 11.01.2019.

EDITORIAL G1. O celular ainda é o melhor meio para acessar o internet banking?. 24.01.2017. Disponível em: [http://g1.globo.com/tecnologia/blog/seguranca-digital/post/o-celular-ainda-e-o-melhor-meio-para-ace
Acesso em: 11.01.2019.

FELIX, Yuri; ROSA, Alexandre Morais da. Novas tecnologias de prova no processo penal: o DNA da delação premiada. Florianópolis: Empório do Direito, 2017.

FRIEDMAN, Barry. Unwarranted: policing without permission. New York: Farrar, Straus and Giroux, 2018.

GIACOMOLLI, Nereu José. O devido processo penal: abordagem conforme a CF (LGL\1988\3) e o Pacto de São José da Costa Rica. 3. ed. São Paulo: Atlas, 2016.

GLOECKNER, Ricardo Jacobsen. Autoritarismo e processo penal. Florianópolis: Tirant Lo Blanch, 2018.

GRECO, Luis. Introdução – O inviolável e o intocável no direito processual penal. São Paulo: Marcial Pons, 2018 (Coleção Direito Penal & Criminologia).

HOFFMANN-RIEM, Wolfgang. Innovaciones en la jurisprudencia del Tribunal Constitucional Alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la Sociedad de la Información. Direito Público. Porto Alegre, ano 12, n. 64, p. 40-61, jul.-ago. 2015.

MORAES, Maurício Zanoide de. Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial. Rio de Janeiro: Lumen Juris, 2012.

ORLANDI, Renzo. Usi investigativi dei cosiddetti captatori informatici. Criticità e Inadeguatezza di uma recente reforma. Revista Italiana di Diritto e Procedura Penale, 2018.

OZUROVICH, Kelly. Riley v. California – Cell phones and technology in the twenty-first century. Loy. L.A. L. Rev., v. 48, p. 507-524, 2015, Disponível em: [https://digitalcommons.lmu.edu/llr/vol48/iss2/8]. Acesso em: 11.01.2019.

PITOMBO, Cleunice Bastos. Da busca e apreensão no processo penal. 2. ed. São Paulo: Revista dos Tribunais, 2005.

PRADO, Geraldo. Prova penal e sistema de controles epistêmicos. São Paulo: Marcial Pons, 2015.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. Il mondo nella rete: quali i diritti, quali i vincoli. Bari: Laterza, 2014.

WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, 1890.

---

1 Declaramos que não há conflito de interesses que comprometa a cientificidade do trabalho apresentado.

2 Cf. GLOECKNER, Ricardo Jacobsen. Autoritarismo e processo penal. Florianópolis: Tirant Lo Blanch, 2018.

3 "Observa-se que os doutrinadores não demonstraram grande preocupação com o estudo da busca e apreensão. Inexiste monografia a respeito. Encontram-se, apenas, esparsos artigos em revistas especializadas; verbetes em dicionários e enciclopédias jurídicas; ou tratamento, inserido em cursos e manuais de processo penal" (PITOMBO, Cleunice Bastos. Da Busca e apreensão no processo penal. 2. ed. São Paulo: Revista dos Tribunais, 2005. p. 17). Muito embora tal afirmação tenha se dado há algum tempo, o tema continua rarefeito na doutrina.

4 PITOMBO, Cleunice Bastos. Da busca e apreensão no processo penal. 2. ed. São Paulo: Revista dos Tribunais, 2005. p. 103.

5 Para uma ampla abordagem sobre o sistema de proteção convencional no campo do processo penal, cf.: GIACOMOLLI, Nereu José. O devido processo penal: abordagem conforme a CF e o Pacto de São José da Costa Rica. 3. ed. São Paulo: Atlas, 2016.

6 Sobre a cadeia de custódia, que não consiste em objeto do presente artigo, cf.: PRADO, Geraldo. Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014. Cf. FELIX, Yuri; ROSA, Alexandre Morais da. Novas tecnologias de prova no processo penal: o DNA da delação premiada. Florianópolis: Empório do Direito, 2017.

7 FRIEDMAN, Barry. Unwarranted: policing without permission. New York: Farrar, Straus and Giroux, 2018.

8 ESTADOS UNIDOS. Suprema Corte. Caso Omstead vs. United States, 277, U.S 438.

Sentença de 04 de junho de 1928. Disponível em: [https://supreme.justia.com/cases/federal/us/277/438/]. Acesso em: 10.12.2018.

9 DERY III, George M.; MEEHAN, Kevin. A new digital divide? Considering the implications of Riley v. California's warrant mandate for cell phone searches. Univ. of Pennsylvania Journal of Law and Social Change, v. 18.4, 2015. p. 338.

10 ESTADOS UNIDOS. Suprema Corte. Caso Katz vs. United States, 389 U. S 347. Sentença de 18 de dezembro de1967. Disponível em: [https://supreme.justia.com/cases/federal/us/389/347/]. Acesso em: 10.12.2018.

11 Trata-se de caso no qual um sujeito foi preso e seu DNA extraído em consonância com uma lei do Estado de Maryland, que determina a extração compulsória de qualquer preso que tenha praticado crime com uso de violência (King tinha sido preso pelo crime de roubo). Subsequentemente, o seu DNA foi comparado com uma base de dados concernente às investigações em aberto (cold cases) no Estado. O seu DNA foi tratado como compatível com o material genético de um crime de estupro praticado seis anos atrás. King foi condenado pelo estupro.

12 FRIEDMAN, Barry. Unwarranted: policing without permission. New York: Farrar, Straus and Giroux, 2018. p. 274.

13 FRIEDMAN, Barry. Unwarranted: policing without permission. New York: Farrar, Straus and Giroux, 2018. p. 274.

14 Cf. CASTELLS, Manuel. A sociedade em rede. Rio de Janeiro: Paz e Terra, 2009. v. 1.

15 O termo portabilidade é utilizado na informática para sinalizar a capacidade de um sistema operacional ser compilado e executado em diversas arquiteturas, tanto de hardware como de software.

16 E que deu causa a exaustivas batalhas judiciais pelo acesso a informações dos utilitários do Twitter nos Estados Unidos, derivada dos casos de vazamento de informações por Snowden (FRIEDMAN, Barry. Unwarranted: policing without permission. New York: Farrar, Straus and Giroux, 2018. p. 236).

17 EDITORIAL G1. O celular ainda é o melhor meio para acessar o internet banking?. 24.01.2017. Disponível em: [http://g1.globo.com/tecnologia/blog/seguranca-digital/post/o-celular-ainda-e-o-melhor-meio-para-ace Acesso em: 11.01.2019.

18 WARREN, Samuel D; BRANDEIS, Louis D. The right to privacy. Harvard Law Review, v. 4, n. 5, 1890. p. 193-220.

19 RODOTÀ, Stefano. Il mondo nella rete: quali i diritti, quali i vincoli. Bari: Laterza, 2014. p. 129.

20 RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 129.

21 RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 129.

22 EDITORIAL ESTADÃO. Brasil já tem mais de um smartphone ativo por habitante, diz estudo da FGV. 19.04.2018. Disponível em: [https://link.estadao.com.br/noticias/geral,brasil-ja-tem-mais-de-um-smartphone-ativo-por-habitante- Acesso em: 11.01.2019.

23 "Le tecnologie informatiche oggi disponibili consentono di acquisire informazioni che vanno ben oltre lo spazio protetto dall'art. 15 cost., quello della comunicazione interpersonale. Come testé accennato, tramite esse è possibile osservare e controllare l'insieme delle relazioni sociali della persona presa di mira, le sue frequentazioni sul web, i frammenti della sua esperienza ricavabili da documenti scritti, fotografici, audio, video" (ORLANDI, Renzo. Usi investigativi dei cosiddetti captatori informatici. Criticità e Inadeguatezza di uma recente reforma. Revista Italiana di Diritto e Procedura Penale, 2018. p. 540).

24 In verbis: "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" (Superior Tribunal de Justiça. Recurso em Habeas Corpus 51.531-RO, da Sexta Turma, Rel. Ministro Nefi Cordeiro, j. 19.04.2016.

25 O Habeas Corpus 91.867-PA e o Mandado de Segurança 23.452-RJ são exemplos do entendimento adotado pelo STF no sentido de exclusão da reserva de jurisdição dos registros telefônicos, ou seja, do acesso aos registros de chamadas do telefone independer de autorização judicial.

26 "The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years" (ESTADOS UNIDOS. Suprema Corte. Caso Riley vs. California, 573 U.S. Sentença de 25 de junho de 2014. Disponível em: [https://supreme.justia.com/cases/federal/us/573/13-132/]. Acesso em: 10.12.2018.

27 Disponível em: [https://link.estadao.com.br/noticias/geral,brasil-ja-tem-mais-de-um-smartphone-ativo-por-habitante-
Acesso em 11.01.2019.

28 Cf. DERY III, George M.; MEEHAN, Kevin. A new digital divide? Considering the implications of Riley v. California's warrant mandate for cell phone searches. Univ. of Pennsylvania Journal of Law and Social Change, v. 18.4, 2015.

29 Tratava-se de um crime tipificado pelo art. 157, § 2º, incisos I e II, do Código Penal, cuja absolvição foi proferida em segunda instância, pela Sexta Câmara Criminal do Tribunal de Justiça do Rio de Janeiro em razão de prova obtida por meios ilícitos. O núcleo de fundamentação do presente recurso extraordinário com agravo conecta-se à possibilidade juridicamente válida e legítima de a autoridade policial, independentemente de autorização judicial, examinar dispositivo de telefone móvel, colhendo informações que reputar satisfatórias para empreender cursos de ação ações investigativas. Após a inadmissão do recurso extraordinário, o Ministério Público do Estado do Rio de Janeiro interpôs agravo, pretendendo ver examinada a questão de fundo, ligada ao exame dos artigos 5º, XII e LVI da Constituição da República. Dessa forma, o recurso interposto pelo Ministério Público trata do exame de constitucionalidade difusa das seguintes regras de natureza constitucional: a) 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; b) LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos.

30 A respeito desse caso, o Instituto Brasileiro de Ciências Criminais (IBCCRIM), o Instituto de Garantias Penais (IGP), o Artigo 19 Brasil e a Witness requereram a admissão no feito na qualidade de amici curiae. Ocorre que a decisão proferida pelo Ministro Dias Toffoli foi no sentido de indeferimento do pedido formulado pelo IBCCRIM,

por ausência de representatividade e de demonstração da "utilidade", bem como indeferimento do requerimento do IGP, do artigo 19 Brasil e da Witness, por ausência de cumprimento do requisito da "oportunidade".

31 HOFFMANN-RIEM, Wolfgang. Innovaciones en la jurisprudencia del Tribunal Constitucional alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la Sociedad de la Información. Direito Público, Porto Alegre, ano 12, n. 64, jul.-ago. 2015. p. 42.

32 HOFFMANN-RIEM, Wolfgang. Innovaciones en la jurisprudencia del Tribunal Constitucional alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la Sociedad de la Información. Direito Público, Porto Alegre, ano 12, n. 64, jul.-ago. 2015. p. 44.

33 HOFFMANN-RIEM, Wolfgang. Innovaciones en la jurisprudencia del Tribunal Constitucional alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la Sociedad de la Información. Direito Público, Porto Alegre, ano 12, n. 64, jul.-ago. 2015. p. 50.

34 ORLANDI, Renzo. Usi investigativi dei cosiddetti captatori informatici. Criticità e Inadeguatezza di uma recente reforma. Revista Italiana di Diritto e Procedura Penale, 2018, p. 541.

35 Chimel vs. California, 395 U. S. 752 (1969).

36 "When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. There is ample justification, therefore, for a search of the arrestee's person and the area 'within his immediate control' – construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence" (Chimel v. California, 395 U. S. 752 (1969) 762-763).

37 Nesse caso, Brima Wurie foi preso pela polícia sob a suspeita de prática de tráfico de drogas: a polícia procedeu à busca em dois celulares do preso, incluindo aí um celular de tecnologia mais antiga, pré-smartphone (flip phone). A polícia verificou que esse celular estava recebendo chamadas de um contato chamado "minha casa". Os policiais abriram o celular e identificaram o número correspondente ao contato "minha casa". E concluíram que se tratava do apartamento de Wurie. Após obter um mandado, encontraram no apartamento de Wurie drogas, dinheiro, munição e arma de fogo.

38 ESTADOS UNIDOS. Suprema Corte. Caso Brigham City vs. Stuart, 547 U. S. 398, 403, Sentença de 2006.

39 "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrong-doing, . . . reasonableness generally requires the obtaining of a judicial warrant" (ESTADOS UNIDOS. Suprema Corte. Vernonia School Dist. 47J vs. Acton, 515 U. S. 646, 653, sentença de 1995).

40 ESTADOS UNIDOS. Suprema Corte. Caso Johnson vs. United States, 333 U. S. 10, 14, sentença de 1948.

41 "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arrest ing officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone

and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one" (ESTADOS UNIDOS. Suprema Corte. Caso Riley vs. California, 573 U.S. Sentença de 25 de junho de 2014. Disponível em: [https://supreme.justia.com/cases/federal/us/573/13-132/]. Acesso em: 10.12.2018.

42 "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers" (ESTADOS UNIDOS. Suprema Corte. Caso Riley vs. California, 573 U.S. Sentença de 25 de junho de 2014. Disponível em: [https://supreme.justia.com/cases/federal/us/573/13-132/]. Acesso em: 10.12.2018.

43 "The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone" (ESTADOS UNIDOS. Suprema Corte. Caso Riley vs. California, 573 U.S. Sentença de 25 de junho de 2014. Disponível em: [https://supreme.justia.com/cases/federal/us/573/13-132/]. Acesso em: 10.12.2018).

44 "A cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form unless the phone is" (ESTADOS UNIDOS. Suprema Corte. Caso Riley vs. California, 573 U.S. Sentença de 25 de junho de 2014. Disponível em: [https://supreme.justia.com/cases/federal/us/573/13-132/]. Acesso em: 10.12.2018.

45 DERY III, George M.; MEEHAN, Kevin. A new digital divide? Considering the implications of Riley v. California's warrant mandate for cell phone searches. Univ. of Pennsylvania Journal of Law and Social Change, v. 18.4, 2015. p. 339.

46 OZUROVICH, Kelly. Riley v. California – Cell phones and technology in the twenty-first century. Loy. L.A. L. Rev., v. 48, , 2015. p. 519-523. Disponível em: [https://digitalcommons.lmu.edu/llr/vol48/iss2/8]. Acesso em: 11.01.2019.

47 A Ley Orgánica 13/2015 introduziu a reforma procesual na legislação espanhola e em seu preâmbulo dispôs: "Entre dichas cuestiones se encuentran el fortalecimiento de los derechos procesales de conformidad con las exigencias del Derecho de la Unión Europea y la regulación de las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución".

48 Cf. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

49 Importante observar alguns dos princípios listados pelo diploma, entre os quais destacam-se:

Princípio de limitação da coleta

7. A coleta de dados pessoais deveria ser limitada e qualquer desses dados deveria ser obtido através de mios legais e justos e, caso houver, informando e pedindo o consentimento do sujeito dos dados.

Princípio de limitação de utilização

10. Dados pessoais não deveriam ser divulgados, comunicados ou utilizados com finalidades ouras das que foram especificadas de acordo com o § 9, salvo

1. com o consentimento do sujeito dos dados

2. por força de lei

50 Esse acórdão diz respeito aos produtores de música da Espanha (Promusicae) contra a empresa de telefonia da Espanha SAL no que tange à divulgação de determinados dados de tráfego e os limites entre a obrigação de divulgação e a proteção da confidencialidade das comunicações eletrônicas. Ademais, também analisava questões de propriedade intelectual que não interessam à temática abordada. A decisão foi baseada no princípio da proporcionalidade, nos seguintes termos:

"[…] o direito comunitário exige que os referidos Estados, na transposição dessas diretivas, zelem por que seja seguida uma interpretação das mesmas que permita assegurar o justo equilíbrio entre os direitos fundamentais protegidos pela ordem jurídica comunitária. Seguidamente, na execução das medidas de transposição dessas diretivas, compete às autoridades e aos órgãos jurisdicionais dos Estados-Membros não só interpretar o seu direito nacional em conformidade com essas mesmas diretivas mas também seguir uma interpretação destas que não entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito comunitário, como o princípio da proporcionalidade" (Cf. Productores de Música de España (Promusicae) vs. Telefónica de España SAU, TJUE, Processo C-275/06, 29.01.2008).

51 A Digital Rights Ireland Ltd. (DRI) é uma sociedade comercial de responsabilidade limitada que tem como objeto estatutário a promoção e proteção dos direitos cíveis no universo das tecnologias de comunicação modernas. A DRI teve suas comunicações tratadas, conservadas e controladas ilegalmente pela autoridade irlandesa, de modo que a empresa solicitou a anulação dos atos de direito interno que possibilitavam às autoridades irlandesas impor aos fornecedores de serviços de telecomunicação a conservação dos dados de telecomunicação, uma vez que entendiam ser inconstitucional, assim como questiona a Diretiva 2006/24 com base na Carta dos Direitos Fundamentais. O Advogado-Geral concluiu que existe um "direito à vida privada relativamente ao tratamento de dados pessoais" uma vez que "[...] o direito proteção dos dados pessoais assenta no direito fundamental ao respeito pela vida privada (52), pelo que, como o Tribunal de Justiça teve oportunidade de salientar (53), os artigos 7° e 8° da Carta estão indissociavelmente relacionados (54) [...] […]72. Em qualquer caso, contudo, a recolha (63) e, sobretudo, a conservação (64), em gigantescas bases de dados, de múltiplos dados, gerados ou tratados no âmbito da maior parte das comunicações eletrónicas correntes dos cidadãos da União (65) constitui uma ingerência caracterizada na sua vida privada, embora estas criem apenas as condições que permitem um controlo retrospetivo das suas atividades pessoais e profissionais. A recolha destes dados cria as condições para uma vigilância que, apesar de destinada a ser exercida apenas retrospetivamente aquando da sua exploração, ameaça, no entanto, permanentemente, durante toda a duração do seu período de conservação, o direito dos cidadãos da União ao segredo das suas vidas privadas. O sentimento difuso de vigilância (66) gerado coloca de forma especialmente premente a questão da duração da conservação de dados. [...]".

52 Trata-se de um litígio que opõe M. Schrems ao Data Protection Comissioner em razão da sua recusa em investigar a queixa de Schrems sobre o Facebook Ireland Ltd. estar transferindo os dados pessoais dos seus utilizadores aos Estados Unidos e conservando em servidores desse país. A decisão do Tribunal de Justiça da União Europeia foi no seguinte sentido: "No que respeita ao nível de proteção das liberdades e direitos fundamentais garantido dentro da União, uma regulamentação dessa proteção que implique uma ingerência nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta deve, segundo a jurisprudência constante do Tribunal de Justiça, estabelecer regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados. A necessidade de dispor destas garantias é ainda mais importante quando os dados pessoais sejam sujeitos a tratamento automático e exista um risco significativo de acesso ilícito aos mesmos (acórdão Digital Rights Ireland e o., C□293/12 e C□594/12, EU:C:2014:238, n. 54 e 55 bem como jurisprudência aí referida)." Nesse sentido, o Tribunal de Justiça da União Europeia declarou: 1) O artigo 25º, n. 6, da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conforme alterada pelo Regulamento (CE) 1882/2003 do Parlamento Europeu e do Conselho, de 29 de setembro de 2003, lido à luz dos artigos 7º, 8º e 47º da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46 relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ), emitidos pelo Department of Commerce dos Estados Unidos da América, através da qual a Comissão Europeia constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado Membro, na aceção do artigo 28º desta diretiva, conforme alterada, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado.

53 Tratava-se de dois litígios. O primeiro dizia respeito à Tele2 Sverige AB e Post-och telestyrelsen (PTS – autoridade sueca de supervisão dos correios e telecomunicações) em razão da conservação dos dados de tráfego e dos dados de localização dos assinantes e utilizadores registrados, bem como de Tom Watson, Peter Brice e Geoffrey Lewis contra Secretary of State for the Home Department (Ministro da Administração Interna) concernente à conformidade com o direito da União da seção 1 do Data Retention and Investigatory Powers Act 2014 (DRIPA – Lei de 2014 sobre a conservação de dados e os poderes de investigação).

54 O caso se tratava de uma investigação sobre um crime de roubo de uma carteira e de um celular em que a solicitação da concessão do acesso a dados pessoais do titular da linha telefônica havia sido indeferida pelo juiz de instrução, cuja fundamentação foi baseada no fato de não se tratar de uma infração "grave" (qual seja, na legislação espanhola, punível com pena-prisão superior a 5 anos). Nesse sentido, o Ministério Fiscal Público espanhol interpôs recurso para a Audiência Provincial de Tarragona, Espanha.

55 UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Digital Rights Ireland e Seitlinger e o, sentença de 8 de abril de 2014.

56 Tribunal de Justiça da União Europeia. Digital Rights Ireland e Seitlinger e o, 8 de abril de 2014. (117).

57 "There are 396 million cell phone service accounts in the United States – for a Nation

of 326 million people. Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called 'cell sites'. Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors. Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas. Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites [...]" (ESTADOS UNIDOS. Suprema Corte. Caso Carpenter vs. United States, 585 U.S. Sentença de 22 de junho de 2018. Disponível em: [https://supreme.justia.com/cases/federal/us/585/16-402/]. Acesso em: 10.12.2018.

58 "[…] Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers. Given that cell phone users voluntarily convey cell-site data to their carriers as "a means of establishing communication," the court concluded that the resulting business records are not entitled to Fourth Amendment protection" (ESTADOS UNIDOS. Suprema Corte. Caso Carpenter vs. United States, 585 U.S. Sentença de 22 de junho de 2018. Disponível em: [https://supreme.justia.com/cases/federal/us/585/16-402/]. Acesso em: 10.12.2018.

59 "Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment" (ESTADOS UNIDOS. Suprema Corte. Caso Carpenter vs. United States, 585 U.S. Sentença de 22 de junho de 2018. Disponível em: [https://supreme.justia.com/cases/federal/us/585/16-402/]. Acesso em: 10.12.2018.

60 ESTADOS UNIDOS. Suprema Corte. Caso Carpenter vs. United States, 585 U.S. Sentença de 22 de junho de 2018. Disponível em: [https://supreme.justia.com/cases/federal/us/585/16-402/]. Acesso em: 10.12.2018.

61 Basicamente, se alguém fornecesse consensualmente seus dados a um terceiro não poderia fazer uso da alegação de violação à privacidade.

62 "The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. […] At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of Smith and Miller. But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records" (ESTADOS UNIDOS. Suprema Corte. Caso Carpenter vs. United States, 585 U.S. Sentença de 22 de junho de 2018. Disponível em: [https://supreme.justia.com/cases/federal/us/585/16-402/]. Acesso em: 10.12.2018.

63 "[…] 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" (ESTADOS UNIDOS. Suprema Corte. Caso Carpenter vs. United States, 585 U.S. Sentença de 22 de junho de 2018. Disponível em: [https://supreme.justia.com/cases/federal/us/585/16-402/]. Acesso em: 10.12.2018.

64 "It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. uch a chronicle implicates privacy concerns far beyond those considered in Smith and Miller" (ESTADOS UNIDOS. Suprema Corte. Caso Carpenter vs. United States, 585 U.S. Sentença de 22 de junho de 2018. Disponível em: [https://supreme.justia.com/cases/federal/us/585/16-402/]. Acesso em: 10.12.2018.

65 ESTADOS UNIDOS. Suprema Corte. Caso Carpenter vs. United States, 585 U.S. Sentença de 22 de junho de 2018. Disponível em: [https://supreme.justia.com/cases/federal/us/585/16-402/]. Acesso em: 10.12.2018.

66 GRECO, Luis. Introdução – O inviolável e o intocável no direito processual penal. São Paulo: Marcial Pons, 2018 (Coleção Direito Penal & Criminologia). p. 32-33.

67 MORAES, Maurício Zanoide de. Presunção de inocência no processo penal brasileiro: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial . Rio de Janeiro: Lumen Juris, 2012. p. 315-316.

68 BRUZZONE, Gustavo. La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal. Estudios sobre Justicia Penal – Homenaje al Profesor Julio B. J. Maier. Buenos Aires: Editores del Puerto, 2005. p. 251-253.

69 PRADO, Geraldo. Prova penal e sistema de controles epistêmicos. São Paulo: Marcial Pons, 2015. p. 63.