DIREITO FUNDAMENTAL DA PRIVACIDADE E DA PROTEÇÃO DE DADOS EM FACE DA PRÁTICA DE CRIMES

Lucas Mikael Reys Oliveira (IC) e Fabiano Augusto Petean (Orientador)

Apoio: PIVIC Mackenzie

RESUMO

O presente artigo visa analisar o direito fundamental da privacidade, em específico dos dados pessoais referentes a conversas em aplicativos de telefonia celular, em face do avanço tecnológico, sendo este aparato tecnológico uma importante ferramenta na prática de crimes. Para isso foi feita uma análise do arcabouço constitucional, das leis infraconstitucionais referentes aos dados pessoais e internet, da lei de interceptação telefônica e da jurisprudência dos tribunais superiores, com a sua adequação à realidade fática e jurídica atual, segundo o método dialético. Conclui-se que a legislação pátria atual carece de técnica legislativa para quanto ao tratamento de dados pessoais de comunicações em aplicativos celulares, tanto no Marco Civil, quanto na Lei Geral de Proteção de Dados, e apesar da Lei de Interceptações Telefônica se aplicar ao casuístico, a mesma carece de um dispositivo específico e atualizado à realidade tecnológica atual, visto que é uma lei antiga, não obstante tais dados possuírem proteção constitucional, com uma jurisprudência conflitante nos tribunais superiores, causando grande insegurança jurídica aos operadores do Direito, sendo necessário um dispositivo legal que trate com a devida especificidade e técnica, para que se faça possível a proteção integral do direito fundamental frente à persecução penal, com um maior amadurecimento da legislação que versa sobre o tratamento de dados e internet.

Palavras-chave: Tratamento de Dados Pessoais, Interceptação Telefônica, Direito à Privacidade

ABSTRACT

This article aims to analyze the fundamental right to privacy, in particular personal data relating to conversations in mobile phone applications, in the face of technological advancement, this technological apparatus being an important tool in the practice of crimes. For this, an analysis was made of the constitutional framework, the infra-constitutional laws regarding personal data and the internet, the law of telephone interception and the jurisprudence of the superior courts, with its adequacy to the current factual and legal reality, according to the dialectical method. It is concluded that the current national legislation lacks legislative technique for the treatment of personal data of communications in mobile applications, both in the Marco Civil and in the General Data Protection Law, and despite the Telephone Interception Law applying to the casuistic , it lacks a specific device and being updated to the current technological reality, since it is an old law, despite such data having constitutional protection, with a conflicting jurisprudence in the superior courts, causing great legal uncertainty to the operators of the Law, being necessary a legal device that deals with the due specificity and technique, so that the full protection of the fundamental right against criminal prosecution is possible, with a greater maturity of the legislation that deals with the processing of data and the internet.

Keywords: Personal Data Protection, Telephone Interception, Right to Privacy.

1. INTRODUÇÃO

A marcha inexorável do avanço tecnológico propositado pelo domínio da técnica pelo homem acarreta mudanças que assolam todas as bases da sociedade no percorrer de sua trajetória histórica, capaz de trazer tanto impactos positivos como negativos ao convívio social.

Tratando-se de um fato que deve ser aceito como condição básica, *conditio sine qua non*, para fazer uma análise integral e eficiente da realidade contemporânea, de suma importância para os estudos jurídicos, de acordo com os paradigmas legais que entram em conflito com a vivência pragmática, precisando ser compreendido em sua totalidade. Baseando-se na Teoria Tridimensional do Direito do ilustre jurista Miguel Reale, em combinar os elementos Fato, Valor e Norma, ao entender a ciência do Direito como estrutura social necessariamente axiológico-normativa (GONZAGA e ROQUE, 2017), uma junção das três dimensões como essenciais ao Direito. Mister é a análise da realidade fática, se tratando, na definição da teoria explicitada, de todas as circunstâncias que rodeiam o ser humano, decorrendo da natureza ou do agir humano, e gerando consequências que influenciam outras ações humanas, em maior ou menor intensidade (REALE, 1999). Para que esse fato seja valorado, e posteriormente normatizado.

Tamanha é a importância e expansão do uso dos *smartphones* na vida cotidiana, que autores consideram o mesmo como uma espécie de “extensão” do corpo humano, produtor de novas sensorialidades e técnicas corporais, criando linguagens próprias para o seu manuseio, afetando-o e sendo afetado pelas tecnologias. Para Erthal:

> O corpo, em suas relações de acoplagem com as novas tecnologias de comunicação, especialmente nesse estudo, com o aparelho de telefone celular, conquistou poderes ubíquos de conectividade perpétua. Ele desenvolve outras linguagens próprias para manuseio de cada aparato, afetando-o e sendo afetado por ele. Constantemente exposto às novas tecnologias, tendo que se adequar a elas como se fosse quase uma imposição, o corpo sente e produz afetação nas novas tecnologias, cujas utilizações e funcionalidades vêm sendo ditadas pelas novas demandas e efemeridades do homem na pós-modernidade. (ERTHAL, 2007):

Segundo dados do IBGE (2019), 82,7% dos domicílios brasileiros possuía acesso à internet em 2019, sendo que 98,6% dos brasileiros com 10 anos ou mais de idade que acessam à internet, a acessam por meio de celulares.

Tais impactos podem ser percebidos em todos os campos da vida contemporânea, e o Direito, a prática forense e a criminalidade não fogem a essa realidade. Com o incessante avanço tecnológico, a criminalidade (como fática consequencial do avanço tecnológico)

avança e cria novas maneiras de se proliferar perante o uso e desenvolvimento dessas técnicas tecnológicas.

Os aparelhos de telefonia móvel, a tecnologia que se tornou a mais presente no convívio diário desde a sua implementação e uso difundido, totem moderno da chamada “era da informação” (JAMIL e NEVES, 2000), cunhada por autores como uma espécie de nova revolução industrial (DRUCKER, 2000), criou novos paradigmas na legislação pátria, visto o conflito de interesses entre o mercado de dados, a necessidade de proteção desses dados informáticos pessoais, o direito fundamental da privacidade e a prática de crimes, tanto abusando de tal direito, como ferindo-o. O uso cotidiano da internet é de tal forma expressivo que é considerado por autores como condição básica para a vida diária. Para Vaz (2008) “Não saber usar a internet em um futuro próximo será como não saber abrir um livro ou acender um fogão, não sabermos algo que nos permita viver a cidadania na sua completitude”.

Acerca do caráter revolucionário do meio digital, Drucker cita o comércio eletrônico como alavanca nesse processo. Comércio esse amplamente permeado de golpes e fraudes eletrônicas, crimes contra o patrimônio.

> O comércio eletrônico representa para a Revolução da Informação o que a ferrovia foi para a Revolução Industrial; um avanço totalmente inusitado, inesperado. E, como a ferrovia de 170 anos atrás, o comércio eletrônico está gerando um ‘boom’ novo e distinto, provocando transformações aceleradas na economia, na sociedade e na política. (DRUCKER, 2000):

Destarte os celulares poderem ser considerados como facilitadores da vida privada e profissional, criminosos utilizam desse meio para a prática de crimes, e desenvolvimento de suas atividades em organizações criminosas, o que torna a sua instrumentalidade de suma importância na investigação criminal e persecução penal.

Dados demonstram a proliferação do uso tecnológico no país pelo crime, pesquisa da empresa de *software* antivírus Norton (2010) revela o Brasil como o terceiro país com mais dispositivos infectados por ameaças, trazendo uma estimativa de que cerca de 71 milhões de brasileiros sofreram ataques cibernéticos nos últimos 12 meses, com a estimativa do impacto financeiro do gasto de 32 bilhões de reais decorrentes. Sendo que o relatório indica o Brasil como *hotspot* de crimes cibernéticos, em qual 76% dos adultos vivenciaram crimes desta espécie.

A título de exemplo, podem ser citados os delitos de fraudes eletrônicas, modalidade qualificada do tipo-crime estelionato (art. 171, § 2º-A), furto eletrônico qualificado (art. 155, §

4º-B), o novel tipo penal de invasão de dispositivo informático trazido pela Lei n. 12.737 de 2012, todos alterados pela Lei n. 14.155 de 2021, todos no Código Penal.

A doutrina moderna classifica os crimes digitais como Puros, Mistos e Comuns, segundo a classificação proposta por Mario Furlaneto Neto e José Augusto Chaves Guimarães (NETO E GUIMARÃES, 2003). Os crimes cibernéticos puros são aqueles em que a conduta delitiva fere o sistema informático direta e primariamente (art. 155, § 4º-B). Nos cibercrimes mistos, o sujeito ativo utiliza o sistema informático como meio essencial de consumação da conduta criminosa, como exemplo dos crimes de pedofilia previstos no Estatuto da Criança e do Adolescente, art. 241-A. Para os crimes informáticos comuns, a internet é apenas um meio de execução de um delito que se encontra previsto na lei penal de forma genérica. Ainda há a classificação de crimes cibernéticos Próprios e Impróprios, onde os próprios são aqueles em que o bem jurídico tutelado primariamente é o referido sistema, e nos impróprios o sistema informático não é o principal bem jurídico protegido pelo tipo penal.

Além das inovações legislativas e tipos específicos destinados a tutelar as relações virtuais informáticas, outros delitos mais tradicionais também podem ser enquadrados tipicamente em suas ações nucleares pela prática criminosa no meio digital, como o tráfico de drogas nas modalidades de "importar, exportar, adquirir, vender, prescreve e ministra" do Art. 33, *caput* da Lei 11.343 de 2006 (com posterior apreensão e realização do exame pericial nos entorpecentes ou não, vide Supremo Tribunal Federal AgRg no HC 213.896, pois "*a mera ausência de apreensão da droga não autoriza a absolvição pelo delito de tráfico de drogas, sobretudo quando presentes nos autos provas robustas da prática do delito" (*AgRg no HC 213.896, Rel. Min. Gilmar Mendes, 2ª Turma, j. 16/05/2022*)*), associação para o tráfico (art. 35), financiamento e custeio (art. 36), o próprio desenvolvimento da prática delitiva em seio de organização criminosa através dos aplicativos de comunicação é capaz de se enquadrar tipicamente no art. 2º da Lei 12.850 de 2013, nos verbos nucleares "promover, constituir, financiar ou integrar".

É possível a incriminação daquele que usa dos aplicativos de comunicação como o *Whatsapp*, *Messenger* e e-mails pelo uso dessas ferramentas tecnológicas para o desenvolvimento de crimes, como exemplificado supra, não constituindo apenas meros atos preparatórios. Constituindo, inclusive, corpo de delito conforme os preceitos do art. 158 do Código de Processo Penal. Se torna de imprescindível debate o possível choque entre o direito fundamental da privacidade e a investigação criminal por meio de esses dispositivos tecnológicos, com a possibilidade de apreensão desses aparelhos e posterior checagem de dados como meio lícito e legítimo de produção probatória, para que se faça possível a persecução penal, efetivação da justiça e desmantelamento das atividades de organizações criminosas.

2. DESENVOLVIMENTO DO ARGUMENTO

A Constituição Federal consagra em seu rol de direitos fundamentais o direito à intimidade e privacidade no art. 5º, X, e a inviolabilidade de comunicações telefônicas no inciso XII. Os dados provenientes de conversas de aplicativos celulares estão abrangidos pela proteção à intimidade e à privacidade do inciso X, juntamente com a inviolabilidade de comunicações e dados do inciso XII[1].

A proteção aos dados pessoais, inclusive nos meios digitais, foi incluída no rol dos direitos fundamentais pela Emenda Constitucional número 115, de 2022, no inciso LXXIX do art. 5º. Novidade que é bem-intencionada pelo legislador, que decidiu dar tratamento específico no rol do art. 5º aos dados pessoais, entretanto, tal condição fundamental dos dados já se encontrava abrangida dentro do direito à privacidade do inciso X[2].

Muito embora os dados telefônicos de conversas de aplicativos celulares estarem protegidos pelas normas fundamentais, tais normas não possuem caráter absoluto, visto o possível choque entre demais direitos fundamentais. Figurando, inclusive, como uma modalidade de princípio hermenêutico da Constituição, o princípio da concordância prática ou Harmonização, que consiste em coordenar e combinar os bens jurídicos em conflito, realizando uma redução proporcional de ambos, para que não se sacrifique um deles integralmente, devido ao seu caráter fundamental, mas sim reduzir proporcionalmente o âmbito de aplicação de cada um deles, para que convivam harmonicamente no sistema jurídico.

Acerca do caráter não absoluto dos Direitos Fundamentais, segundo a teoria da relatividade, Padilha leciona que o exercício dessas prerrogativas constitucionais não pode ser danoso à ordem pública e aos demais direitos e garantias fundamentais:

> Alguns doutrinadores sustentam, como mais uma caraterística, a relatividade dos direitos fundamentais sob o argumento de que não existe direito fundamental absoluto. Esse foi o entendimento que o STF firmou no MS 23.452 (Rel. Celso de Mello, DJ. 12.05.2000), em que afirma que, com base no princípio da convivência entre liberdades, nenhuma prerrogativa pode ser exercida de modo danoso à ordem pública e aos direitos e garantias

[1] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação
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;

[2] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais

> fundamentais, os quais sofrem limitações de ordem ético-jurídica. É certo que podem existir restrições a direitos fundamentais, mas isso somente ocorrerá por disposição expressamente constitucional (restrição imediata), e.g., art. 5.º, XI e XII, ou por meio de lei ordinária promulgada com fundamento imediato na própria Constituição (restrição mediata), v.g., art. 5.º, LVIII. (PADILHA, 2019).

Assim, sendo os celulares ferramentas utilizadas nas práticas delitivas, fica claro que é possível uma redução proporcional da regra contida nos incisos X, XII e LXXIX do art. 5º. Ainda mais se observada a disposição da última parte do inciso XII, onde o sigilo das comunicações telefônicas poderá ser afastado por ordem judicial devidamente fundamentada, uma norma constitucional de eficácia contida, restringível ou redutível, em que a sua aplicabilidade é não-integral, em que sua própria redação constitucional permite uma redução de sua extensão por ato superveniente do Poder Público, e possui regulação na Lei 9.296 de 1996, a lei que dispõe sobre as interceptações telefônicas e telemáticas.

Moraes ressalta o caráter não absoluto do referido direito, e reforça que as interceptações são possíveis sempre que tais dados estejam sendo utilizados como instrumento de salvaguarda à prática ilícita, desde que respeitados os parâmetros constitucionais:

> 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. Ocorre, porém, que apesar de a exceção constitucional expressa referir-se somente à interceptação telefônica, entende-se que nenhuma liberdade individual é absoluta, sendo possível, respeitados certos parâmetros, a interceptação das correspondências e comunicações telegráficas e de dados sempre que as liberdades públicas estiverem sendo utilizadas como instrumento de salvaguarda de práticas ilícitas. (MORAES, 2021)

O arcabouço constitucional permite a interceptação das comunicações telefônicas, aqui inclusos os dados de conversas de aplicativos em celulares e afins, sempre que houver ordem judicial expressa nesse sentido, princípio da reserva de jurisdição, pois não é razoável que os direitos fundamentais sejam salvos-condutos para o crime e danifiquem a ordem social e jurídica, em um Estado Democrático de Direito.

Para o Supremo Tribunal Federal e o Superior Tribunal de Justiça, é imprescindível o cumprimento da cláusula de reserva de jurisdição, ou seja, toda interceptação telefônica deve ser submetida à fulcro do Poder Judiciário, que decidirá motivadamente em decisão

fundamentada, sob pena de nulidade e ilicitude das provas obtidas sem o devido cumprimento legal, como foi decidido nos precedentes HC 168.052/SP do Supremo Tribunal Federal, RHC 89.981/MG e RHC 51.531/RO do Superior Tribunal de Justiça. Precedentes estes que tratam de conversas de *WhatsApp* em provas penais, no RHC 51.531/RO, inclusive, o Superior Tribunal de Justiça equiparou as mensagens de texto às comunicações telefônicas. O Superior Tribunal de Justiça no RHC 89.981/MG, de relatoria do Ministro Reynaldo Soares da Fonseca: "*a análise dos dados armazenados nas conversas de WhatsApp, revela manifesta violação da garantia constitucional à intimidade e à vida privada, razão pela qual se revela imprescindível a autorização judicial*" (RHC 89.981/MG, Rel. Min. Reynaldo Soares da Fonseca, 5ª Turma, DJe 13.12.2017).

Ainda sobre a necessidade da submissão ao Juiz, o Superior Tribunal de Justiça decidiu no julgamento do recurso RHC 75.800/PR, de relatoria do Ministro Felix Richter, que a ordem judicial de medida de busca e apreensão torna lícito o acesso aos dados de mensagens, sem necessidade de se atender aos requisitos da Lei de Interceptações, e outra ordem judicial, por haver uma pressuposição do acesso aos dados que neles estejam armazenados na ordem de apreensão de aparelho celular ou smartphone, sob pena da busca e apreensão resultar em medida írrita. Decidindo também que tais dados não se submetem aos ditames da referida Lei. Visto isto, segue a ementa da decisão:

> PROCESSUAL PENAL. OPERAÇÃO "LAVA-JATO". MANDADO DE BUSCA E APREENSÃO. APREENSÃO DE APARELHOS DE TELEFONE CELULAR. LEI 9296/96.
> OFENSA AO ART. 5º, XII, DA CONSTITUIÇÃO FEDERAL. INOCORRÊNCIA.
> DECISÃO FUNDAMENTADA QUE NÃO SE SUBORDINA AOS DITAMES DA LEI 9296/96. ACESSO AO CONTEÚDO DE MENSAGENS ARQUIVADAS NO APARELHO. POSSIBILIDADE. LICITUDE DA PROVA. RECURSO DESPROVIDO.
> I - A obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei 9296/96.
> II - O acesso ao conteúdo armazenado em telefone celular ou smartphone, quando determinada judicialmente a busca e apreensão destes aparelhos, não ofende o art. 5º, inciso XII, da Constituição da República, porquanto o sigilo a que se refere o aludido preceito constitucional é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos.
> III - Não há nulidade quando a decisão que determina a busca e apreensão está suficientemente fundamentada, como ocorre na espécie.
> IV - Na pressuposição da ordem de apreensão de aparelho celular ou smartphone está o acesso aos dados que neles estejam armazenados, sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal.
> V - Hipótese em que, demais disso, a decisão judicial expressamente

> determinou o acesso aos dados armazenados nos aparelhos eventualmente apreendidos, robustecendo o alvitre quanto à licitude da prova. Recurso desprovido.
> (RHC 75.800/PR, Rel. Ministro FELIX FISCHER, QUINTA TURMA, julgado em 15/09/2016, DJe 26/09/2016).

Interessante ressaltar que a jurisprudência dos Tribunais Superiores e a doutrina excepciona o sigilo nos *registros telefônicos* das *comunicações telefônicas*, afastando assim a cláusula de reserva de jurisdição, assim como também excepciona os dados cadastrais. Tais registros consistem em ligações armazenadas e documentadas, e listas de contatos dos telefones, sem os dados e comunicações em si. Hipótese em que não há a necessidade de autorização, e tais registros podem ser verificados prontamente, por forças policiais em situação de flagrância por exemplo, constituindo prova lícita e legal. Situação essa idêntica à do precedente do Supremo Tribunal Federal para tais registros, o HC 91.867/PA, em que se firmou entendimento de que não se confunde a comunicação telefônica e registros telefônicos, não se podendo "*interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados*" (HC 91867, Relator(a): GILMAR MENDES, Segunda Turma, julgado em 24/04/2012, ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012). Para Uadi Lammêgo Bulos:

> O sigilo telefônico pode ser rompido por ordem judicial. Aliás, o sigilo telefônico não se confunde com o sigilo dos *registros telefônicos*. Estes, que não se sujeitam ao princípio da reserva de jurisdição (CF, art. 5º, XII), equivalem às ligações armazenadas e documentadas nas companhias telefônicas. Numa palavra, designam telefonemas feitos no passado, os quais se encontram registrados nos bancos de dados dessas companhias. (BULOS, 2021).

O Supremo Tribunal Federal, no julgamento do HC 91.867/PA também firmou entendimento de que a Polícia agiu corretamente segundo o seu dever expresso de proceder à coleta de material probatório de indícios de materialidade e autoria criminosa, assim como com a discricionariedade de sua atuação e de suas medidas investigativas contidas no art. 6º do Código de Processo Penal, cumprindo as suas atribuições constitucionais previstas no art. 144 da Constituição Federal:

HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA. 1. Inépcia da denúncia. Improcedência. Preenchimento dos requisitos do art. 41 do CPP. A denúncia narra, de forma pormenorizada, os fatos e as circunstâncias. Pretensas omissões – nomes completos de outras vítimas, relacionadas a fatos que não constituem objeto da imputação –- não importam em prejuízo à defesa. 2. Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corréu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação.[3] 2.4 À guisa de mera argumentação, mesmo que se pudesse reputar a prova produzida como ilícita e as demais, ilícitas por derivação, nos termos da teoria dos frutos da árvore venenosa (fruit of the poisonous tree), é certo que, ainda assim, melhor sorte não assistiria à defesa. É que, na hipótese, não há que se falar em prova ilícita por derivação. Nos termos da teoria da descoberta inevitável, construída pela Suprema Corte norte-americana no caso Nix x Williams (1984), o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado. Bases desse entendimento que parecem ter encontrado guarida no ordenamento jurídico pátrio com o advento da Lei 11.690/2008, que deu nova redação ao art. 157 do CPP, em especial o seu § 2º. 3. Ilicitude da prova das interceptações telefônicas de conversas dos acusados com advogados, ao argumento de que essas gravações ofenderiam o disposto no art. 7º, II, da Lei n. 8.906/96, que garante o sigilo dessas conversas. 3.1 Nos termos do art. 7º, II, da Lei 8.906/94, o Estatuto da Advocacia garante ao advogado a inviolabilidade de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, eletrônica, telefônica e telemática, desde que relativas ao exercício da advocacia. 3.2 Na hipótese, o magistrado de primeiro grau, por reputar necessária a realização da prova, determinou, de forma fundamentada, a interceptação telefônica direcionada às pessoas investigadas, não tendo, em momento algum, ordenado a devassa das linhas telefônicas dos advogados dos pacientes. Mitigação que pode, eventualmente, burlar a proteção jurídica. 3.3 Sucede que, no curso da execução da medida, os diálogos travados entre o paciente e o advogado do corréu acabaram, de maneira automática, interceptados, aliás, como qualquer outra conversa direcionada ao ramal do paciente. Inexistência, no caso, de relação jurídica cliente-advogado. 3.4 Não cabe aos policiais

[3] Grifo do autor.

> executores da medida proceder a uma espécie de filtragem das escutas interceptadas. A impossibilidade desse filtro atua, inclusive, como verdadeira garantia ao cidadão, porquanto retira da esfera de arbítrio da polícia escolher o que é ou não conveniente ser interceptado e gravado. Valoração, e eventual exclusão, que cabe ao magistrado a quem a prova é dirigida. 4. Ordem denegada. (HC 91867, Relator(a): GILMAR MENDES, Segunda Turma, julgado em 24/04/2012, ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012).

Outros julgados interessantes que excepcionam o sigilo e nulidade da checagem dos dados são o HC 481.071/SC do Superior Tribunal de Justiça em que a entrega do aparelho celular, fornecimento de senha e anuência do investigado para os agentes policiais afasta a nulidade da coleta probatória ali realizada. O RHC 86.076/MT, também do Superior Tribunal de Justiça, onde foi decidido que não havia ilegalidade na perícia realizada pela polícia no celular da vítima que foi morta, tendo o seu telefone sido entregue por sua esposa, não havendo assim "*mais sigilo algum a proteger do titular daquele direito"* (RHC 86.076/MT, Rel. Ministro SEBASTIÃO REIS JÚNIOR, Rel. p/ Acórdão Ministro ROGERIO SCHIETTI CRUZ, SEXTA TURMA, julgado em 19/10/2017, DJe 12/12/2017). O HC 546.830/PR do Superior Tribunal de Justiça retirou o sigilo quando o aparelho for apreendido em interior de estabelecimento prisional, sem a necessidade de autorização judicial para tanto.

Os RHC 99.735 e RHC 79.848 do Superior Tribunal de Justiça caminham em sentido contrário, declarando a nulidade de provas obtidas por intermédio do espelhamento do *WhatsApp*, modalidade em que se acessa o aplicativo por meio de computador, o *WhatsApp Web*, pela ferramenta permitir o envio de novas mensagens a exclusão de mensagens antigas ou recentes, sendo que eventual exclusão não deixa vestígio no aplicativo ou no computador, de forma a inviabilizar a presunção relativa do princípio da presunção de legitimidade dos atos praticados por servidores públicos (os policiais no caso), tornando a presunção em absoluta, pois nos julgados a possibilidade de devassidão das mensagens pelos agentes públicos foi o argumento utilizado pelos ministros para invalidar a licitude do meio de produção probatória. Para Renato Brasileiro, o entendimento é acertado, pois a contraprova seria uma "prova diabólica", pois a exclusão de mensagens não deixaria vestígios nem para o usuário nem para o destinatário (LIMA, 2020), porém, segundo a devida vênia, essa é uma situação que não se verifica, porque a exclusão de mensagens deixa vestígios para ambos os usuários, pois há duas modalidades de exclusão de mensagens, "apagar para todos" e "apagar para mim", quando na modalidade "apagar para todos", demonstrando que a mensagem foi apagada, e na modalidade "apagar para mim", somente no celular de um dos interlocutores as mensagens são apagadas. Com o princípio da igualdade das partes, da "paridade de armas", ambas as partes possuem igualdade no que tange à produção de material probante, ônus, e obrigações

e faculdades da defesa e acusação, assim como as suas provas têm igual valor perante o órgão julgador, e a parte contrária poderia demonstrar, segundo os vestígios em seu celular, que a autoridade pública agiu de maneira ilícita, devendo ser responsabilizada, não se tratando de "prova diabólica" com o referido princípio. Esta hipótese de nulidade poderia ser sanada com dispositivos legais que tratassem com maior técnica o uso de dados pessoais em processo penal.

Apesar de os dados pessoais de conversas em aplicativos celulares receberem proteção constitucional, não há um dispositivo infraconstitucional específico, uma lei específica, que regule a coleta e uso em processo penal desses dados, se aplicando a Lei 9.296 de 1996[4], Lei das Interceptações Telefônicas e Telemáticas, não havendo tratamento individual para esses dados nesta lei, apesar de a lei ditar que a mesma se aplica para a interceptação do "fluxo de comunicações em sistemas de informática e telemática". Como observado, há precedentes dos Tribunais Superiores que aplicam a lei a esses dados, e outros precedentes que afastam tal aplicação, causando grande insegurança jurídica aos atores processuais, principalmente forças policiais em atividade executiva de polícia judiciária, quanto ao tratamento desses dados em sede processual penal.

A problemática avança, pois, a Lei 9.296/96 erige critérios específicos para que seja possível a decretação de interceptações, além de ordem judicial devidamente fundamentada e motivada. Tais critérios estão descritos no art. 2º e seus incisos de forma excludente[5], exigem que haja indícios razoáveis de autoria ou participação em infração penal, II. a interceptação seja imprescindível à produção probatória, que não haja outros meios probatórios disponíveis, e III. que o fato investigado seja punido com, no mínimo, pena de detenção, assim como estabelece critérios temporais no art. 5º[6], com prazo máximo renovável de 15 dias. Os critérios se afiguram rígidos com a crescente expansão do uso dos aparelhos

[4] Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

[5] Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
I - não houver indícios razoáveis da autoria ou participação em infração penal;
II - a prova puder ser feita por outros meios disponíveis;
III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.
Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

[6] Art. 5° A decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova.

celulares em delitos, como explicitado anteriormente, havendo delitos que ocorrem puramente no meio informático.

Além de que é imprescindível anotar a criminalização daquele que realiza a interceptação telefônica, telemática ou informática sem autorização judicial ou com objetivos não autorizados em lei no art. 10[7], com a alteração trazida pela Lei 13.869/19 no Parágrafo Único[8], Lei de Abuso de Autoridade, que adicionou a incorrência específica para a autoridade judicial que determine a execução da medida com objetivo não autorizado em lei no parágrafo único do referido artigo. Com a ausência de disposição própria aos dados de conversas, fica sinuosa a tipicidade e antijuridicidade a ser avaliada na conduta da autoridade judicial que determina a medida para esses dados, causando ainda mais insegurança jurídica aos operadores do Direito.

No âmbito infraconstitucional, a Lei Geral de Proteção de Dados e o Marco Civil da Internet visam tutelar a proteção de dados pessoais e regular os princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

O Marco Civil da Internet elenca a inviolabilidade e sigilo do fluxo das comunicações pela internet no art. 7º, II e III, salvo por ordem judicial, bem como no art. 10, § 2º, erige novamente a necessidade de ordem judicial para que se faça possível a interceptação do conteúdo das comunicações privadas. Apesar de desprender tratamento mais específico a esses dados, a Lei 12.965/14 o faz de maneira geral, remetendo no art. 7º somente que a comunicação e fluxo são invioláveis[9], e ao estabelecer critérios no art. 10[10], o faz também como cláusula geral, prevendo a devida atenção à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas, sem estabelecer maior

[7] Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei: (Redação dada pela Lei nº 13.869. de 2019)
Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 13.869. de 2019)

[8] Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no caput deste artigo com objetivo não autorizado em lei. (Incluído pela Lei nº 13.869. de 2019)

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

[10] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

rigor como no art. 13 e seguintes que tratam da guarda de registros de conexão e acesso a aplicações, com hipóteses de requisição legal pela autoridade policial e Ministério Público.

A lei acerta ao fazer a distinção com critérios objetivos dos "registros" (aqui entendidos como dados cadastrais que informem qualificação pessoal, filiação e endereço) com a "comunicação" de fato, conforme a ausência de se submeter ao julgo da reserva de jurisdição, no § 3º do art. 10[11]. Nesse sentido:

> Dados são os cadastros e os registros de acesso (IP, data, hora e fuso horário) e não possuem proteção constitucional, podendo sua obtenção mediante ordem judicial ocorrer em qualquer caso de crimes ou contravenções, independentemente da pena. Já o conteúdo de conversações em e-mail, chats, postagens, etc. configura o objeto da proteção constitucional e só pode ser violado mediante ordem judicial nas hipóteses abrangidas pela Lei nº 9.296/96. (BARRETO e BRASIL, 2016).

Já a Lei Geral de Proteção de Dados exclui do seu âmbito de proteção os dados aqui discutidos, por se tratar de matéria relativa a fins exclusivos de segurança pública, atividades de investigação e repressão de infrações penais. A Lei Geral de Proteção de Dados é taxativa em seu art. 4º, I ao dizer que não se aplicará ao tratamento de dados: realizados por pessoa natural para fins exclusivamente particulares e não econômicos; e no inciso III itens "a, b, c e d", que não se aplicará para dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança de Estado e atividades de investigação e repressão de infrações penais. Essas limitações aqui explanadas se baseiam, segundo Pinheiro:

> A delimitação da aplicabilidade da lei em relação aos tipos de dados que são considerados regulados pela LGPD demonstra que o tratamento de dados pessoais deve seguir um propósito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado. Da mesma forma, o uso doméstico com fins não econômicos não recebe a aplicação da lei, tendo em vista que um dos focos de ação do dispositivo é regular as atividades cujo objetivo seja a oferta ou o fornecimento de bens ou serviços. Essa restrição do campo de alcance contribui para reduzir os impactos econômicos e sociais, visto que há elevados custos na implementação das exigências trazidas pela legislação de proteção de dados pessoais. Além disso, há sempre necessidade de equilibrar a proteção da privacidade (como um direito individual) e a proteção da segurança pública (como um direito coletivo), especialmente diante da

[11] § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

> obrigação de fortalecer o combate ao crime organizado, à fraude digital e ao terrorismo. (PINHEIRO, 2021):

Apesar dessa hipótese de exclusão legal também estar presente no tratamento de dados do direito comunitário europeu, no Regulamento Geral sobre a Proteção de Dados 2016/679 (General Data Protection Regulation (GDPR)) em seu art. 2º (2) d, e ser bem-vista por parte da doutrina específica (VAINZOF, 2019), o próprio autor ressalta a necessidade de amadurecimento mais profundo e gradual na alteração das leis já em vigor que regulam os dados pessoais, faltando um marco legal que verse sobre o tratamento de dados pessoais para fins de segurança pública.

> Em vez de criar um grande marco legal que também pudesse versar sobre as hipóteses legais em que se autorizariam o tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, o legislador preferiu excepcionar a aplicação da LGPD para as finalidades listadas, de forma correta, na perspectiva deste autor, diante da necessidade de um amadurecimento ainda mais profundo e gradual na eventual necessidade de alteração das legislações já em vigência que autorizam e limitam o tratamento de dados pessoais, sopesando segurança e privacidade, que devem sempre caminhar de mãos dadas. O GDPR também contempla exceção de sua aplicabilidade para tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Porém, com a diferença da edição na UE, de forma concomitante ao GDPR, da Diretiva 2016/680. (MALDONADO *et al.,* 2019).

Tal marco legal se figura de extrema importância atualmente, visto o conflito na jurisprudência dos Tribunais Superiores, a falta de critérios específicos na legislação do Marco Civil e Lei Geral de Proteção de Dados, a obsolescência e falta de dispositivo específico na Lei de Interceptações Telefônicas com a necessidade de se maturar a legislação pátria para que se possa haver a proteção integral do direito fundamental frente a persecução penal.

3. CONSIDERAÇÕES FINAIS

Há muitas lacunas e falta de proteção legal tanto para a atuação dos servidores de persecução penal, como para a efetivação do art. 5º da Constituição Federal. Sendo os celulares, com seus aplicativos de comunicação, importantes instrumentos para os agentes criminosos e o aumento da criminalidade digital (tendo unicamente o campo informático como possível cadeia de custódia), é necessário ter uma legislação que trate com maior rigor

técnico, não deixando somente de cláusula geral como na legislação atual, e não deixando somente ao campo jurisprudencial, que é conflitante e causa insegurança jurídica, para que seja adequada à realidade atual.

Apesar de a Lei de Interceptações telefônicas se aplicar ao caso, a mesma carece de dispositivo específico e atualizado à realidade tecnológica atual, visto que é uma lei datada de 1996, anterior a qualquer tecnologia de *smartphones*. Não restam dúvidas de que é necessária uma ordem judicial para que se faça o acesso aos dados, porém, isso não é o suficiente, sendo necessário maior rigor legislativo e adequação à realidade atual, com necessidade de um dispositivo próprio que trate desses dados na lei, e com as peculiaridades excludentes citadas pela jurisprudência, que necessitam de um aporte maior que somente julgados e doutrina, que atualmente são conflitantes, para maior segurança jurídica dos agentes de segurança pública e efetiva tutela fundamental.

Vale ressaltar, que apesar da falta legislativa, o tema será discutido no Supremo Tribunal Federal a partir do dia 18 de agosto de 2022 em pauta de repercussão geral no ARE 1042075/RJ, com o Tema 977: "Aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime". Porém mesmo assim, mesmo após a decisão em sede de repercussão geral, ainda será necessário o devido aporte legislativo, pois a lei possui maior força normativa e impositiva.

4. REFERÊNCIAS

B.B.E.A. **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020.

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética:** À luz do Marco Civil da Internet**.** Rio de Janeiro: Brasport. 2016.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional**. 14ª Ed. São Paulo: Saraiva, 2021.

CAPEZ, Fernando. **Curso de Processo Penal**. 24ª ed. São Paulo. Saraiva. 2017.

DRUCKER, P. **O futuro chegou**. Exame, 22 mar. 2000. p. 112-126, 2000.

ERTHAL, A. A. **O telefone celular como produtor de novas sensorialidades e técnicas corporais**. Contemporânea n. 8, 2007

FERRAZ JR., Tercio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. Cadernos de Direito Constitucional e Ciência Política. São Paulo: Revista dos Tribunais, nº 1, 1992.

GONZAGA, Alvaro de Azevedo, ROQUE, Nathaly Campitelli. **Teoria Tridimensional do Direito, Tomo Teoria Geral e Filosofia do Direito**. Enciclopédia Jurídica PUCSP. Edição 1, 2017.

GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães. **Nulidades no Processo Penal**. 2ª ed. São Paulo. Malheiros Editores. 1992.

IBGE – Instituto Brasileiro de Geografia e Estatística. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2019**. Rio de Janeiro. 2019.

JAMIL, George Leal. NEVES, Jorge Tadeu de Ramos. **A era da informação: considerações sobre o desenvolvimento das tecnologias da Informação**. Belo Horizonte: Perspectivas em ciência da informação. 2000.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

LIMA, Renato Brasileiro de. **Legislação Criminal Especial Comentada:** volume único. 8ª Ed. Salvador: Juspodivm, 2020.

MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados Comentada.** 2ª Ed. São Paulo: Thomson Reuters. 2019.

M.A.D. **Direito Constitucional**. São Paulo: Grupo GEN, 2021.

NORTON-SYMANTEC. **Relatório de Crimes Cibernéticos NORTON:** O impacto humano. 2010.

NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. **Crimes na Internet:** elementos para uma reflexão sobre a ética informacional. 2003.

PADILHA, Rodrigo. **Direito Constitucional**. São Paulo: Grupo GEN, 2019.

PINHEIRO, P. P. **PROTEÇÃO DE DADOS PESSOAIS:** COMENTÁRIOS À LEI N. 13.709/2018 (LGPD). Editora Saraiva, 2021.

PRADO, Leandro Cadenas. **Provas ilícitas:** teoria e a interpretação dos tribunais superiores. 2 ed. - Rio de Janeiro: Impetus, 2008.

REALE, Miguel. **Filosofia do direito.** 19ª Ed. São Paulo: Saraiva. 1999.

VAZ, Conrado Adolpho. **Google marketing:** O guia definitivo de marketing digital. 2ª. ed. São Paulo: Novatec, 2008.

Contatos: lucx.mikael@gmail.com, fabiano.petean@mackenzie.br