1. INTRODUÇÃO

A invenção do aparelho celular marca um dos avanços tecnológicos mais significativos da era moderna, originada a partir das fundamentais descobertas das ondas eletromagnéticas por Heinrich Rudolf Hertz[1]. Essas descobertas pavimentaram o caminho para o desenvolvimento de dispositivos capazes de transmitir informações através dessas ondas, um feito que transformaria radicalmente as comunicações humanas.

No início do século XX, a Bell Company, um dos pioneiros nesse campo, desenvolveu um sistema telefônico que operava com antenas, uma inovação que permitia comunicações móveis limitadas, inicialmente usadas em veículos. Entretanto, foi Martin Cooper[2], da Motorola, quem realizou a primeira ligação entre dois aparelhos celulares, marcando o início de uma nova era na comunicação móvel.

Os primeiros celulares, produzidos pela Motorola entre 1983 e 1994, eram dispositivos volumosos, rapidamente apelidados de "tijolões" devido ao seu tamanho e peso. Naquele tempo, a principal função desses aparelhos era facilitar a comunicação de voz em tempo real. Contudo, a evolução dos celulares desde então tem sido extraordinária, com uma taxa de desenvolvimento sem precedentes. Em menos de meio século, passamos de um dispositivo capaz de realizar uma simples chamada de voz para aparelhos que permitem a comunicação simultânea de múltiplas pessoas por meio de vídeo, uma ideia que outrora pertencia ao domínio da ficção científica.

O advento da internet e sua subsequente integração aos dispositivos móveis ampliou ainda mais as capacidades do telefone celular. De um mero instrumento de comunicação, o celular evoluiu para se tornar uma extensão do usuário, armazenando uma quantidade significativa de informações pessoais, desde fotos e vídeos até dados bancários e documentos pessoais. Este armazenamento concentrado de dados pessoais em um único dispositivo levantou novas preocupações sobre privacidade e segurança.

Por outro lado, o potencial dos aparelhos celulares para facilitar práticas criminosas também aumentou. Originalmente utilizados por criminosos para comunicações relacionadas à coordenação de atividades ilícitas, a conexão desses dispositivos à internet abriu novas avenidas

---

[1] Heinrich Rudolf Hertz, físico alemão nascido em 1857, foi pioneiro no campo eletromagnético, comprovando experimentalmente a existência de ondas eletromagnéticas e suas semelhanças com as ondas luminosas. Sua descoberta fundamental, que as ondas eletromagnéticas se propagam, refletem, refratam e podem ser polarizadas como a luz, levou à nomeação da unidade de medida de frequência, hertz (Hz), em sua homenagem.

[2] Martin Cooper, um engenheiro eletrotécnico e inovador americano, é frequentemente reconhecido como o "pai" do telefone celular, uma inovação distinta do telefone veicular. A sua inspiração para criar um dispositivo de comunicação pessoal portátil veio, em parte, do seriado de TV "Jornada nas Estrelas", especificamente dos comunicadores usados pelos personagens da série.

para a perpetração de crimes cibernéticos. Diante dessa realidade, os celulares se tornaram instrumentos valiosos nas investigações criminais, frequentemente apreendidos durante diligências policiais na busca por evidências.

A legalidade da prova obtida a partir de aparelhos celulares tem sido um tema recorrente nos Tribunais Superiores, dada a ausência de regulamentação específica no direito processual penal[3]. Este vácuo legal levanta questões importantes sobre a proteção de dados e os direitos fundamentais dos indivíduos, exigindo uma consideração cuidadosa no tratamento de tais dispositivos como fontes de prova. A volatilidade e a riqueza de informações contidas nos dispositivos móveis apresentam desafios únicos para o direito penal, que busca equilibrar a eficácia das investigações com a proteção dos direitos individuais em um ambiente tecnológico em constante evolução.

2. A natureza jurídica do parelho celular no processo penal

No âmbito do direito processual penal, as terminologias "fonte de prova", "meio de prova" e "meio de obtenção de prova" são frequentemente empregadas de forma intercambiável. Contudo, a distinção entre essas categorias possui importância significativa, uma vez que, fundamentada nessa diferenciação, as repercussões — especialmente aquelas relacionadas a debates sobre a legalidade ou legitimidade das evidências apresentadas — divergem substancialmente.

A expressão “fonte de prova” pode ser conceituada como qualquer elemento que possa, de alguma forma, contribuir para o esclarecimento de um crime. As fontes de prova podem ser classificadas como pessoais, que são os indivíduos que, de certa forma, mantiveram qualquer contato com o crime (vítima, investigado, testemunhas, peritos) ou reais, que são os documentos relacionados ao crime [4].

Nesse sentido, destacamos os ensinamentos de Lima (2022, p. 574), para quem:

> A expressão *fonte de prova* é utilizada para designar as pessoas ou coisas das quais se consegue a prova, daí resultando a classificação em fontes pessoais (ofendido, peritos, acusado, testemunhas) e fontes reais (documentos, em sentido amplo). Cometido o fato delituoso, tudo aquilo que possa servir para esclarecer alguém acerca da existência desse fato pode ser conceituada como fonte de prova. Derivam do fato delituoso em si, independentemente da existência do processo, ou seja, são anteriores a ele, sendo que sua introdução no feito se dá através dos meios de prova. Exemplificando, suponha-se que determinado crime tenha sido praticado dentro de uma sala de aula. Todas as pessoas que presenciaram o cometimento do delito serão consideradas fontes de prova. Essas pessoas poderão ser levadas à apreciação do juiz,

[3] Não são raros os casos em que juízes se utilizam da Lei nº 9.296/96 (Interceptação Telefônica) ou da Lei nº 12.965/14 (Marco Civil da Internet) para decidir casos envolvendo a quebra do sigilo telefônico do aparelho pertencente ao investigado.

[4] A palavra documento aqui possui sentido amplo, significando qualquer objeto ou coisa que possa servir de prova de um crime.

> o que se dará pela sua introdução no processo pelos meios de prova, *in casu,* pela prova testemunhal.

Importante observar que as fontes de provas subsistem e são anteriores ao processo. Ou seja, independentemente de haver ou não uma relação processual, a fonte de prova, através da nossa percepção do mundo exterior, permanece real e é passível de demonstrar que determinado fato ocorreu ou não. Podemos assim dizer que ela possui existência extraprocessual ou fora do processo.

Já a expressão "meio de prova" está diretamente relacionada à atividade processual, ou seja, consiste na forma de introduzir no processo uma fonte de prova, transformando-a em elemento de convicção perante o julgador. Assim, enquanto a fonte de prova permanece fora do processo, só há falar em meio de prova dentro de determinado processo. Desse modo, a existência do meio de prova é endoprocessual. Nesse sentido, Badaró (2003, p. 166):

> (...) a testemunha de um fato é a fonte de prova, enquanto suas declarações em juízo são o meio de prova. O documento é uma fonte de prova, a sua incorporação ao processo é o meio de prova. O livro contábil é a fonte de prova, enquanto a perícia contábil é o meio de prova.

O meio de prova possui como uma de suas características próprias, a necessidade de ser produzido sob a égide do contraditório, com conhecimento da acusação e da defesa, em debate processual perante o juiz, que analisará a sua validade e relevância para o deslinde da causa. Em caso de haver irregularidades insanáveis, o meio de prova será declarado nulo (e não ilegal).

Por fim, quando se fala em "meio de obtenção da prova", estamos a tratar de métodos de investigação da prova, utilizados geralmente pelos órgãos de investigação criminal, e regulamentados por leis. Para que os meios de obtenção de prova possam atingir a finalidade pretendida, geralmente são colocados em prática sem a comunicação à parte contrária (investigado). Como exemplos, podemos destacar a busca e apreensão domiciliar, interceptações telefônicas, reguladas pela Lei n° 9.296/96, infiltração de agentes, prevista tanto na Lei n° 11.343/06 (art. 53, inciso I) e na Lei n° 12.850/13 (arts. 10 a 14).

A diferenciação entre o que se entende por "meio de prova" e "meio para obtenção da prova" é relevante, pois, a partir dela, surge uma importante consequência jurídica quando se trata do tema "prova ilícita no processo penal"[5]. Conforme bem apontado por Lima (2022, p. 575):

---

[5] A expressão "prova ilícita no processo penal" é utilizada aqui no seu sentido amplo, significando quaisquer irregularidades ocorridas quando do momento de sua produção.

> Essa distinção entre meios de prova e meios de obtenção de prova também é importante quando se aponta as consequências de eventuais irregularidades ocorridas quando do momento de sua produção. Deveras, eventual vício quanto aos meios de prova terá como consequência a nulidade da prova produzida, haja vista referir-se a uma atividade endoprocessual. Lado outro, verificando-se qualquer ilegalidade no tocante à produção de determinado meio de obtenção de prova, a consequência será o reconhecimento de sua inadmissibilidade no processo, diante da violação de regras relacionadas à sua obtenção (CF, art. 5º, LVI), com o consequente desentranhamento dos autos do processo (CPP, art. 157, *caput*).

Assim, caso a haja irregularidade na produção de uma determinada prova, devemos verificar se tal ocorreu com meio de prova, em atividade endoprocessual, o que ocasionará a sua nulidade. Já se a irregularidade se deu pelo desrespeito à ao modelo típico estabelecido para realização de determinado meio de obtenção da prova, o caso será de inadmissibilidade da prova no processo.

Realizada essa digressão, podemos afirmar que o aparelho celular, no cenário atual, trata-se de uma rica fonte de prova, que geralmente é conseguida na fase investigativa através de uma busca e apreensão domiciliar ou da apreensão quando da realização de uma prisão em flagrante delito de determinada pessoa[6] (meios de obtenção da prova). Já as informações conseguidas a partir do aparelho celular são introduzidas no processo como um meio de prova documental, geralmente em forma de relatório circunstanciado elaborado por analistas policiais investigadores.

Em nossa ótica, devido a relevância dos dados contidos em dispositivos móveis para investigações, é importante que ele passe a ser tratado como um meio de obtenção de prova, devendo a sua apreensão, extração de dados e análise, serem devidamente regulamentadas através de lei, o que trará segurança jurídica para os atores do processo penal e, acima de tudo, mais amplitude de proteção aos direitos fundamentais à privacidade, intimidade e proteção de dados dos investigados, à luz do que estabelece o art. 5º, Inc. LXXIX da Constituição Federal, que incluiu de forma expressa no texto constitucional o direito fundamental à proteção de dados.

3. Da privacidade à proteção de dados: um caminho asfaltado pela era digital

O conceito tradicional de privacidade está relacionado à ideia de alguma informação de caráter pessoal, que não haja, a princípio, um interesse em sua divulgação a terceiras pessoas. Ao afirmarmos que todos têm o direito fundamental à privacidade, reafirmamos a ideia de que todo ser humano possui o direito de manter certas informações e aspectos de sua vida fora do domínio público. O "*direito de ser deixado só, estar a salvo de interferências alheias, do*

[6] Vale ressaltar que o aparelho celular também pode ser apreendido de outras formas durante uma investigação. Esse é o caso da entrega do aparelho pertencente à vítima de crime de homicídio pelos seus familiares ou a apreensão pela autoridade policial durante as diligências em local de crime ou em revista a estabelecimentos prisionais.

segredo ou sigilo que são direitos calibrados pela dicotomia das esferas pública e privada. A pessoa tem o direito de retrair aspectos de sua vida do domínio público" (BIONI, 2021, p. 91).

A doutrina identifica a obra *'The Right To Privacy'*, de Samuel Warren e Louis Brandeis, publicada em 1890, como um marco histórico documental no que tange ao direito à privacidade. Neste texto, os autores norte-americanos elaboram a concepção de privacidade como uma essencial proteção psicológica do indivíduo. Tal proteção é articulada por meio do controle sobre o acesso de terceiros a informações pessoais, destacando como este conhecimento pode influenciar e, em alguns casos, alterar significativamente a personalidade do indivíduo[7].

Antes disso, como bem explica Magalhães e Oliveira (2021, p. 57-58):

> (...) a privacidade era entendida sob o prisma da propriedade, que era um direito inviolável e sagrado, ninguém dela podendo ser privado, protegida contra intromissões arbitrárias do Estado. Assim, na evolução do conceito da privacidade, esta sai de um direito extrínseco ao indivíduo, que é a propriedade, passando a ser um direito intrínseco, inerente à esfera íntima e à personalidade – cabendo não só ao Estado, mas a todos, o cuidado da não intromissão na vida privada.

Diante de um direito de contornos ainda em formação, naquele momento histórico, buscava-se, por meio de outros dogmas já consagrados, a proteção a esse aspecto tão relevante da vida do homem em sociedade. Assim, Rebellato (2020, p. 18) afirma que na ausência de um direito formalmente reconhecido à privacidade, recorria-se à interpretação extensiva de outros direitos e valores, estendendo-se aquele as noções protetivas relacionadas à vida, liberdade, propriedade e domicílio.

Em 1948, em resposta aos conflitos globais devastadores, a Organização das Nações Unidas - ONU publicou a Declaração Universal dos Direitos Humanos, doravante DUDH, documento que pesar de não ter força jurídica vinculante, tornou-se a pedra angular para muitos textos legais e constituições focadas em direitos humanos, incluindo a nossa Constituição Federal de 1988. A importância simbólica da DUDH e seu papel como padrão ético e moral são inegáveis.

Para o nosso estudo, destacamos o teor das garantias básicas de direitos humanos previstas no artigo 12 da Declaração Universal dos Direitos Humanos, que aborda o direito à privacidade nos seguintes termos *"ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação.*

[7] A importância de assegurar que os indivíduos controlem quais informações pessoais são divulgadas é fundamental para a preservação de sua autonomia na construção de suas identidades

Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques" (ONU, 1948).

O dispositivo faz referência à vida privada, ao lar, à correspondência, honra e reputação, mas numa ótica de um mundo não informatizado existente à época de sua criação. Mesmo assim, os termos utilizados por ele possuem significados abrangentes e principiológicos que, numa interpretação extensiva, podem ser aplicados até os dias atuais, mas que, forçoso dizer, não satisfazem os anseios do mundo moderno, altamente informatizado e com grande armazenamento e circulação de dados pessoais de natureza privada no meio digital.

Em 1966, o Pacto Internacional de Direitos Civis e Políticos[8], um marco jurídico, detalhou os princípios estabelecidos pela DUDH. Posteriormente, a Declaração serviu de base para a elaboração de diversas convenções internacionais com enfoques específicos. Muitos desses tratados internacionais enfatizam a proteção da vida privada e foram internalizados em nosso sistema jurídico.

Como dito, fazendo-se uma interpretação alargada, o conceito de direito à privacidade poderia ser aplicado para proteção dos dados pessoais, inclusive no ambiente digital informatizado. Porém, essa proteção se tornou um tanto quanto vaga, pois, num cenário de pulverização de informações, verificamos características e detalhes que não haviam no mundo para o qual a DUDH e os documentos posteriores que lhes deram normatividade foram redigidos. Exemplo disso é quantidade de pessoas que podem ter acesso a determinada informação ao mesmo tempo em todo o planeta e a velocidade com que essa informação é transmitida. O conceito de fronteira no meio digital não existe, ou ainda não foi definido.

De outro lado, à medida em que os meios de comunicação foram evoluindo, num esforço de defesa, o direito à privacidade também o fez, destacando-se o seu aspecto de proteção de dados. Isso se tornou cada vez mais relevante considerando uma sociedade geradora de relações digitais multifacetadas e complexas, que, inevitavelmente, condensa em si muito mais riscos de exposição da vida privada dos indivíduos a pessoas indesejadas.

No entanto, o conceito de privacidade não acompanhou plenamente as transformações das relações sociais na era digital, tornando-se, em certo aspecto, insuficiente para salvaguardar

[8] O Pacto Internacional sobre Direitos Civis e Políticos foi adotado pela XXI Sessão da Assembleia-Geral das Nações Unidas, em 16 de dezembro de 1966. O Congresso Nacional aprovou o texto do referido diploma internacional por meio do Decreto Legislativo n° 226, de 12 de dezembro de 1991, sendo a Carta de Adesão depositada em 24 de janeiro de 1992, entrando em vigor, para o Brasil, em 24 de abril de 1992, na forma de seu artigo 49, parágrafo 2. Em seu art. 17 trata do direito à privacidade nos seguintes termos "1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

esse campo vital da vida das pessoas. Atualmente, com a internet permeando quase todas as ações, a privacidade adquiriu uma dimensão relativa. Nossos dados pessoais, preferências e comportamentos, sejam compartilhados voluntariamente[9] ou não[10], estão constantemente nas mãos de plataformas digitais. Essas plataformas processam e utilizam tais informações para traçar perfis detalhados, fomentando assim o consumo exacerbado. Neste contexto, Sarlet e Ferreira Neto (2019, p. 20) destacam a emergência de:

> (...) um absoluto descontrole no manuseio, na armazenagem e no acesso dos dados pessoais que estão pulverizados na *Internet*, o que acaba por fragmentar o nosso senso de privacidade e de personalidade, tornando-nos vulneráveis em relação ao que os demais pensam e falam sobre nossa esfera individual e sobre o nosso passado.

O envio de informações a essas plataformas foi fomentado em muito pela tecnologia hoje existente nos aparelhos celulares (dispositivos móveis), os quais se transformaram em verdadeiros computadores com capacidades para armazenamento de aplicativos que, ao mesmo tempo em que nos ajudam a realizar tarefas dificultosas, rastreiam-nos a todo momento, coletando informações sobre localização, compras realizadas, relações interpessoais, e outras tantas.

O celular se tornou um repositório pessoal, armazenando detalhes íntimos da vida de seus usuários utilizado como ferramenta pelas apresas de aplicações de internet, as quais exigem para o uso dos seus produtos e serviços, a autorização para que possam acessar e coletar nossos dados pessoais de privacidade. Em outras palavras, os nossos dados viraram uma espécie de moeda de troca. Essa prática transformou os dispositivos móveis em uma valiosa fonte de evidências em investigações criminais, atuando como um banco de dados privado do indivíduo, uma vez que os aplicativos neles instalados estão recheados de dados pessoais. A análise deste fenômeno, e seus aspectos durante a investigação criminal, é o foco deste estudo.

No contexto acima exposto, passou a ser debatido na doutrina a existência, nos ordenamentos jurídicos modernos, de um direito fundamental à proteção de dados. Ao discorrer sobre o tema, Sarlet e Saavedra (2020, p. 41) afirmam que *"ao nível do direito internacional público, tanto no âmbito do sistema universal de proteção da ONU quanto na esfera do Direito*

[9] A Meta (Facebook e Instagram) coleta diversas informações de usuários em suas plataformas, incluindo conteúdo criado, mensagens enviadas, interações com anúncios, uso de apps, transações financeiras e detalhes de atividades como hashtags e tempo gasto. A empresa destaca que não acessa o conteúdo de mensagens criptografadas a menos que sejam denunciadas

[10] No próprio site também existe a seguinte informação "o que acontecerá se você não permitir nossa coleta de determinadas informações? Algumas informações são necessárias para que nossos Produtos funcionem. Outras informações são opcionais, mas, sem elas, é possível que a qualidade da sua experiência seja afetada" (META, 2024).

europeu, um direito à proteção de dados tem sido deduzido em especial do direito à privacidade, embora com este não se confunda".

Diante disso, torna-se evidente que o direito à privacidade, tal como estabelecido pela Declaração Universal dos Direitos Humanos e pela Constituição Federal brasileira de 1988, especialmente em seu artigo 5º, incisos X, XII, não é mais suficiente para proteger as informações pessoais no ambiente digital. Essa insuficiência se deve ao fato de que os próprios usuários, conscientemente ou não, estão compartilhando seus dados com terceiros como forma de pagamento pelo acesso a serviços específicos. Estamos diante de uma nova realidade que desafia os paradigmas tradicionais de privacidade.

Nesse sentido, Facchini Neto e Demoliner (2019, p. 128), citando o caso de Bobbi Duncan, uma estudante da Universidade do Texas[11], chamou a atenção para a necessidade de aplicação do *"conceito evoluído de proteção da privacidade, que significa o controle de nossos dados, chamado na Alemanha de autodeterminação informativa"*[12].

4. O reconhecimento implícito do direito à proteção de dados na Constituição Federal

Não é de hoje que a doutrina reconhece a existência implícita de um direito fundamental à proteção de dados na Constituição Federal. Para tanto, embasam o entendimento nos seguintes dispositivos: a) princípio da dignidade da pessoa humana (art. 1°, Inc. III, CF/88); b) garantia da inviolabilidade da intimidade, a vida privada, a honra e a imagem das pessoas (art. 5º, Inc. X); c) proteção da comunicação de dados[13] (art. 5º, XII) e; d) a ação constitucional de habeas data (art. 5º, Inc. LXXII). Nesse sentido, aponta Sarlet e Saavedra (2020, p. 41):

---

[11] Estudante teve revelada sua inclinação homossexual ao seu pai, o que causou enorme stress familiar, culminando com a ruptura de relações entre ela e seu pai. Bobbi escondia sua inclinação sexual de seu pai, ajustando os mecanismos de privacidade de seus contatos. Todavia, a revelação se deu quando ela ingressou em um grupo do Facebook que reunia pessoas com idêntica orientação (UT's Queer Chorus). Quando o criador do grupo adicionou Bobbi ao grupo, o Facebook automaticamente enviou mensagem a todos os "friends" de Bobbi, noticiando seu ingresso num novo Grupo. Dentre tais amigos encontrava-se seu pai" (FACCHINI NETO; DEMOLINER, 2019, p. 128).

[12] A autodeterminação informativa é um direito fundamental sob a LGPD, permitindo que indivíduos controlem seus dados pessoais, garantindo a supervisão e o respeito à sua autonomia no tratamento dessas informações, estendendo a proteção da privacidade para além da intimidade.

[13] Por um lado, a privacidade é encarada como um direito fundamental, as informações pessoais em si parecem, a uma parte da doutrina, serem protegidas somente em relação à sua "comunicação", conforme art. 5º, XII, que trata da inviolabilidade da comunicação de dados. Tal interpretação traz consigo o risco de sugerir uma grande permissividade em relação à utilização de informações pessoais. Nesse sentido, uma decisão do STF, relatada pelo Ministro Sepúlveda Pertence, reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais... O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade... Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica... A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho... A decisão tem sido, desde então, constantemente mencionada como precedente em julgados nos quais

> No caso do Brasil, como já antecipado, a Constituição Federal de 1988 (CF), embora faça referência, no art. 5º, XII, ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas), não contempla expressamente um direito fundamental à proteção e livre disposição dos dados pelo seu respectivo titular, sendo o reconhecimento de tal direito algo ainda relativamente recente na ordem jurídica brasileira.

Ainda que de maneira implícita, o ordenamento jurídico brasileiro já contemplava a proteção de dados como um direito fundamental, ancorado na necessidade de atualizar a tutela da privacidade para enfrentar os desafios impostos pela era digital. Em síntese, a proteção tradicionalmente oferecida pela privacidade mostrou-se insuficiente para abranger integralmente os dados pessoais no contexto da informatização. O manto protetor da privacidade se tornou muito curto para agasalhar os dados pessoais na era da informatização, surgindo, assim, o direito à proteção de dados como forma de enfrentar a nova realidade.

Embora os dispositivos constitucionais citados acima sejam comumente empregados para fundamentar o direito à proteção de dados no nosso ordenamento, parte da doutrina sustenta que a base de sua existência derivava do direito ao livre desenvolvimento da personalidade, ligado diretamente ao princípio da dignidade da pessoa humana e ao direito geral de liberdade. Nesse sentido, destacamos:

> Mas, possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana, que, de acordo com tradição jurídica já consolidada no direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (mas não se limita ao!) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa (SARLET; SAAVEDRA, 2020 *apud* MOTA PINTO, 2018, p. 642 e ss.)

Diante das discussões na comunidade jurídica e da urgente necessidade de regular o direito fundamental à proteção de dados, surgiram diversas legislações infraconstitucionais. Por exemplo, o Marco Civil da Internet (Lei nº 12.965/14) delineou princípios e diretrizes para a utilização da Internet no Brasil, enquanto a Lei Geral de Proteção de Dados (Lei nº 13.709/18) especificou regras para o tratamento de dados pessoais, visando a salvaguarda da liberdade e da privacidade, além do desenvolvimento pessoal do indivíduo. Ambas as normas constituem esforços para estabelecer um marco regulatório na proteção de dados, mesmo na ausência de uma previsão explícita desse direito na Constituição Federal no momento de suas promulgações.

---

o STF identifica que a natureza fundamental da proteção aos dados está restrita ao momento de sua comunicação. (DONEDA, 2011, p. 105).

No âmbito jurisprudencial, notadamente no Supremo Tribunal Federal, observou-se o reconhecimento do direito à proteção de dados como um direito fundamental autônomo. Um exemplo emblemático é a Ação Direta de Inconstitucionalidade (ADIn) 6387, julgada em 07/05/2020, na qual se contestou a constitucionalidade da Medida Provisória nº 954/20, que exigia das operadoras de telefonia o compartilhamento de dados pessoais de mais de cem milhões de brasileiros com o IBGE[14]. O STF julgou a medida inconstitucional, argumentando que violava direitos fundamentais como privacidade, intimidade e sigilo de dados, por não atender aos princípios de proporcionalidade e razoabilidade. Nesse julgamento, consolidou-se a compreensão de que o direito à proteção de dados pessoais é independente e possui um espectro de proteção distinto do direito à privacidade[15].

5. O reconhecimento expresso do direito à proteção de dados como direito fundamental

Em meio a essas discussões, em 10 de fevereiro de 2022, foi promulgada a Emenda Constitucional de nº 115 (oriunda da PEC nº 17/2019 do Senado Federal), que acrescentou o inciso LXXIX ao art. 5º da Constituição Federal, colocando expressamente o direito à proteção de dados no rol dos direitos fundamentais. Com isso, trouxe total autonomia em relação aos demais direitos dessa categoria, asseverando que *"é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"* (BRASIL, 2020).

O direito à proteção de dados, a partir da referida Emenda, não mais necessita de um esforço interpretativo para se chegar à conclusão da sua existência e vigência. Não há que se perquirir se ele deriva do direito à privacidade, dignidade humana ou qualquer outro. Possui, a partir de então, espectro de proteção autônomo e diferente dos demais direitos fundamentais. Nesse sentido finaliza Scheuermann (2023, p. 271):

> (...) pode-se concluir que com o fato da sociedade exercer diversos ramos de sua vida no ciberespaço, o direito brasileiro, por muito tempo, esteve um tanto quanto omisso em relação aos dados pessoais, cenário que veio a mudar em especial com a inserção da proteção de dados no rol dos direitos fundamentais, transformando-o em um direito autônomo e não como mera extensão da intimidade e da privacidade.

Além de reconhecer expressamente a proteção de dados como um direito fundamental, a Constituição atribuiu à União a competência para organizar e fiscalizar a proteção e o

[14] Instituto Brasileiro de Geografia e Estatística, é um instituto público da administração federal brasileira criado em 1934 e instalado em 1936 com o nome de Instituto Nacional de Estatística.

[15] (...) Nesse sentido, transcreve-se trecho do julgado: 6. ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros (BRASIL, 2020).

tratamento de dados pessoais, conforme estabelecido no art. 21, Inc. XXVI, CF. Além disso, confere ao Congresso Nacional a competência legislativa exclusiva sobre a matéria, conforme disposto no art. 22, Inc. XXX, CF.

Com envergadura de direito fundamental expressamente previsto em nossa Constituição, faz-se oportuno estabelecer o significado do direito à proteção de dados, seuas contornos e abrangência, bem como a sua possível aplicação durante a persecução penal, especialmente no que se refere ao uso do aparelho celular como fonte de prova, já que o equipamento, como bem apontado, consiste em um rico banco de dados sobre o usuário. No entanto, antes disso, precisamos definir o que é dado, dado pessoal e banco de dados e se o aparelho celular, sob essa ótica, pode ser considerado um repositório de dados pessoais.

6. O reconhecimento do aparelho celular como banco de dados pessoais

Dado, de uma maneira resumida, consiste em qualquer elemento que ainda não passou por uma triagem ou análise e que se constitui em fonte de possível informação, considerado em sua forma isolada ou em conjunto com outros elementos diferentes. A partir dessa premissa, o Decreto de nº 8.771/16, que regulamenta a Lei nº 12.965/14 (Marco Civil da Internet), estabelece o que vem a se entender por dado pessoal:

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
> I - **dado pessoal** - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa (BRASIL, 2016, grifo nosso).

No mesmo sentido, a Lei nº 13.709/18 (Lei Geral de Proteção de Dados), em seu art. 5º, inc. I, estabelece que, para os seus fins, considera-se dado pessoal como a *"informação relacionada a pessoa natural identificada ou identificável"*[16]. Assim, temos que um dado é considerado como pessoal a partir do momento em que se verifica a possibilidade de sua vinculação a determinada pessoa, seja ela identificada ou não. Em outras palavras, qualquer elemento, seja físico ou digital (dado físico ou digital), que possa ser vinculado a um determinado ser humano, possibilitando a sua identificação, é considerado dado pessoal.

Definido o que é dado e o que se entende por dado pessoal, o conceito de "banco de dados" pode ser estabelecido como *"a ferramenta que possibilita a sistematização de volumes que podem chegar a ser gigantescos de informação e que teve seu potencial exponencialmente incrementado com o advento da informática"* (Doneda, 2011, p. 92). E continua o autor explicando que:

---

[16] Aqui há uma atecnia do legislador, pois **dado** não se confunde com **informação**, sendo essa a ideia que se extrai daquele a partir de sua análise.

> Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações (DONEDA, 2011).

Nessa perspectiva, a ideia de banco de dados pode ser empregada para definição de qualquer ambiente, equipamento, programa ou ferramenta, públicos ou privados, que possam guardar e estruturar dados para utilização em uma finalidade precípua ou secundária. Se esses dados forem elementos de vinculação a pessoas identificadas ou identificáveis, estaremos diante de um banco de dados pessoais.

Ainda, podemos afirmar que bancos de dados são úteis na criação de uma informação que *"pode gerar proveito, como resulta claro ao verificar que é milenar a prática de coleta sistematizada de informações por alguma modalidade de censo populacional, instrumento de imensa serventia para governantes de qualquer época*" (Doneda, 2011, p. 92). É com esse viés que o acesso a banco de dados, principalmente pessoais, gera uma restrição a direitos fundamentais como privacidade, intimidade e, agora expressamente previsto de forma autônoma, ao direito à proteção de dados.

Assim, ousamos afirmar que o aparelho celular consiste em verdadeiro banco de dados pessoais, respaldando-nos na complexidade e natureza dos dados armazenados nesses dispositivos e na necessidade de tutelar a privacidade, intimidade e proteção de dados dos indivíduos, direitos esses garantidos pela Constituição Federal.

Nesse sentido, tanto o Supremo Tribunal Federal (STF) quanto o Superior Tribunal de Justiça (STJ) reconhecem a extensão e a profundidade das informações contidas nos dispositivos móveis, que vão desde comunicações pessoais até informações sensíveis como localização, dados bancários e registros de atividades diárias, configurando um verdadeiro repositório da vida privada do indivíduo. Tal entendimento está alinhado ao princípio da dignidade da pessoa humana e à garantia da vida privada, previstos nos artigos 1º, III, e 5º, X, da Constituição Federal, respectivamente.

Ademais, o enquadramento do celular como um banco de dados pessoais demanda a aplicação rigorosa dos princípios de legalidade, proporcionalidade e necessidade no que tange à sua análise e acesso por terceiros, especialmente em investigações criminais. A legislação vigente e a jurisprudência dos tribunais superiores, inclusive do Tribunal de Justiça do Estado de Pernambuco (TJPE), têm estabelecido salvaguardas para assegurar que qualquer intrusão nesse banco de dados pessoais seja meticulosamente justificada e autorizada judicialmente, a fim de evitar abusos e proteger os direitos fundamentais dos cidadãos.

Ocorre que, com a inclusão expressa do direito fundamental à proteção de dados no inciso LXXIX do art. 5º da Constituição Federal em 2022, na condição de norma constitucional de eficácia limitada, para realização de quebra do sigilo telefônico relativos aos dados contidos em dispositivos móveis de investigados, passou-se a ser exigida a elaboração de uma lei infraconstitucional, prevendo os pressupostos e requisitos para realização de tal medida investigativa.

7. O direito fundamental à proteção de dados: norma de eficácia limitada e consequências para investigação

Desde sua concepção, a Carta Magna insinuava, de maneira subentendida, a existência de um direito inerente à salvaguarda de dados pessoais. Com o fluxo do tempo, essa noção foi progressivamente cristalizada e amplificada por um consenso emergente na doutrina, nas decisões judiciais e nos estatutos infraconstitucionais. Com a promulgação da Emenda Constitucional nº 115/2022, essa prerrogativa foi finalmente erigida ao panteão dos direitos e garantias fundamentais, estabelecida de forma explícita no art. 5º, inc. LXXIX, da Constituição Federal, articulada nos termos seguintes:

> 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:
> (...)
> LXXIX - é assegurado, **nos termos da lei**, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (grifo nosso).

Antes de adentrarmos na classificação da norma que instituiu de forma expressa o direito à proteção de dados, há de se indagar qual seria a importância de se promulgar uma Emenda Constitucional com a finalidade de prevê um direito que já se fazia presente em nosso sistema constitucional? E como resposta, trazemos as lições de Sarlet e Saavedra (2020, p. 47), para quem, entre as razões, destacam-se os seguintes pontos:

> a) a despeito das interseções e articulações com outros direitos, fica assegurada à proteção de dados a condição de direito fundamental autônomo, com âmbito de proteção próprio;
> b) ao direito à proteção de dados passa a ser atribuído de modo inquestionável o pleno regime jurídico-constitucional relativo ao seu perfil de direito fundamental em sentido material e formal já consagradas no texto da CF, bem como na doutrina e na jurisprudência constitucional brasileira, ou seja:
> 1) como parte integrante da constituição formal, os direitos fundamentais possuem *status* normativo superior em relação a todo o restante do ordenamento jurídico nacional;
> 2) na condição de direito fundamental, assume a condição de limite material à reforma constitucional, devendo, ademais disso, serem observados os assim chamados limites formais, circunstanciais e temporais, nos termos do art. 60, §§ 1 a 4º, da CF;
> 3) também as normas relativas ao direito à proteção de dados são – nos termos do art. 5º, § 1º, da CF – dotadas de aplicabilidade imediata (direta) e vinculam todos os atores

> públicos, bem como – sopesadas as devidas ressalvas, consoante será tratado em tópico específico – os atores privados.

O ponto crucial e que requer toda atenção diz respeito ao fato de que o direito fundamental à proteção de dados, da forma que foi redigido pelo constituinte derivado no art. 5º, inc. LXXIX da Constituição Federal, consiste em norma constitucional de eficácia limitada, exigindo do legislador infraconstitucional a iniciativa lei integrativa, principalmente, para imposição de restrições ao alcance de sua proteção.

O mandamento insculpido no texto incluído na Constituição, ao fincar a expressão "nos termos da lei", deixa evidente que se trata de uma norma constitucional de eficácia limitada de princípio institutivo impositiva. Nesse sentido, Leite (2020, p.69), interpretando os ensinamentos do mestre José Afonso da Silva, detalha que referidas normas:

> (...) necessitam de uma integração normativa por parte do legislador ordinário para que possam produzir os efeitos essenciais almejados pelo constituinte originário. No tocante à sua tipologia, José Afonso da Silva apresenta as seguintes subespécies de normas de eficácia limitada: (a) normas constitucionais de princípio institutivo e (b) normas constitucionais de princípio programático.
> As normas constitucionais de princípio institutivo – também denominadas normas de princípio orgânico ou organizativo – são aquelas que traçam as diretrizes ou princípios estruturais de instituições, órgãos ou entidades, permitindo que o legislador ordinário, por meio de lei, os estruture. O que essencialmente as caracteriza é o fato de requererem uma legislação futura que lhes permita uma efetiva aplicação. Tais normas não se confundem com as de conteúdo programático, dado que a sua matéria é nitidamente estrutural, guarda relação com a composição e o funcionamento das instituições constitucionais. Portanto, a legislação integradora surgirá para instrumentalizar a estrutura institucional inicialmente concebida pela norma constitucional.
> As normas constitucionais de princípio institutivo comportam duas subespécies: impositivas ou facultativas. As impositivas determinam ao legislador o dever de criar a lei integradora, ao passo que as facultativas permitem ao legislador realizar um juízo de conveniência acerca da necessidade ou não de edição da norma integrativa.

Ao explicitar o direito à proteção de dados como uma norma constitucional de eficácia limitada, o constituinte derivado delegou ao legislador a tarefa de elaborar normas que regulamentem a aplicação desse direito. Notavelmente, esse processo de regulamentação já estava em curso antes mesmo da aprovação da emenda correspondente, através da Lei nº 12.965/14, conhecida como Marco Civil da Internet, e da Lei nº 13.709/18, referente à Lei Geral de Proteção de Dados (LGPD), indicando que o direito à proteção de dados já estava sendo parcialmente normatizado. Entretanto, no contexto específico do uso de dispositivos móveis como evidência em processos penais, as disposições do Marco Civil da Internet e da LGPD não são aplicáveis.

8. Da necessidade de lei que regulamente a quebra do sigilo de dados armazenados em aparelhos celulares

Ao abordar a questão da apreensão de aparelhos celulares em investigações policiais, o procedimento padrão exige que o delegado de polícia, ou o promotor de justiça, solicite uma autorização judicial para acessar os dados contidos no dispositivo. Essa medida visa garantir a legalidade da prova, evitando que informações obtidas sem a supervisão de um juiz sejam consideradas ilícitas. Ao avaliar esses pedidos, o Judiciário tem se baseado em legislações específicas como a Lei das Interceptações Telefônicas e Telemáticas (Lei nº 9.296/96) e o Marco Civil da Internet (Lei nº 12.965/14), além de realizar uma análise criteriosa que equilibra o direito à privacidade e a intimidade do indivíduo com a necessidade de progresso na investigação.

Com a recente adição do inciso LXXIX ao artigo 5º da Constituição Federal, que qualifica o aparelho celular como um repositório de dados pessoais, surge um novo paradigma. Embora os tribunais ainda não tenham se debruçado especificamente sobre essa questão, é razoável prever a exigência de uma fundamentação mais sólida para a violação do sigilo desses dados, ancorada na necessidade de legislação específica. Isso se dá pela natureza do novo dispositivo constitucional, que, por ser uma norma de eficácia limitada, requer regulamentação detalhada para sua plena aplicação.

Nesse ponto, crucial considerarmos os precedentes estabelecidos tanto pelo Supremo Tribunal Federal quanto pelo Superior Tribunal de Justiça. Ambas as cortes têm consistentemente interpretado que a Lei nº 9.296/96, que regula as interceptações telefônicas e telemáticas, não se aplica a dados estáticos. Esta lei é direcionada especificamente ao monitoramento de dados em fluxo, isto é, em transmissão ou comunicação em tempo real. Portanto, suas disposições não abarcam os dados que foram armazenados previamente e que se encontram na memória dos dispositivos móveis sob custódia do Estado. Este entendimento reforça a distinção entre a interceptação de comunicações ativas e o acesso a informações já armazenadas. Nesse sentido:

> (...) 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. (...) (BRASIL, 2012, grifo nosso).

No mesmo sentido, a aplicação da Lei nº 12.965/14, conhecida como Marco Civil da Internet, à quebra do sigilo de dados armazenados em dispositivos móveis encontra obstáculos significativos. Essa legislação, em seu artigo 1º, estabelece os princípios, garantias, direitos e deveres para a utilização da internet no Brasil, além de definir as diretrizes para a atuação dos entes federativos no que tange a essa matéria. O escopo da lei é direcionado primordialmente aos provedores de conexão e serviços de internet, bem como aos desenvolvedores de aplicações online. Portanto, estender suas disposições para abarcar dados locais armazenados em celulares apreendidos em investigações apresenta uma incongruência.

A tentativa de aplicar o Marco Civil da Internet aos dados armazenados em dispositivos móveis apreendidos em operações de investigação encontra fundamentos jurídicos frágeis. Isso se deve ao fato de que os dados em questão estão localizados na memória interna do aparelho, agora sob a custódia do Estado, distanciando-se assim do ambiente virtual controlado por provedores de internet ou serviços online. Esta diferença essencial levanta dúvidas significativas sobre a adequação legal de estender o Marco Civil da Internet a tais circunstâncias.

A ausência de paralelos diretos entre os dados armazenados internamente em dispositivos físicos e aqueles mantidos em infraestruturas digitais de terceiros, sublinha a complexidade de invocar analogias legais para justificar tal aplicação. Portanto, diante da especificidade do contexto e das características intrínsecas dos dados armazenados em dispositivos apreendidos, conclui-se que a aplicação do Marco Civil da Internet não encontra sustentação jurídica que a embase nesse cenário.

É imperativo também destacar o escopo da Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados (LGPD), que, conforme estipula explicitamente o inciso III, alínea 'd', do seu artigo 4º, exclui da sua aplicabilidade o tratamento de dados pessoais efetuado exclusivamente para fins de investigação e repressão de infrações penais. Essa disposição legal corrobora a tese de que, mesmo em um cenário onde a proteção de dados assume uma relevância cada vez maior, reconhece-se a necessidade de adaptar as regulamentações às particularidades das atividades de investigação penal.

Analogamente, a recente inclusão do inciso LXXIX no art. 5º da CF/88, em 2022, ecoa o desafio previamente enfrentado pelo inciso XII do mesmo artigo, que condicionava a interceptação de comunicações telefônicas à criação de uma lei específica que regulamentasse a matéria, classificando-a como uma norma constitucional de eficácia limitada. Este contexto obrigou o Supremo Tribunal Federal a confrontar diversas situações onde interceptações

telefônicas haviam sido realizadas antes da promulgação da Lei nº 9.296/96, resultando frequentemente na declaração de ilegalidade dessas ações. Nesse sentido:

> EMENTA: HABEAS-CORPUS. CRIME QUALIFICADO DE EXPLORAÇÃO DE PRESTÍGIO (CP, ART. 357, PÁR. ÚNICO). COMETIDO CONTRA MAGISTRADO. PROVA ILÍCITA: CONJUNTO PROBATÓRIO ORIGINADO, EXCLUSIVAMENTE, DE INTERCEPTAÇÃO TELEFÔNICA, POR ORDEM JUDICIAL, PORÉM, PARA APURAR OUTROS FATOS (TRÁFICO DE ENTORPECENTES): VIOLAÇÃO DO ART. 5º, XII e LVI, DA CONSTITUIÇÃO. 1. O art. 5º, XII, da Constituição, que prevê, excepcionalmente, a violação do sigilo das comunicações telefônicas para fins de investigação criminal ou instrução processual penal, não é auto-aplicável: exige lei que estabeleça as hipóteses e a forma que permitam a autorização judicial. Precedentes. a) Enquanto a referida lei não for editada pelo Congresso Nacional, é considerada prova ilícita a obtida mediante quebra do sigilo das comunicações telefônicas, mesmo quando haja ordem judicial (CF, art. 5º, LVI). b) O art. 57, II, a, do Código Brasileiro de Telecomunicações não foi recepcionado pela atual Constituição (art. 5º, XII), a qual exige *numerus clausus* para a definição das hipóteses e formas pelas quais é legítima a violação do sigilo das comunicações telefônicas. 2. A garantia que a Constituição dá, até que a lei o defina, não distingue o telefone público do particular, ainda que instalado em interior de presídio, pois o bem jurídico protegido é a privacidade das pessoas, prerrogativa dogmática de todos os cidadãos. 3. As provas obtidas por meios ilícitos contaminam as que são exclusivamente delas decorrentes; tornam-se inadmissíveis no processo e não podem ensejar a investigação criminal e, com mais razão, a denúncia, a instrução e o julgamento (CF, art. 5º, LVI), ainda que tenha restado sobejamente comprovado, por meio delas, que o Juiz foi vítima das contumélias do paciente. 4. Inexistência, nos autos do processo-crime, de prova autônoma e não decorrente de prova ilícita, que permita o prosseguimento do processo. 5. Habeas-corpus conhecido e provido para trancar a ação penal instaurada contra o paciente, por maioria de 6 votos contra 5. (BRASIL, 1996)

Este precedente histórico destaca a complexidade e a necessidade de uma abordagem legislativa clara e específica para a quebra do sigilo de dados armazenados em dispositivos móveis. Ressalta-se, assim, a importância de se considerar os paralelos entre as circunstâncias históricas e as atuais demandas por regulamentações adequadas que abordem as peculiaridades tecnológicas e as práticas investigativas contemporâneas, evitando-se, desta forma, repetir os impasses jurídicos enfrentados no passado.

9. CONCLUSÃO

Após uma investigação aprofundada sobre a natureza e a evolução dos dispositivos móveis nas últimas décadas, concluímos que estes se configuram, essencialmente, como repositórios de dados pessoais. Essa característica singular dos aparelhos celulares os torna instrumentos valiosos na coleta de evidências durante investigações criminais, contribuindo significativamente para a elucidação de uma ampla gama de delitos.

Dada a centralidade dos smartphones na vida contemporânea, muitos dos crimes cometidos atualmente, quer sejam perpetrados por meio da internet ou de outras formas, de

alguma maneira envolvem o uso desses dispositivos, seja de maneira direta ou indireta. Assim, sua apreensão em contextos investigativos não apenas é estratégica, mas também crucial, pois os dados contidos nesses aparelhos podem revelar conexões, padrões e evidências fundamentais para a construção de casos no âmbito do processo penal.

Embora a relevância dos dispositivos móveis em investigações criminais seja amplamente reconhecida, a regulamentação específica para a manipulação dessas evidências digitais permanece insuficiente, mesmo após a promulgação da Emenda Constitucional nº 115/2022, que incorporou expressamente o direito fundamental à proteção de dados no artigo 5º, Inciso LXXIX, da Constituição Federal, categorizando-o como uma norma de eficácia limitada.

Por outro lado, é fundamental destacar a complexidade do quadro legal brasileiro no que tange à proteção da privacidade, intimidade e dos dados pessoais. Embora legislações como a Lei das Interceptações Telefônicas e Telemáticas, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) estabeleçam importantes salvaguardas, existe uma lacuna significativa na sua aplicabilidade aos dados armazenados em dispositivos móveis. Essa particularidade revela uma discrepância relevante no ordenamento jurídico, na medida em que as proteções oferecidas por essas leis não se estendem de forma direta e explícita aos conteúdos presentes nesses aparelhos.

A ausência de legislação detalhada que discipline os procedimentos para a apreensão de dispositivos móveis e a subsequente quebra do sigilo dos dados armazenados representa uma lacuna significativa no ordenamento jurídico brasileiro. Esta lacuna não apenas desafia a eficácia das investigações criminais, mas também levanta preocupações sérias sobre a proteção dos direitos fundamentais dos indivíduos, em um contexto onde as fronteiras entre a segurança pública e a privacidade pessoal se tornam cada vez mais tênues.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021, p. 91.

MAGALHÃES, Rodrigo Almeida; OLIVEIRA, Erika Cristina Rodrigues Nardoni. O DIREITO À PRIVACIDADE NA ERA DIGITAL. **Revista Jurídica da Fa7**, [S.L.], v. 18, n. 1, p. 55-70, 28 jun. 2021. Educadora Sete de Setembro. http://dx.doi.org/10.24067/rjfa7;18.1:1173.

DUTRA, Flora Ardenghi. A história do telefone celular como distinção social no Brasil: da elite empresarial ao consumo da classe popular. **Revista Brasileira de História da Mídia**, Teresina, v. 5, n. 2, p. 102-116, jul. 2016.

REBELLATO, Luiz Fernando Bugiga. **Análise Constitucional do Sigilo e da Privacidade nas Investigações Criminais**: acesso a dados armazenados em aparelhos celulares. 2020. 18 f. Dissertação (Mestrado) - Curso de Direito, Universidade de São Paulo, São Paulo, 2020.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**: volume único. 11. ed. São Paulo: JusPodivm, 2022. 574 p.

BADARÓ, Gustavo Henrique Righi Ivahy. **Ônus da Prova no Processo Penal**. São Paulo: Editora Revista dos Tribunais, 2003. 166 p.

FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. **Direito À Privacidade Na Era Digital – Uma Releitura Do ART. XII Da Declaração Universal Dos Direitos Humanos (DUDH) NA Sociedade Do Espetáculo**. Revista Internacional Consinter de Direito, [S.L.], p. 119-140, 18 dez. 2019. CONSINTER. http://dx.doi.org/10.19135/revista.consinter.00009.06.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos, 10.12.1948**. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 11 mar. 2024.

SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. **O direito ao "esquecimento" na sociedade da informação.** Porto Alegre: Livraria do Advogado, 2019. p. 20.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988:** contributo para a construção de uma dogmática constitucionalmente adequada. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. **Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais**. **Revista de Direito Público**, Brasília, v. 17, n. 93, p. 33-57, jun. 2020.

MENDES, Laura Schertel. **A encruzilhada da proteção de dados no Brasil e o caso do IBGE**. *Jota*, 23.04.2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020>. Acesso em: 13 mar. 2020.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. In: *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91-108, jul./dez. 2011.

MOTA PINTO, Paulo. **Direitos de personalidade e direitos fundamentais**: estudos. Coimbra: Gestlegal, 2018, p. 642 e ss.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. Relator: Rosa Weber. Brasília, DF, 07 de maio de 2020. **Diário da Justiça Eletrônico**. Brasília, 20 nov. 2020. n. 276. Disponível em: https://portal.stf.jus.br/servicos/dje/listarDiarioJustica.asp?tipoPesquisaDJ=AP&classe=ADI&numero=6387#. Acesso em: 15 mar. 2024.

META, Plataforma. **Política de Privacidade**. 2024. Política de Privacidade explica como coletamos, usamos e compartilhamos suas informações. Disponível em: https://mbasic.facebook.com/privacy/policy/printable/. Acesso em: 15 mar. 2024.

LEITE, George Salomão. **Eficácia e aplicabilidade das normas constitucionais**. Brasília: Senado Federal, Conselho Editorial, 2020. (Edições do Senado Federal; v. 275).

SCHEUERMANN, Gabriela Felden. Dados pessoais como um direito fundamental autônomo a partir da Emenda Constitucional nº 115/2022. **Revista da Defensoria Pública RS**, Porto Alegre, v. 3, n. 33, p. 253-254, 22 maio 2023.

SILVA, José Afonso da. **Aplicabilidade das normas constitucionais**. 7. ed. 2. tir. São Paulo: Malheiros, 2008. p. 83.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei Geral de Proteção de Dados Pessoais (Lgpd)**. Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 abr. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Marco Civil da Internet**. Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 abr. 2024.

BRASIL. Supremo Tribunal Federal. Acórdão nº 91867. Relator: Gilmar Ferreira Mendes. Brasília, DF, 24 de abril de 2012. **Diário da Justiça Eletrônico**. Brasília: STF, 20 set. 2012.

BRASIL. Supremo Tribunal Federal. Acórdão nº 72588. Relator: Maurício José Corrêa. Brasília, DF, 12 de junho de 1996. **RTJ**. Brasília: STF, 04 ago. 2000. v. 174, n. 491.