CIÊNCIAS SOCIAIS APLICADAS EM REVISTA
Administração | Ciências Contábeis | Direito
ISSN: 1982-3037

Organização: Centro de Ciências Sociais Aplicadas
Unioeste – Mal. C. Rondon/PR
Disponível em: https://e-revista.unioeste.br/index.php/csaemrevista

Avaliado pelo sistema *double blind review*
Recebido: 27 jul. 2023 | Revisado: 26 fev. 2024| Aprovado: 18 ago. 2024
DOI: 10.48075/csar.v29i49.31590

O princípio da não autoincriminação e o acesso a banco de dados pessoal armazenado em nuvem no âmbito do processo penal

The principle of non-self-incrimination and access to a personal database stored in the cloud within the scope of criminal proceedings

Anderson Araujo Fernandes do Couto[1], Débora de Souza Demétrio[2], Gabriel Iago de Souza Cruz Cavalcante[3], Klemenson Marcolino[4] e Zedequias de Oliveira Júnior[5]

[1] Universidade Federal Fluminense, Graduando em Direito, email: andersoncouto@id.uff.br
[2] Universidade Federal de Roraima, Graduanda em Direito, email: deborawdemetriodd@gmail.com
[3] Universidade Federal de Roraima, Graduando em Direito, email: email: gabriel_iago_coc@hotmail.com
[4] Universidade Federal de Roraima, Graduando em Direito, email: eklemensonmarcolino@gmail.com
[5] Universidade Federal de Roraima, Doutor em Recursos Naturais pela Universidade Federal de Roraima-UFRR, Mestre em Direito Ambiental pela Universidade do Estado do Amazonas, Graduado em Direito pela Faculdade Anhanguera de Ciências Humanas, Professor da UFRR e Promotor de Justiça do Ministério Público do Estado de Roraima, email: zedequiasjunior@hotmail.com

RESUMO
O presente artigo tem por objetivo analisar o acesso a banco de dados pessoal armazenado em nuvem para fins de obtenção de provas durante a investigação e o processo penal em si, à luz do princípio da não autoincriminação - *nemo tenetur se detegere*. Realizou-se pesquisa documental e bibliográfica em doutrinas, jurisprudência dos tribunais superiores e na legislação pátria que versam acerca do tema, com abordagem metodológica qualitativa. Inicialmente a pesquisa apresenta reflexões acerca do princípio em comento, para então ser abordada a questão do armazenamento de dados em nuvem, obtenção de seu conteúdo como documento e seu tratamento para ser admitido como prova no âmbito do inquérito e da persecução penal. Ademais, a pesquisa contemplou a obrigatoriedade do fornecimento de dados armazenados em nuvem e a necessidade de determinação judicial para a quebra de sigilo e posterior acesso à nuvem pessoal. Assim, as principais conclusões alcançadas são que não é obrigatório ao acusado o fornecimento de senhas ou o franqueamento ao acesso a seus aparelhos eletrônicos, sob a proteção do princípio estudado, no entanto, fruto de determinação judicial para quebra do sigilo de comunicações privadas, os provedores de serviços de armazenamento de dados, mesmo estrangeiros, devem disponibilizá-los, sujeitando-se à legislação brasileira. Ademais, essa determinação judicial deve fundamentar-se em indícios razoáveis de autoria, na presença de materialidade delitiva e na plausibilidade das acusações, limitando-se ao necessário à busca da verdade real, sob pena de incorrer na devassa da vida privada, ferindo outros princípios fundamentais, como o superprincípio da dignidade da pessoa humana.
Palavras-chave: Autoincriminação. Processo penal. Armazenamento em nuvem. Quebra de sigilo.

ABSTRACT
This article aims to analyze the access to a personal database stored in the cloud for the purpose of obtaining evidence during the investigation and the criminal procedure itself, in light of the principle of non-self-incrimination - *nemo tenetur se detegere*. Documentary and bibliographical research was carried out in doctrines, jurisprudence of the superior courts and in the national legislation that deal with the subject, with a qualitative methodological approach. Initially, the research presents reflections on the principle under discussion, to then address the issue of cloud data storage, obtaining its content as a document and its treatment to be admitted as evidence within the scope of the investigation and of criminal prosecution. In addition, the research included the obligation to provide data stored in the cloud and the need for a court order to break secrecy and subsequent access to the personal cloud. Thus, the main conclusions reached are that it is not mandatory for the accused to provide passwords or grant access to their electronic devices, under the protection of the studied principle, however, as a result of a court order to break the confidentiality of private communications, data storage service providers, even foreign ones, must make them available, subject to Brazilian legislation.In addition, this judicial determination must be based on reasonable evidence of authorship, the presence of criminal materiality and the plausibility of the accusations, limited to what is necessary in the search for the real truth, under penalty of incurring the investigation of private life, violating other principles fundamental principles, such as the super principle of the dignity of the human person.
Key-words: Self-incrimination. Criminal proceedings. Cloud Storage. Breach of secrecy.

1 INTRODUÇÃO

Com a evolução da tecnologia, novas formas de armazenar e transmitir informações vão surgindo, criando novas possibilidades de provas que visam a alcançar a verdade real no processo. Atualmente existe a possibilidade de se armazenar todo tipo de arquivo em servidores interligados por meio da internet por meio da computação em nuvem, e, com a evolução tecnológica, vem se popularizando o uso de bancos de dados virtuais (FERNANDES et al., 2021). Nesse contexto, é fundamental a observação dos preceitos constitucionais e processuais penais na obtenção dessas provas.

Não obstante a possibilidade de produção de diversos tipos de prova, é peremptório que estas sejam lícitas, não podendo serem obtidas em violação a normas constitucionais ou legais (BRASIL, 1941). Uma das vedações presentes no ordenamento jurídico brasileiro é o princípio da não autoincriminação, conhecido como *nemo tenetur se detegere*, o qual implica em o acusado não poder ser obrigado a gerar prova contra si mesmo, sendo-lhe assegurado, por exemplo, a faculdade de não responder perguntas que lhe forem formuladas, não fornecer qualquer tipo de declaração, informar dados ou apresentar objeto que o incrimine direta ou indiretamente, tampouco produzir escrito de próprio punho para utilização em perícia (AVENA, 2023).

De igual modo, Lopes Jr. (2023) aduz que o silêncio do réu não pode importar em confissão de culpa por parte do investigado ou acusado, tampouco pode influenciar o convencimento do juiz, não podendo o silêncio prejudicar, de nenhuma forma o réu, constituindo-se em prova ilícita o interrogatório sob coação.

Dentre as tecnologias da informação e comunicação (TIC) da atualidade, os serviços de armazenamento de dados pessoais em nuvem, que, de acordo com Fernandes et al. (2021), têm a função de guardar e compartilhar arquivos que contenham dados de maneira segura, constituem-se fontes de possíveis provas para diversos tipos penais. Essa realidade desperta a necessidade de se estudar os limites ao acesso a dados pessoais, ante a proteção do princípio da não auto incriminação.

A imunidade à auto acusação é decorrência natural de uma série de princípios constitucionais, conforme ensina Nucci (2022), entre eles a presunção de inocência, a ampla defesa e o direito humano fundamental de manter o silêncio ante qualquer acusação. Assim, se o indivíduo é inocente até que se prove o contrário, possuindo o amplo direito de produzir provas em seu favor e de permanecer em silêncio sem nenhum prejuízo processual, conclui-se que não esteja, em nenhuma situação, obrigado a produzir prova contra si mesmo (NUCCI, 2022).

Esse princípio faz parte de um conjunto maior de princípios que conferem proteção ao réu ante o Estado, que é a parte mais forte na persecução penal, detentor de meios e agentes capazes de buscar e produzir provas contra o autor da infração penal, prescindindo da colaboração deste. Dentre esses princípios destaca-se o *in dubio pro reu* que garante que havendo dúvida razoável, o juiz deve decidir em favor do réu (NUCCI, 2022).

Assim, deve-se tratar com cautela o acesso a banco de dados pessoais com a finalidade de produzir provas, uma vez que, em primeira análise e com base no direito fundamentais do réu, este não poderia ser obrigado a franquear o acesso à nuvem pessoal, uma vez que se caracterizaria a produção de provas contra si mesmo.

Dessa maneira, e para elucidar a questão, serão tecidas reflexões acerca do princípio *nemo tenetur se detegere*, analisados aspectos da obtenção da prova na nuvem e estudada a possibilidade de fornecimento obrigatório de dados em virtude de quebra de sigilo.

2 REFLEXÕES ACERCA DO PRINCÍPIO *NEMO TENETUR SE DETEGERE*

Trata-se de um princípio de caráter garantista, visando a preservar a dignidade da pessoa humana, protegendo o acusado contra abusos e excessos durante a persecução penal, não havendo incompatibilidade entre este princípio e a busca pela verdade real no processo penal, uma vez que o Estado possui outros meios para constituir provas sem empreender violência física ou moral para compelir o réu a contribuir com a investigação (MALAQUIAS, 2014).

Esse princípio surgiu, como hoje se entende, na modernidade, após superado o modelo de provas tarifadas e a confissão como rainha das provas, o que levava à prática até mesmo da tortura, uma vez que o acusado era considerado um objeto do qual deveria ser extraída a verdade a todo custo (CASTRO, 2022).

Nas civilizações clássicas como Grécia e Roma, admitia-se a tortura para a obtenção de confissões e delações, permanecendo comum assa prática até a idade média, na qual era aceitável extrair a verdade do acusado a qualquer custo, em um contexto de processo inquisitório em que partia-se do pressuposto da culpa, e era inimaginável o direito ao silêncio (MALAQUIAS, 2014).

Com a gradativa exclusão da tortura dos meios estatais de obtenção de provas, e com a Declaração dos Direitos de Virgínia de 1774, da Declaração dos Direitos do Homem de 1789, o acusado deixou de ser mero objeto de prova e passou a ser tratado como sujeito de diretos, tendo direito à presunção da inocência (CASTRO, 2022).

O interrogatório é um verdadeiro ato de defesa, no qual o acusado deve exercer sua defesa

pessoal. Assim, a defesa pessoal negativa, que envolve a faculdade de permanecer em silêncio e não fazer prova contra si mesmo sem que isso implique em qualquer prejuízo para si, pode ser considerada não apenas um direito, mas também um dever (LOPES JR. 2023).

Não estar obrigado a produzir prova contra si mesmo, para Nucci (2023), é decorrência natural da confluência dos princípios constitucionais da presunção de inocência, da ampla defesa, e de o réu poder permanecer calado perante a qualquer acusação. Nesse sentido, o autor defende que o indivíduo é inocente até que seja provada sua culpa, podendo constituir provas em seu favor de maneira ampla, e podendo negar-se a falar, sem qualquer prejuízo, fica claro que não se pode forçar o acusado, em hipótese alguma, a gerar prova contra si mesmo.

Avena (2023) aduz, ainda, que, ao início de qualquer interrogatório, seja ele policial ou judicial, o acusado deve ser cientificado de que é albergado pelo direito de permanecer em silêncio, não podendo esse silêncio ser interpretado como uma confissão, nem tampouco influenciar o julgamento. Sobre o assunto, o autor ainda ressalta que essa garantia se estende a qualquer outro meio probatório, seja fornecer sua grafia para perícia, seja participar de acareação, seja contribuir na reconstituição do crime.

A expressão latina *nemo tenetur se detegere*, significa, em termos literais, “nada a temer por se deter” e se desdobra no direito ao silêncio e à autodefesa negativa (LOPES JR., 2023, p.207).

Outra consideração importante é a de que constitui-se abuso de autoridade prosseguir com o interrogatório de acusado que manifestou o desejo de permanecer em silêncio, assim, se, ao ser informado deste direito, o interrogado escolher por exercê-lo, o ato deve ser imediatamente encerrado, seja em âmbito policial, seja em âmbito judicial (AVENA, 2023).

No entanto, também é possível que o réu utilize-se do silêncio seletivo, que, conforme Avena (2023) é a hipótese em que o acusado decide não responder às perguntas de todos os atores processuais, procedimento comum em sede de Tribunal do Júri, por exemplo, ocasião na qual ocorre de o réu deixar de responder às perguntas do Ministério Público.

No que tange à legislação brasileira, o direito à não autoincriminação encontra guarida tanto na CRFB quanto na legislação infraconstitucional. A Carta Magna consagra expressamente o referido princípio no art. 5º, LXIII, ao mencionar que o preso deve ser informado de seus direitos, estando entre estes, o de permanecer calado, garantindo também a assistência familiar de advogado (BRASIL, 1988).

Tal previsão se encontra ainda no art. 8.2, g, da Convenção Americana Sobre Direitos Humanos (CADH), recepcionada pelo Decreto nº 678, de 6 de novembro de 1992, do qual é

possível extrair que toda pessoa acusada de delito, estando presa ou em liberdade, tem o direito de não ser obrigada a prestar depoimento que a incrimine, nem a declarar-se culpada (BRASIL, 1992).

O direito de silêncio é apenas uma manifestação de uma garantia muito maior, insculpida no princípio *nemo tenetur se detegere*, segundo o qual o sujeito passivo não pode sofrer nenhum prejuízo jurídico por omitir-se de colaborar em uma atividade probatória da acusação ou por exercer seu direito de silêncio quando do interrogatório (LOPES JR., 2023).

Infraconstitucionalmente, no Código de Processo Penal, há a sua previsão expressa, especificamente, no art. 186, parágrafo único, que teve a redação atual determinada pela lei 10.792/2003, passando a determinar que o silêncio não significa confissão e tampouco pode ser interpretado contra o acusado (BRASIL, 1941).

Cabe-se destacar o art. 198 do mesmo diploma legal que não teve sua redação alterada, indo de encontro ao artigo citado anteriormente, uma vez que possibilitaria ao juiz utilizar-se do silêncio do acusado para formar seu convencimento. Sobre o assunto, Nucci (2023) ensina que a parte final deste artigo não foi recepcionada pela nova ordem constitucional iniciada em 1988.

Nesse contexto, Pegoraro e Pegoraro (2019) pontuam que a não autoincriminação é aplicada em conjunto com outros princípios, que estabelecem limites à atuação do Estado na repressão do fato criminoso. Assim, não deve-se dissociá-lo dos princípios do devido processo legal, da presunção de inocência, da ampla defesa e da responsabilidade penal subjetiva (PEGORARO e PEGORARO, 2019)

3 NUVEM: A OBTENÇÃO DA PROVA DIGITAL

3.1 O ADVENTO DA PROVA DIGITAL

A Constituição Federal de 1988 (CRFB), em seu art. 5º, incisos X e XII, discorre sobre os direitos e as garantias individuais, em tese, invioláveis, dentre eles o sigilo de correspondência, das comunicações telegráficas, telefônicas e de dados (BRASIL, 1988). Tal direito pode ser excetuado por força de ordem judicial, para investigação criminal ou instrução processual, previsto em lei (BRASIL, 1966).

Sobre o dispositivo constitucional que trata de inviolabilidade, Lima (2020, p. 809) ressalta que “não há que se falar em direito fundamental absoluto. Todos os direitos fundamentais devem ser submetidos a um juízo de ponderação quando entram em rota de colisão com outros direitos fundamentais, preponderando aqueles de maior relevância”.

A tecnologia passou a integrar a rotina humana em um ambiente no qual alteram realidades de maneira imediata, já que não se resumem a ligações telefônicas, pois aglutinam diversos aplicativos contendo som, imagem, vídeo, mídias sociais, jogos e outras funções num único aparelho. (PARODI, 2022). Fruto disso, pessoas e lugares nunca estiveram tão conectados devido a trabalhos em home office, relações de amizade via redes sociais, interações em vários ambientes ao mesmo tempo, várias vezes por dia, todos os dias da semana (PARODI, 2022).

O fato é que vivemos cada vez mais num único mundo, na medida em que os indivíduos, grupos e nações estão cada vez mais interdependentes, e isso se traduz em impacto nos mais diversos campos da vida em sociedade, num processo de retroalimentação que é impulsionado pelo desenvolvimento tecnológico, e seu amplo espectro, que permite o fluxo de dados, voz e imagem, ao arrepio de quaisquer limitações territoriais existentes entre os países.

Por essa razão, o debate sobre a obtenção de dados com o uso de novas tecnologias se faz necessário. Por meio dos smartphones o acesso à internet aumentou consideravelmente na última década, com uma taxa de duas pessoas por aparelho em 2010, passando da marca de dois aparelhos por pessoa em 2021, um aumento de mais de 400% (MEIRELLES, 2021).

Em uma década, os smartphones tornaram-se a primeira opção de acesso à rede e principais responsáveis por sua expansão, ficando à frente dos computadores (PARODI, 2022). No ano de 2015, o número de dispositivos digitais passava de 300 milhões, cujo uso era de 50% para cada um deles. Em maio de 2021, o Brasil possuía 440 milhões desses dispositivos, dos quais 198 milhões eram computadores e 242 milhões eram smartphones, 53% do total (MEIRELLES, 2021).

Para acompanhar essa tendência tecnológica, a Lei nº 12.850/2013, que trata de organizações criminosas, também inovou ao dispor um capítulo para tratar da investigação e de meios de obtenção de prova, prevendo que, em qualquer fase da persecução penal, serão permitidas interceptações de comunicações telefônicas e telemáticas, entendida esta última como o procedimento que produz prova de documento eletrônico (BRASIL, 2013).

Com o aumento do uso de equipamentos eletrônicos e do uso da internet, a interceptação telemática ganhou mais espaço e utilidade. Contudo, os serviços em rede podem ser fornecidos de qualquer espaço, dispensando infraestrutura física, pessoal ou instalações no país dos usuários. Eles também não carecem de local específico para o armazenamento de dados, que é eleito segundo as conveniências do provedor de serviços, majoritariamente no intento de reduzir custos, otimizar lucros, proteger dados e oferecer melhor acesso e desempenho (GONÇALVES, 2017).

Já as ações para a busca de dados que necessitam de autorização judicial são classificadas,

de acordo com Gonçalves (2017), como ações de Inteligência Policial Judiciária. Tais ações são de natureza sigilosa e envolvem o emprego de técnicas especiais visando à obtenção de dados (indícios, evidências ou provas de autoria ou materialidade de um crime) (GONÇALVES, 2017).

Segundo uma interpretação extensiva e contemporânea do art. 232 do Código de Processo Penal, dados são documentos, porém armazenados em meio digital ou virtual. E, como são documentos, pode ser determinada a sua apreensão para instruir investigação criminal. No caso de dados virtuais, a forma de se obter esses documentos é por meio da determinação da quebra do sigilo legal e constitucional que os protege (BADARÓ, 2021).

3.2 A ERA DIGITAL EM EXPANSÃO

A grande quantidade de dispositivos digitais se assemelha a um enxame digital, ou seja, uma grande quantidade de pessoas conectadas à rede de computadores, por isso a identificação do usuário pode ser difícil, favorecendo o anonimato do homem digital no cometimento de crimes e na sensação de impunidade (HABOWSKI; CONTE, 2018). Em busca da verdade real, existe grande necessidade da quebra do sigilo de diálogos e dados, em busca de provas, sendo que muitas delas se assemelham aos emails, e têm a natureza jurídica de dados e não de conversas telefônicas, uma vez que o conteúdo dos diálogos fica arquivado, seja nos referidos dispositivos ou em locais externos, nas denominadas nuvens, diferente do que ocorre com ligações telefônicas convencionais, em que o registro se limita a aspectos periféricos da conversa, como números envolvidos, data e horário, mas sem a gravação do conteúdo dos diálogos ocorridos (HABOWSKI; CONTE, 2018).

Em busca de estratégias empresariais, os provedores de serviço de internet, percebendo a fragilidade da regulação estatal no ambiente virtual, comumente adotam dois caminhos: (a) prestam serviços em determinado país sem a presença de estabelecimento físico ou; (b) criam subsidiárias para funcionar no local, apenas com a função de vender serviços, mantendo o armazenamento sob o encargo de outro ente do grupo econômico, em país com a legislação que mais lhe beneficie (SMUHA, 2018). O objetivo é claro, maximizar as oportunidades, afastando qualquer empecilho em sentido contrário.

Por conseguinte, as provas aptas a elucidar delitos cometidos em determinado país, estão ordinariamente armazenados em território estrangeiro, sem conexão entre o caso sob investigação no Estado em questão e o Estado do local de armazenamento ou da sede principal do prestador de serviços, originando o que se tem chamado de globalização das evidências criminais (BADARÓ, 2021).

3.3 A NUVEM DE DADOS E AS PROVAS INTACTAS

Se antes os órgãos investigativos ocupavam-se majoritariamente com provas testemunhais, documentais e periciais (focadas em objetos materiais), cada vez mais os vestígios digitais assumem destaque na persecução criminal (GONÇALVES, 2017). Isso decorre de um motivo de todo evidente, visto que as ferramentas tecnológicas e as plataformas de mídia social atualmente ocupam espaço fundamental na vida em sociedade, servindo como uma das principais formas de armazenamento de fotos, documentos, mensagens de texto e de voz, vídeos, e-mails e outros tipos de arquivos. Exatamente por isso, Fernandes (2021) defende que o conteúdo compartilhado nessas plataformas e guardado em nuvem, que pode ser entendido como supostamente criminoso, passa a ser considerado como possível espécie de prova processual em específico, a prova digital.

Os principais provedores de serviços que mantêm dados em nuvem (ou de outra forma armazenados remotamente) que são frequentemente fonte de provas utilizadas em ações penais são Google (Google Drive e Gmail), Apple (ICloud), Microsoft (OneDrive e Outlook/Hotmail/Skype) e Facebook (FERNANDES, 2021).

No trato da questão de obtenção de provas eletrônicas, há o caso envolvendo prestadores de serviços estrangeiros em funcionamento no Brasil, a Corte Especial do Superior Tribunal de Justiça (STJ), harmonizando a legislação federal, tem entendimento consolidado no sentido de que o local de armazenamento não afasta a jurisdição do país para requisitar diretamente o fornecimento de metadados ou dados de conteúdo, imprescindíveis a descoberta de crime ocorrido em território nacional, envolvendo brasileiros (BRASIL, 2013).

O caso, que levou ao entendimento acima, tratava de recusa do Google Brasil em fornecer, diretamente às autoridades brasileiras, o conteúdo de e-mails trocados entre brasileiros investigados pela prática de crimes graves (associação criminosa, corrupção, lavagem de dinheiro etc), sob a justificativa que os dados estavam armazenados em território americano, ao abrigo da controladora Google Inc. Nesse passo, a subsidiária argumentou que além de não ter acesso ao conteúdo, a legislação americana proibia sua divulgação, salvo por meio da assistência jurídica mútua (FERNANDES, 2021).

Posteriormente, a Lei 12.965/14, conhecida como Marco Civil da Internet (MCI) regulou o assunto no Art. 11, caput, §§1.º e 2.º:

> Art. 11. (...).
> § 1.º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja

> localizado no Brasil.
> § 2.º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil (BRASIL, 2014).

Como se percebe, o MCI alarga os critérios da jurisprudên, sujeitando as pessoas jurídicas estrangeiras à lei brasileira, ainda quando não tenham sede no Brasil, desde que prestem serviço no país, sempre que qualquer operação de coleta, armazenamento, guarda, tratamento de metadados ou dados de conteúdo tenha ocorrido em território nacional. Antes dela, o Art. 11, §1.º da Lei de Introdução às normas do Direito Brasileiro Brasil, (1942) e o Art. 21, parágrafo único do Código de Processo Civil Brasileiro Brasil, (2015) previam que a pessoa jurídica estrangeira que tivesse agência, filial ou sucursal no Brasil, ficaria sujeita à lei naciona.

A necessidade premente, obstaculizada pelo armazenamento de dados em nuvem, com data centers situados em território estrangeiro e estratagemas societários que cindem as funções de uma pessoa jurídica prestadora de serviços, por meio de subsidiárias, tem levado a uma reação da Justiça brasileira quanto a artificial maneira de definir o território competente, em evidente prejuízo à soberania e à jurisdição.

Destarte, nas situações em que os dados eletrônicos circunscritos a nacionais e residentes suspeitos da prática de crime em determinado país, o fato de as provas estarem armazenadas em outro território não tem o condão de impedir sua obtenção direta pelas autoridades competentes. Dessa maneira, o acesso aos dados constantes em nuvem, por vezes o torna crucial para o fiel cumprimento da legislação pátria e cooperação na elucidação de condutas ilícitas, especialmente quando regularmente quebrado por decisão judicial o sigilo de dados dos envolvidos (GONÇALVES, 2017).

Nessa perspectiva, quando o órgão investigativo entender que o acesso ao conteúdo digital armazenado em nuvem é importante para a elucidação dos fatos, ele deve solicitar formalmente ao juízo competente que determine a quebra de sigilo dos dados telemáticos armazenados em um determinado provedor de serviços de nuvem (como as empresas Google, Apple, Microsoft e outras) (FERNANDES, 2021).

O armazenamento em nuvem é uma estratégia empresarial que não interfere na obrigação de observância da legislação brasileira quando o serviço é prestado em território nacional, logo, empresas que prestam serviços de aplicação na internet em território brasileiro devem necessariamente se submeter ao ordenamento jurídico pátrio, independentemente da circunstância

de possuírem filiais no Brasil.

Portanto, o armazenamento em nuvem, estrategicamente utilizado por diversas empresas nacionais e estrangeiras, que possibilita que armazenem dados em todos os cantos do globo, não pode interferir na obrigação de entregá-los às autoridades judiciais brasileiras quando envolvam a prática de crime em território nacional (MEIRELLES, 2021).

O aparente conflito de jurisdição na produção probatória é solucionado ao afastar o fictício vínculo criado com o país estrangeiro, decorrente de estratégia empresarial deturpada dos instrumentos do Direito Internacional Privado. A filial brasileira de empresa com sede no exterior, sendo pessoa jurídica de direito interno, deve se submeter à legislação vigente no país. Essa necessidade já foi afastada por precedente da Corte Especial do STJ, como se pode ver da seguinte ementa de julgamento:

> QUESTÃO DE ORDEM. DECISÃO DA MINISTRA RELATORA QUE DETERMINOU A QUEBRA DE SIGILO TELEMÁTICO (GMAIL) DE INVESTIGADOS EM INQUÉRITO EM TRÂMITE NESTE STJ. GOOGLE BRASIL INTERNET LTDA. DESCUMPRIMENTO. ALEGADA IMPOSSIBILIDADE. INVERDADE. GOOGLE INTERNATIONAL LLC E GOOGLE INC. CONTROLADORA AMERICANA. IRRELEVÂNCIA. EMPRESA INSTITUÍDA E EM ATUAÇÃO NO PAÍS. OBRIGATORIEDADE DE SUBMISSÃO ÀS LEIS BRASILEIRAS, ONDE OPERA EM RELEVANTE E ESTRATÉGICO SEGUIMENTO DE TELECOMUNICAÇÃO. TROCA DE MENSAGENS, VIA E-MAIL, ENTRE BRASILEIROS, EM TERRITÓRIO NACIONAL, COM SUSPEITA DE ENVOLVIMENTO EM CRIMES COMETIDOS NO BRASIL. INEQUÍVOCA JURISDIÇÃO BRASILEIRA. DADOS QUE CONSTITUEM ELEMENTOS DE PROVA QUE NÃO PODEM SE SUJEITAR À POLÍTICA DE ESTADO OU EMPRESA ESTRANGEIROS. AFRONTA À SOBERANIA NACIONAL. IMPOSIÇÃO DE MULTA DIÁRIA PELO DESCUMPRIMENTO.(BRASIL, 2013)

Assim, tendo a autoridade judicial requisitado informações atinentes à apuração de um crime praticado no território brasileiro, deve a empresa controlada prestá-las, sem que para isso tenham que ser acionados os meios diplomáticos para a sua obtenção.

3.4 ADMISSIBILIDADE DAS PROVAS DIGITAIS

Toda prova, digital ou não, precisa ser produzida de acordo com as normas constitucionais, advindas de tratados e convenções internacionais de que o Brasil seja parte, e também de normas infraconstitucionais, a exemplo do MCI, para ser assim considerada lícita e, por via de consequência ser admitida no processo. A inobservância às determinações legais resulta na ilicitude da prova e no seu desentranhamento, conforme previsto no artigo 5º, inciso LVI, da Constituição (BRASIL, 1988) e no artigo 157 do Código de Processo Penal brasileiro (BRASIL, 1941).

O fato dos grandes provedores e gerenciadores da nuvem como, Google, Facebook, Apple, entre outros, estarem sediados em outros países, não tem o condão de eximi-los do cumprimento

das leis e decisões judiciais brasileiras, uma vez que disponibilizam seus serviços para milhões de usuários que se encontram em território nacional. Como visto antes, em seu art. 11, o MCI é claro na determinação de aplicação da legislação brasileira a operações de coleta, armazenamento, guarda e tratamento de dados por provedores de aplicações, exigindo apenas que um desses atos ocorra em território nacional (FERNANDES, 2021).

A prova digital, diferente de outros tipo de prova, exige maior cautela durante a sua produção e manuseio, em razão de suas características estritamente peculiares, já que possui caráter não material, isto é, não palpável, que não possui uma materialidade imediatamente constatável, além de sua congênita mutabilidade. Por essa razão, a prova digital assume um caráter de maior vulnerabilidade e fragilidade, tornando-se ainda mais passível de destruição, contaminação e falsificação (PARODI, 2022).

Assim sendo, existe ainda, além da necessária decisão judicial para deferir o pedido de quebra de sigilo rigorosamente fundamentada, é preciso assegurar que o dado ou arquivo digital não sofra nenhuma alteração ou contaminação, seja ela voluntária ou involuntária, garantindo-se a sua autenticidade e fiabilidade (PARODI, 2022).

A validação deste ciclo de obtenção de provas coletadas nas nuvens, finaliza-se com o seu armazenamento por uma segura cadeia de custódia que consiste em um mecanismo voltado a garantir a autenticidade das evidências coletadas e examinadas, de maneira que se assegure que correspondem ao caso investigado, evitando que haja lugar para qualquer tipo de adulteração (LIMA, 2020).

Neste caso, em que pese o Código de Processo Penal ser silente quanto às especificidades de cada prova digital, existem normas gerais e técnicas que tratam de sua gestão e de sua cadeia de custódia, além de estabelecerem diretrizes específicas ao tratamento a ser dado às evidências digitais. Existem, porém, normas gerais sobre a gestão das provas e de sua cadeia de custódia (artigos 158, 158-A a 158-F e 159 CPP, Portaria Senasp nº 82/2014, entre outros) e, de forma mais ampla, sobre a necessidade de garantir o acesso da defesa às provas íntegras e integrais (artigo 5º CF).

Existem também normas técnicas que tratam do assunto, notadamente a norma ABNT ISO IEC 27037:2013, vigente no país desde 2014, gerida pelo órgão brasileiro de normatização técnica, que prevê procedimentos próprios a serem observados para que haja a adequada custódia das evidências digitais. Esses procedimentos são: (1) a devida identificação dos dispositivos de armazenamento de mídia digital e aqueles que podem conter evidência digital relevante; (2) a coleta

da evidência digital, que será removida da localização original em que ocupa e será remetida a um ambiente controlado; (3) a aquisição, consistente na produção de cópia da evidência digital e documentação dos métodos utilizados; e (4) a preservação da evidência, consistente na proteção desta contra possíveis adulterações (PARODI, 2022).

E com o objetivo de garantir a integridade da evidência digital, a referida norma ainda recomenda o uso da função *hash*, que é um número indicadors individualizado, que é gerado por algoritmo, capaz de verificar se uma imagem é idêntica à mídia de origem, o *hash verificado* (PARODI, 2022).

Nesse sentido, o *hash* possui a finalidade de documentar a manutenção da integridade dos arquivos, ou seja, registrar que eles não sofreram alteração após a apreensão. Tudo isso com objetivo de se evitar que um determinado dado colhido seja posteriormente modificado, substituído ou eliminado sem que haja qualquer rastro de alteração.

Devido às peculiaridades da prova digital, a ausência de uma identificação segura e que garanta preservação desse dado acarreta risco iminente de sua manipulação. E é essa inviabilidade de identificar possíveis alterações que ocasiona a quebra da cadeia de custódia da prova e gera patente prejuízo ao réu/investigado, que será impossibilitado de contraditar uma evidência cujas origens e meios de obtenção são desconhecidos. Isso pode gerar, por consequência, a inadmissibilidade de uma prova digital.

4 O FORNECIMENTO OBRIGATÓRIO DE DADOS E A QUEBRA DE SIGILO

É fato ressaltar que houve a ampliação do meio de prova a partir da utilização de computadores, smartphones, tablets etc. Anteriormente, o meio de prova se restringia principalmente a documentos físicos, testemunhos orais e objetos tangíveis. No entanto, a tecnologia trouxe consigo novas formas de provas as quais se tornaram poderosas ferramentas para a coleta e apresentação de evidências em diversos contextos, incluindo o campo jurídico. Intrinsecamente a estes meios, relacionam-se como valor probatório arquivos, chamadas telefônicas, e-mails, interações sociais, mídias, geolocalização, dados armazenados em nuvem e quaisquer outras formas legais à persecução penal por meio digital.

Ao passo que os aparelhos eletrônicos tornaram-se fontes de grandes depositários de informações, especificamente, os dados armazenados em nuvem, importa-se tratar acerca do acesso a estes diante o processo penal. Conforme art. 7º, incisos II e III, da Lei nº 12.965/14 (BRASIL,

2014), vê-se a fundamentação legal acerca do acesso aos dados armazenados, respectivamente, *in verbis*:

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

Assim como no art. 5º, inciso XII, da CRFB (BRASIL, 1988)

> Art. 5º [...] XII - e 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;

O avanço tecnológico e a era digital têm gerado debates sobre como conciliar esse direito fundamental com a necessidade de investigação e obtenção de provas digitais para fins legais. Por vezes, não se alcança um resultado desejável quando da aplicação de dispositivos legais acerca de provas físicas aos meios de produção de provas digitais, pois acaba-se por efetuar acessos não autorizados, constituindo-se em atos invasivos da privacidade mediante investigações que contrariam o sigilo de dados estabelecido e assegurado pela Constituição Federal.

Cresce a importância de se limitar as investigações à exploração de dados armazenados em nuvem por meio de procedimentos adequados para a coleta e uso dessas informações. As informações obtidas por dados em nuvem podem se enquadrar em uma infinidade de aspectos (ex.: dados bancários) que possuem seu devido amparo de inviolabilidade do sigilo, logo, a partir disso, nota-se sua essencialidade. É fato que a adoção de objetividade e procedimentos a essa medida impactaria a não caracterização de abuso por parte dos agentes, protegeria a privacidade individual, garantindo o equilíbrio entre a investigação e a preservação dos direitos fundamentais, além de não anular os meios de provas até então obtidos ao se ater ao objeto pretendido.

A premissa da garantia constitucional do princípio do *nemo tenetur se detegere*, em que ninguém é obrigado a produzir prova contra si, a se auto-incriminar, a fornecer informações ou provas que possam incriminá-lo em processo penal, possui implicações importantes quanto ao fornecimento obrigatório de dados. Especificamente no tocante aos dados em nuvem, ninguém será obrigado a fornecer senhas, acessos de *emails*, a desbloquear aparelhos móveis, a transferir dados em nuvem, ou quaisquer formas que possam caracterizar o fornecimento de evidências autoincriminatórias em dispositivos ou banco de dados pessoais.

Justificativas fundamentadas no art. 5º, inciso LXIII, CRFB *in verbis*: *"*o preso será informado de seus direitos, entre os quais o de permanecer calado, sendo-lhe assegurada a assistência da família e de advogado.", preconizando também o direito ao silêncio do preso em não importar parcialidade do juízo e/ou consequências penais. Dessa forma, o réu não tem obrigação de fornecer dados armazenados em nuvem a quem o requerer, inclusive há alguns entendimentos em que o fornecimento voluntário de senhas e dados por parte do réu ou anuir que acessem seus dados tornar-se-iam nulos, exceto mediante ordem judicial (requisição), como se prevê no art. 7º, inciso III, da Lei Federal nº 12.965 e art. 5º, inciso XII, da Constituição Federal. Perfaz-se a necessidade de requisição de dados em juízo, conforme expressa Antonialli e Fragoso (2019, p. 144)

> Conquanto a redação do citado dispositivo mencione "comunicações privadas armazenadas" e nem todos os dados e documentos contidos em um aparelho eletrônico sejam, necessariamente, provenientes de uma "comunicação privada", a nova disciplina conferida pela Lei 12.965/2014 ocasionou uma alteração na orientação jurisprudencial, que começou a considerar o acesso ao conteúdo de tais dispositivos objeto de reserva jurisdicional, com destaque para o Superior Tribunal de Justiça, que a partir de 2016 passou a anular decisões lastreadas na obtenção de dados armazenados em equipamentos eletrônicos sem autorização prévia do Poder Judiciário [...].

Importante expor que as mensagens e dados armazenados acabam por receber proteção contra o risco de iminente invasão da esfera íntima e privada das pessoas (ANTONIALLI; ABREU, 2018). O Estado deve ainda evitar ações invasivas quando da exploração dos dados armazenados, que devem ser fundamentadas em indícios razoáveis de autoria, lapso temporal quanto ao fato e a proporcionalidade da medida, portanto, a quebra de sigilo de dados contempla a fixação do lapso temporal, período estritamente necessário à obtenção da prova como a identificação precisa do objeto investigado que se pode buscar, fundamentados por ordem judicial (NARDELLI, 2021).

Como expressa Antonialli e Fragoso (2019, p. 52) "deve haver a autorização judicial mesmo nos casos em que há autorização do titular do telefone, porque o acesso afeta outras pessoas. Ao contrário disso, a prova se torna ilícita, logo, deve haver autorização judicial", que se vê no julgado abaixo em que houve a nulidade de provas digitais obtidas por policiais, mesmo que com o consenso do réu, pois não se precedeu de ordem/autorização judicial,

> PENAL. PROCESSUAL PENAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. TRÁFICO DE DROGAS. NULIDADE DA PROVA. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL PARA A PERÍCIA NO CELULAR. CONSTRANGIMENTO ILEGAL EVIDENCIADO.
> 01. Ilícita é a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente

> pela polícia em celular apreendido no flagrante, sem prévia autorização judicial.
> 02. Recurso ordinário em habeas corpus provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos. (BRASIL, 2018)

Destarte, resta evidente que só haverá acesso a dados em nuvem mediante autorização judicial, não havendo a possibilidade de seu fornecimento obrigatório à autoridade competente ou até mesmo por consentimento do réu, salvo reivindicada prévia ordem judicial, hipótese fundamentada pelo MCI e CRFB nos dispositivos já citados que asseguram a inviolabilidade e o sigilo de dados armazenados e das comunicações. A quebra de sigilo de dados somente será procedida após ordem judicial, conforme Antonialli e Abreu (2018, p. 103) de que "os juízes a noção de que o acesso às comunicações eletrônicas armazenadas dependeria de ordem judicial fundamentada, independentemente da finalidade penal da medida ou da natureza do crime objeto de investigação."

Acerca da quebra do sigilo de dados armazenados em nuvem importante destacar julgado do TJDFT, sobre a quebra de sigilo de dados armazenados no *gmail* e *google drive*, em investigação de crime de concorrência desleal.

> 1. Conforme entendimento do Supremo Tribunal Federal, a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação "de dados" e não dos "dados em si mesmos".
> 2. Os dados armazenados em nuvem não evidenciam uma comunicação de dados, mas representam o armazenamento de dados em um provedor de serviços na nuvem ("cloud storage"). Nessa medida, a quebra de sigilo referente a dados armazenados em nuvem não está abrangida pela Lei nº 9.296/96, uma vez que não há interceptação; e sim o conhecimento quando eles já foram armazenados. [...]
> 4. Portanto, mostra-se inviável a aplicação da Lei de Interceptações Telefônicas para a quebra de sigilo de correspondências eletrônicas, porquanto a sua apreciação recai sobre dados em si mesmos, e não sobre fluxo de informações. Ademais, de se observar que o artigo 7º, inciso III, da Lei nº 12.965 (Marco Civil da Internet) excepciona a inviolabilidade e sigilo de comunicações privadas armazenadas diante de ordem judicial. (DISTRITO FEDERAL, 2020).

O Relator ressalta que estes não são regidos pela Lei de Interceptação Telefônica, tendo em vista que não se caracteriza comunicação de dados ou fluxo de comunicações, pois se trata de acesso a dados/informações armazenadas em um provedor de serviços na nuvem, e sua inviolabilidade é garantida pela Lei do MCI, salvo a quebra mediante ordem judicial.

5 CONSIDERAÇÕES FINAIS

Dados em nuvem são documentos, e como tal estão sujeitos a que seja determinada a sua apreensão por meio da quebra de sigilo legal e constitucional pela autoridade competente. Nesse contexto, o mundo digital favorece o anonimato, atraindo transgressores da lei, que se utilizam da dificuldade da obtenção de dados por vias tradicionais para permanecerem impunes.

Soma-se a isso a fragilidade da regulação estatal do ambiente virtual, permitindo que as prestadoras de serviço hospedem os dados no exterior, onde a legislação mais lhe beneficie, muitas vezes mantendo apenas uma representação no país, gerando a chamada globalização das evidências criminais.

Com o papel de destaque assumido pelos vestígios digitais gerados pela crescente interação nas redes sociais, a busca pela verdade real em conteúdo armazenado em bancos de dados em nuvem se tornou crucial, uma vez que se tornaram fonte de provas, as provas digitais. Nesse contexto, o MCI sujeita as pessoas jurídicas estrangeiras à lei brasileira, bastando prestarem serviço no Brasil, que devem apresentar informações atinentes à apuração de crimes praticados em solo nacional, tendo em vista que, por vezes, os únicos meios de prova disponíveis encontram-se armazenados em nuvem. Assim, legitima-se a quebra do sigilo por decisão judicial, sem que seja necessário utilizar-se de meios diplomáticos para a tramitação de tais dados.

No entanto, toda prova, seja digital ou não, deve ser produzida em observância dos preceitos legais, sob pena de se tornar ilícita, e por conseguinte não ser admitida no processo penal. A característica não material e a mutabilidade das provas digitais, tornam-na especialmente frágil a contaminação, destruição e falsificação, o que leva à necessidade de garantia que seja autêntica e confiável, devendo-se observar a adequada cadeia de custódia, o que passa pela adequada identificação do dispositivo de armazenamento, a adequada coleta da evidência, a documentação dos métodos utilizados para sua aquisição e a preservação dessa evidência contra adulterações. Assim, a falta da preservação adequada da cadeia de custódia no que tange à prova digital, pode levar à sua inadmissibilidade.

No contexto da prova digital, e sob a égide do princípio da não autoincriminação, não pode haver a obrigatoriedade de o acusado desbloquear aparelho celular, fornecer senha de banco de dados ou mesmo transferir informações pessoais, sendo possível declarar a nulidade de decisões baseadas em provas obtidas de dispositivos eletrônicos pessoais sem autorização judicial, mesmo com anuência do réu, em especial a partir da vigência da Lei nº 12.965.

Ressalta-se ainda que a quebra do sigilo deve ser fundamentada em indícios razoáveis de autoria e com período estritamente necessário à obtenção da prova, para se evitar a devassa na vida privada por ações invasivas do Estado.

Assim, o acesso a dados armazenados em nuvem não se caracteriza em interceptação, uma vez que os dados já se encontram armazenados, devendo a quebra do sigilo recair sobre os dados em si, e não sobre o fluxo de informações. Sendo, para esse fim, necessário a determinação judicial da quebra de sigilo de comunicações privadas, amparado no MCI. Tal determinação deve ser fundamentada, e as informações obtidas devem receber tratamento especial, a fim de garantir sua incorruptibilidade e confiabilidade na busca pela verdade real no processo penal.

Por fim, conclui-se que devido ao princípio da não autoincriminação, o acesso a banco de dados pessoal armazenado em nuvem só pode ser realizado mediante ordem judicial fundamentada, sendo vedado qualquer meio de compelir o acusado a fornecer o acesso, sob pena de nulidade do feito, invalidando as provas adquiridas nesse contexto.

REFERÊNCIAS

ANTONIALLI, Dennys; FRAGOSO, Nathalie. **Direitos fundamentais e processo penal na era digital**: doutrina e prática em debate. São Paulo: Internetlab, 2019. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2019/08/InternetLabCongressoII_dupla.pdf. Acesso em 17 maio 2023.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. **Direitos Fundamentais e Processo Penal na Era Digital**: doutrina e prática em debate. São Paulo: Internetlab, 2018. Disponível em: https://www.santoandre.sp.gov.br/pesquisa/ebooks/418910.pdf. Acesso em 17 maio 2023.

AVENA, Norberto. **Processo Penal**. 15. ed. Rio de Janeiro: Grupo GEN, 2023. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559647774/. Acesso em: 30 jun. 2023.

BADARÓ, Gustavo. **Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia**. Boletim IBCCRIM – Ano 29 – Nº 343 – junho/2021. p. 7. Disponível em: PDF.js viewer (badaroadvogados.com.br). Acesso em 12 maio 2023.

BRASIL. 1ª Câmara Criminal do TJDFT. Acórdão nº 1276346. Relator: Desembargador JOÃO TIMÓTEO. Brasília, DF, 19 de agosto de 2020. **Poder Judiciário da União**. Brasília. Disponível em: 1276346.pdf (internetlab.org.br). Acesso em 17 maio 2023.

BRASIL. Superior Tribunal de Justiça. PENAL. PROCESSUAL PENAL. RECURSO EM HABEAS CORPUS. HOMICÍDIO TENTADO. NULIDADE DA PROVA. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL PARA A PERÍCIA NO CELULAR. CONSTRANGIMENTO ILEGAL EVIDENCIADO. Recurso em Habeas Corpus nº 83.681. Carla de Oliveira Gomes e

Ministério Público do Estado de São Paulo. Relator: Ministro Nefi Cordeiro. DJ, Acórdão 21 ago. 2018. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700958225&dt_publicacao=03/09/2018. Acesso em: 18 maio 2023.

_____. Código de Processo Penal. decreto lei nº 3.689, de 03 de outubro de 1941. Disponível em: http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm Acesso em: 10 mai. 2023.

_____. Código de Processo Civil. Lei nº 13.105, de 16 de março de 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 10 mai. 2023.

_____. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 16 mai. 2023.

_____. Decreto nº 678, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF, 1992. Disponível em: D678 (planalto.gov.br). Acesso em: 30 jun. 2023.

_____.Lei de Introdução às normas do Direito Brasileiro. Decreto lei nº 4.657, de 4 de setembro de 1942. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso em 15 de mai. 2023.

_____. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do Art. 5º da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 21 maio 2023.

_____. Lei nº 12850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, meios de prova, infrações penais e correlatas e o procedimento criminal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm Acesso em: 21 maio 2023.

_____. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://bit.ly/3R3IhpA . Acesso em: 21 maio 2023.

_____. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm . Acesso em 21 mai. 2023.

_____. Ministério da Justiça Doutrina Nacional de Inteligência de Segurança Pública – DNISP. 4. ed. rev. e atual. Brasília. Secretaria Nacional de Segurança Pública, 2016. Disponível em: DSpace MJ: Portaria nº 2, de 12 de janeiro de 2016. Acesso em 21 maio 2023.

_____. Superior Tribunal de Justiça. Inquérito n.º 784/DF. Relatora Ministra Laurita Vaz. 28 de ago. 2013. Disponível em: https://bit.ly/3RehtD6 . Acesso em: 21 mai. 2023.

_____, Supremo Tribunal Federal. (2. Turma). Habeas Corpus nº 96986/MG. Relator: Min. Gilmar

Mendes, 15 maio. 2012. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur214433/false . Acesso em 16 maio 2023.

CASTRO, B. G. DE. A GARANTIA DA NÃO AUTOINCRIMINAÇÃO NO PROCESSO PENAL BRASILEIRO. **Virtuajus**, v. 7, n. 12, p. 151-162, 6 abr. 2022. Disponível em: Vista do A GARANTIA DA NÃO AUTOINCRIMINAÇÃO NO PROCESSO PENAL BRASILEIRO (pucminas.br). Acesso em: 30 jun. 2023.

DANTAS, Dimitrius. PF pode acessar arquivos do celular de Torres pela 'nuvem', mas sucesso depende de 'sorte'. O Globo, 2023. Disponível em: https://oglobo.globo.com/politica/noticia/2023/01/pf-pode-acessar-arquivos-do-celular-de-torres-pela-nuvem-mas-sucesso-depende-de-sorte-alertam-peritos.ghtml . Acesso em: 16 maio 2023.

DISTRITO FEDERAL, Tribunal de Justiça do Distrito Federal e dos Territórios. **Inviolabilidade das comunicações telefônicas não alcança correio eletrônico e dados em nuvem**. 2021. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/fevereiro/correio-eletronico-e-dados-em-nuvem-podem-ter-sigilo-quebrado-por-ordem-judicial#:~:text=Acrescentou%20que%20a%20quebra%20de,mas%20acesso%20a%20informa%C3%A7%C3%B5es%20armazenadas . Acesso em: 18 maio 2023.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e dos Territórios. Agravo Regimental Criminal 0714619-24.2020.8.07.0000. Relator: Desembargador João Timóteo. DJ, Acórdão 19 agosto 2020. Disponível em: 1276346.pdf (internetlab.org.br). Acesso em: 25 jun. 2023

DUARTE, Evandro C. Piza. **Criminologia & racismo**. Curitiba: Juruá, 2002.

FERNANDES, Márcio Aurélio de Souza et al. Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da Computação em Nuvem. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E42, p. 374-385, 2021. Disponível em: Impactos-da-Lei-de-Proteção-de-Dados-LGPD-brasileira-no-uso-da-Computacao-em-Nuvem.pdf (researchgate.net). Acesso em: 29 jun. 2023

FLOR, Ana. **PF tenta obter, via nuvem de dados, informações de celular que Torres não trouxe ao Brasil**. G1, 2023. Disponível em: http://bit.ly/3HeynOi . Acesso em: 18 maio 2023.

GONÇALVES, Joasnival Brito. Atividade de inteligência e legislação correlata. 5. ed. Niterói, RJ: Impetus, 2017.

HABOWSKI, Adilson Cristiano; CONTE, Elaine. Resenha de HAN, Byung-Chul. No enxame: perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. Crítica Cultural – Critic, Palhoça, SC, v. 16, n. 1, p. 125-131, jan./jun. 2021. Disponível em: Vista do RESENHA DE HAN, BYUNG-CHUL. NO ENXAME: PERSPECTIVAS DO DIGITAL. TRADUÇÃO DE LUCAS MACHADO. PETRÓPOLIS: VOZES, 2018 (animaeducacao.com.br). Acesso em: 30 jun. 2023.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**. Volume único. 8. ed. Salvador. Editora

JusPodivm, 2020.

LOPES JR., Aury. **Direito Processual Penal.** 20. ed. São Paulo: SaraivaJur, 2023. ePUB. Disponível em: https://app.minhabiblioteca.com.br/books/9786553626355. Acesso em: 30 jun. 2023.

MALAQUIAS, Roberto Antônio Darós. Princípio nemo tenetur se detegere no estado democrático de direito. **Revista dos Tribunais**. ano, v. 103, p. 145-176, 2014. Disponível em: Art-DAROS-Principio-Nemo-Tenetur-Detegere-RT-libre.pdf (d1wqtxts1xzle7.cloudfront.net). Acesso em 30 jun. 2023.

MEIRELLES, Fernando de Souza. Uso da TI - Tecnologia de Informação nas Empresas: Pesquisa Anual do FGVcia 32. ed. 2021. Disponível em: https://eaesp.fgv.br/producao-intelectual/pesquisa-anual-uso-ti. Acesso em: 19 maio 2023.

MOTTA, Eduardo Titão. Cadeia de custódia da prova digital e a ilegalidade do uso de prints de tela como elementos de prova no processo penal. Instituto Brasileiro de Direito Penal Econômico, 2022. Disponível em: https://ibdpe.com.br/cadeia-de-custodia-da-prova-digital-e-a-ilegalidade-do-uso-de-prints-de-tela-como-elementos-de-prova-no-processo-penal/#_ftn6 Acesso em: 16 maio 2023.

NUCCI, Guilherme de S. **Manual de Processo Penal**. 3. ed. Rio de janeiro: Grupo GEN, 2022. *E-book.* Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559643691/. Acesso em: 30 jun. 2023.

PARODI, Lorenzo. Cadeia de custódia das provas digitais vindas das nuvens, à luz do CPP. Revista Consultor Jurídico, 10 de abril de 2022. Disponível em: https://www.conjur.com.br/2022-abr-10/lorenzo-parodi-cadeia-custodia-provas-digitais . Acesso em: 16 maio 2023.

PEGORARO, C. P.; PEGORARO, L. N. **O DIREITO À NÃO AUTOINCRIMINAÇÃO**: ASPECTOS TEÓRICOS E PRÁTICOS NA LEGISLAÇÃO INFRACONSTITUCIONAL. *In:* CONGRESSO NACIONAL DO CONPEDI, XXVIII., 2019, BELÉM – PA. **Anais** [...]. Belém: Conselho Nacional de Pesquisa e Pós-Graduação em Direito, 2019. p. 100-115, Disponível em:O Direito à não Autoincriminação Aspectos Teóricos e Práticos na Legislação Infraconstitucional (conpedi.org.br). Acesso em: 30 jun. 2023.

SMUHA, Nathalie A. Towards the EU Harmonization of Access to Cross-Border E Evidence: Challenges for Fundamental Rights & Consistency. European Criminal Law Review, vol. 8(1), 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3501421. Acesso em: 30 jun. 2023.