



ESCOLA DA MAGISTRATURA DO ESTADO DO RIO DE JANEIRO

ANÁLISE CRÍTICA SOBRE A SUSPENSÃO DOS SERVIÇOS DE
TELECOMUNICAÇÃO POR ORDEM JUDICIAL E A POSITIVAÇÃO DA PROVA
DIGITAL.

Thuane Ângela Sendreti de Oliveira

Rio de Janeiro
2020

THUANE ÂNGELA SENDRETI DE OLIVEIRA

ANÁLISE CRÍTICA SOBRE A SUSPENSÃO DOS SERVIÇOS DE
TELECOMUNICAÇÃO POR ORDEM JUDICIAL E A POSITIVAÇÃO DA PROVA
DIGITAL.

Artigo científico apresentado
como exigência de conclusão de Curso de
Pós-Graduação *Lato Sensu* da Escola
da Magistratura do Estado do Rio de
Janeiro.

Professores Orientadores:
Mônica C. F. Areal
Nelson Carlos Tavares Jr.

Rio de Janeiro
2020

ANÁLISE CRÍTICA SOBRE A SUSPENSÃO DOS SERVIÇOS DE TELECOMUNICAÇÃO POR ORDEM JUDICIAL E A POSITIVAÇÃO DA PROVA DIGITAL

Thuane Angela Sendreti de Oliveira

Graduada pela Universidade de Barra
Mansa - UBM. Advogada.

Resumo – com a era digital em voga, decisões judiciais são proferidas no sentido de suspender os serviços de comunicação como sanção, no entanto o argumento jurídico usado para amparar essas medidas são frágeis. O presente trabalho visa analisar a constitucionalidade das sanções impostas, de modo a privilegiar o direito a comunicação e privacidade, além de ressaltar a importância da regulamentação da prova digital no ordenamento jurídico brasileiro. Nesse prisma, serão analisados dispositivos da Lei nº 12.965/2014, doutrina e artigos científicos sobre a criptografia.

Palavras-chave – Direito Constitucional. Marco Civil da Internet. Suspensão dos serviços de comunicação. Direito à privacidade e comunicação. Criptografia. Direito Processual Penal. Prova digital.

Sumário – Introdução. 1. A fundamentação jurídica para suspensão dos serviços de telecomunicação e o conflito de constitucionalidade na proteção dos direitos à privacidade e comunicação. 2. O sigilo das comunicações na era digital. 3. A relevância da regulamentação da prova digital no ordenamento jurídico brasileiro. Conclusão. Referências.

INTRODUÇÃO

O presente trabalho aborda análise crítica acerca da legalidade da suspensão dos serviços de comunicação, tendo em vista que a fundamentação legal usada para amparar as decisões judiciais são aplicadas de forma equivocada além de serem conflitantes com direitos fundamentais previstos na CRFB/88. Ante a era digital que permeia no ordenamento jurídico, o estudo aqui apresentando também é realizado com intuito de demonstrar a relevância da regulamentação da prova digital.

Inicia-se o primeiro capítulo do trabalho sendo pontuado os artigos do Marco Civil da Internet usados como fundamento jurídico para amparar as decisões judiciais que visam a suspensão dos serviços de comunicação. Será pontuada a controvérsia inicial que consiste na finalidade da Lei nº 12.965/2014 em proteger os usuários de internet, mas que é usada

para amparar decisões judiciais com interesse exclusivamente público de modo a distorcer a finalidade da Lei fragilizando a proteção do usuário.

Ainda nesse contexto, demonstrará de acordo com pareceres técnicos, que a quebra da criptografia de um usuário acarreta riscos ao sigilo da comunicação de todos os outros, portando, ao solicitar essa violabilidade ainda que em caráter excepcional, é inconstitucional por violar direitos resguardados pela CRFB/88.

Após apresentar análise sobre a legalidade dos dispositivos do MCI, no segundo capítulo será debatido sobre o sigilo das comunicações na era digital, destacando que a tecnologia tomou espaços inimagináveis na sociedade trazendo aspectos positivos e negativos, ao passo que contribui para a praticidade do cotidiano, mas também faz com que os usuários estejam vulneráveis a riscos invisíveis. Usa o ponto de vista jusnaturalista para explicar a razão de ser mais importante garantir a inviolabilidade das comunicações e do sigilo, do que criar meios para fragilizá-los.

No terceiro e último capítulo, serão analisados os motivos pelos quais é importante a regulamentação da prova digital no ordenamento jurídico, especificamente no Código de Processo Penal. Com foco no contexto histórico, de modo a apontar o cenário atual inovador no quesito técnico da prova, o que expõe as razões de um código defasado pelo tempo e os aspectos a serem melhorados com as devidas atualizações.

A pesquisa se estrutura na metodologia hipotético-dedutiva, uma vez que o pesquisador se posiciona elegendo um conjunto de questionamentos, os quais acredita serem viáveis e adequadas para analisar o objeto da pesquisa, com intenção de comprová-las ou rejeitá-las de forma argumentativa.

Portando, a abordagem desta pesquisa jurídica é necessariamente qualitativa, a qual o pesquisador tem por base a análise de legislação, doutrina e artigos científicos em torno do tema.

1. A FUNDAMENTAÇÃO JURÍDICA PARA SUSPENSÃO DOS SERVIÇOS DE TELECOMUNICAÇÃO E O CONFLITO DE CONSTITUCIONALIDADE NA PROTEÇÃO DOS DIREITOS À PRIVACIDADE E COMUNICAÇÃO

A Lei do Marco Civil da Internet, promulgada no ano de 2014, dispõe no art. 10, § 2, sobre a requisição judicial de conteúdos de comunicação privada mediante ordem judicial, desde que em acordo com as hipóteses previstas no art. 7, II e III, da referida lei, além de

prever no art. 12, sanção para infrações do art. 10 e 11¹. Esse fundamento legal ampara as decisões e ordens judiciais que visam suspender os serviços de telecomunicação. No entanto, esses dispositivos estão em conflito com os direitos constitucionais da privacidade e comunicação, razão pela qual são alvos de controvérsias.

O primeiro aspecto relevante para debate é a combinação do art. 10, §2 com o art. 7º, II e III, isso porque aquele prevê a requisição de conteúdo de comunicação privada mediante ordem judicial enquanto este, previsto no capítulo de direitos e garantias dos usuários, dispõe respectivamente sobre a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, e das comunicações privadas armazenadas, salvo por ordem judicial.

A controvérsia consiste no uso desses dispositivos quando é usado para atender interesse público tendo em vista que o legislador teve como objetivo proteger o usuário. Na remota hipótese de violação do sigilo das informações, deveria ser para garantir os direitos individuais e não o oposto, ou seja, é incabível usar esses dispositivos legais para violar as garantias dos usuários atribuídas pela legislação. No entanto, o Poder Judiciário pratica equívocos nesse contexto.

Nesse prisma a doutrina faz crítica a forma de aplicação dos dispositivos, e pontua que²:

Por ora, a atenção deve ser voltada para a forma pela qual uma lei editada para garantir direitos na internet, dentre eles a liberdade de expressão, foi interpretada de modo a restringir uma aplicação utilizada por milhões de brasileiros, inclusive pelo próprio Poder Judiciário para a prática de certas atividades jurisdicionais.

É sabido que, em razão do tema ser embrionário no ordenamento jurídico brasileiro, por vezes os magistrados fizeram uso do poder de cautela³ com o intuito de suprir as lacunas legais para os casos concretos colocados à sua frente⁴. No entanto, com advento do Marco Civil da Internet o aspecto legal deveria ser fortificado, o que não ocorreu e as normas são aplicadas com interpretação equivocada.

Outro ponto controvertido é a o art. 7, II, com previsão de inviolabilidade e sigilo do fluxo das comunicações na internet salvo por ordem judicial. Ao se referir ao “fluxo” remete a ideia de interceptação em tempo real, mas tecnicamente essa possibilidade já foi refutada

¹ BRASIL. *Lei nº 12.965 de 2014*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 03 jul. 2020.

² SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina. *Marco Civil da Internet: comentários a jurisprudência*. São Paulo: Revista do Tribunais, 2017, p. 69.

³ O poder geral de cautela, regado pelo art. 798 do CPC, é a impossibilidade de que o legislador preveja todos os casos concretos que o magistrado possa vir a encontrar, criando condições para que o mesmo, possa conferir efetividade à prestação jurisdicional.

⁴ SOUZA; LEMOS; BOTTINO, op. cit., p. 64.

por estudos realizado pelo MIT materializados na obra “*Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*”⁵. A pesquisa esclarece que a única possibilidade de quebra de sigilo de usuários específicos coloca em risco o sigilo de todos os outros.

Assim violaria o direito à privacidade, do qual está previsto na CRFB/88 como um dos direitos fundamentais com o objetivo de garantir o mínimo de dignidade privada ao indivíduo. Se esse dispositivo não pode ser garantido a todos torna-se inconstitucional.

A preservação do direito à privacidade⁶ na era digital é defendido majoritariamente no ordenamento jurídico brasileiro e internacional. No âmbito dos direitos humanos a ideia de que toda e qualquer pessoa é sujeito de direitos e detentora do direito à privacidade é uma importante premissa. De acordo com o art. 12 da Declaração Universal de Direitos Humanos, “Ninguém sofrerá intromissões arbitrárias na sua vida privada [...]”⁷.

Com a evolução informática a ONU colocou em pauta em Assembleia Geral o impacto negativo que a vigilância e a interceptação de comunicações podem ter sobre os direitos humanos. E por meio da Resolução nº 68/167 com o tema “*The right to privacy in the digital age*”, determinou aos estados membros que respeitem e protejam o direito à privacidade, inclusive no contexto de comunicação digital⁸.

No Brasil existe esforço para que o direito à privacidade na era digital seja preservado, motivo pelo qual existem duas ações em tramite no Supremo Tribunal Federal, com julgamento pendente, em que se discute a constitucionalidade dos bloqueios e suspensão do serviço *Whatsapp* em razão de descumprimento de ordem judicial.

A suspensão dos serviços de comunicação é confrontada com o direito à privacidade e comunicação. Apesar de as decisões e ordens do juízo a quo serem unânimes no sentido de considerar legal a suspensão do *Whatsapp*, o Supremo Tribunal Federal tem se manifestado por meio do voto ministerial em sentido oposto, considerando a inconstitucionalidade da suspensão e a violação a preceitos fundamentais, observando a intenção do legislador de proteger o usuário.

⁵ MIT Libraries. Disponível em: <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8&isAllowed=y>. Acesso em: 03 jul. 2020.

⁶ BRASIL. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 03 jul. 2020.

⁷ ASSEMBLEIA GERAL DA ONU. (1948). *Declaração Universal dos Direitos Humanos*. Paris. Disponível em: <https://www.un.org/en/universal-declaration-human-rights/>. Acesso em: 03 de jul. 2020.

⁸ ASSEMBLEIA GERAL DA ONU. (2013). *The right to privacy in the digital age*. Disponível em: <https://undocs.org/A/RES/68/167>. Acesso em: 03 de jul. 2020.

O Ministro Edson Fachin, corrobora com a tese de que o artigo 7, II, e art. 12, III, devem ser declarados parcialmente inconstitucional, afirma ser necessário o afastamento da interpretação do dispositivo que autoriza a ordem judicial a requisitar conteúdo de comunicação criptografada, em razão do risco a violação do direito à privacidade caso a criptografia seja quebrada.

O entendimento do Ministro contextualiza de forma sucinta o cenário jurídico na era digital e diverge levemente do entendimento da Ministra Rosa Weber⁹ :

[...]O aplicativo *WhatsApp* não permite que o conteúdo das comunicações trocadas entre os usuários seja disponibilizado, porque isso exigiria que o aplicativo alterasse seu sistema de criptografia, introduzindo uma vulnerabilidade em seu sistema. Com as vênias da e. Min. Rosa Weber, ordens judiciais, ainda que para fins de investigação criminal ou instrução processual penal – como ocorre nas ações que são impugnadas na presente arguição –, não podem determinar que o aplicativo de internet modifique seu sistema de criptografia. Daí porque a necessidade de inconstitucionalidade sem redução de texto do art. 7º, II, e 12, III, ambos do Marco Civil da Internet [...]

Em análise crítica ao art. 12, III e IV da Lei nº 12.965/2014, é de se esclarecer, a permissão de suspensão ou proibição, das atividades que envolvem a “operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações”¹⁰ é para preservar a integridade desses dados em face de provedores, para exclusiva proteção dos usuários. São dados que por sua natureza são armazenados, diferente de interceptação em tempo real, a qual é instantaneamente assistida, mas não pode ser captada nem guardada em razão da criptografia.

Verifica-se que a discussão recai sobre texto legal, do qual não constitui permissão em hipótese alguma para imposição de sanções em decorrência do descumprimento de ordem judicial. É oportuno ressaltar o entendimento doutrinário sobre o tema: “é importante guardar a observância do princípio da reserva legal, evitando que uma interpretação ampliativa possa levar situações de extrema insegurança jurídica – justamente o que a edição do Marco Civil da Internet procurou evitar”¹¹ .

O Marco Civil da Internet disciplina o uso da internet no Brasil, se propõe a harmonizar princípios como a garantia da liberdade de expressão e de comunicação, a

⁹ BRASIL. Supremo Tribunal Federal. *Ação direta de inconstitucionalidade nº 5.527*. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>. Acesso em: 03 de jul. 2020.

¹⁰ Os registros de conexão são gerados toda vez que uma pessoa se conecta à Internet. O objetivo desses registros é identificar de onde o computador acessou a rede, a que horas, e por quanto tempo. Deve-se esclarecer, contudo, que os registros de conexão demonstram a conexão de uma máquina (terminal) a um provedor que possibilitou sua conexão, e não de seres humanos.

¹¹ SOUZA; LEMOS; BOTTINO, op. cit., p. 64.

proteção da privacidade e dos dados pessoais e a responsabilização dos agentes de acordo com suas atividades. Nota-se a intenção de harmonização dos direitos inerentes principalmente ao sujeito de direito de modo a protegê-lo.

Nesse ponto é pertinente trazer a confirmação por Gilmar Mendes de que a Lei nº 12.965/2014, visa proteger os usuários¹²:

[...]o chamado “marco civil da internet” . Entre as garantias estabelecidas na referida lei, uma importante inovação: restou expressamente assegurado aos usuários da internet no Brasil não apenas o sigilo do fluxo de comunicações, já regulamentado pela Lei n. 9.296/96, como também a inviolabilidade e o sigilo dos dados armazenados (art. 7º, II e III), tema até então sem legislação específica, a motivar controvérsias na doutrina e na jurisprudência.

Eis o questionamento, se o MCI visa a proteção dos usuários de internet como poderia ser usada em face destes violando o seu direito à privacidade e à comunicação. De acordo com o entendimento supracitado, Gilmar Mendes frisa que além de existir expressa proteção ao sigilo do fluxo das comunicações, protege-se também os dados armazenados. Sob essa ótica as controvérsias são supridas pelo artigo 7º, II e III.

Portanto, o que se constata em torno das decisões de suspensão dos serviços de telecomunicação com fundamento no Marco Civil da Internet é que são medidas violadoras da CRFB/88 em que são aplicados equivocadamente os artigos 7º, II e 12, III e IV. Isso porque a legislação visa a proteção dos usuários no sentido de garantir todos os direitos fundamentais em torno do fluxo das comunicações e armazenamento de dados. No entanto os dispositivos legais foram aplicados em sentido contrário para acessar as informações privadas que deveriam ser legalmente protegidas.

2. O SIGILO DAS COMUNICAÇÕES NA ERA DIGITAL

Existem diversas justificativas para aplicação incorreta da Lei nº 12.965/2014, uma delas é a de que o sistema jurídico ainda está se moldando à novidade da era digital. A título de exemplo menciona-se a interceptação telefônica positivada por meio da Lei nº 9.296/1996, há mais de vinte anos. Aponta-se lacunas legais em razão do tempo decorrido desde a criação da lei, enquanto a tecnologia evolui, é certo de que passa a existir a necessidade de adequação legal ao novo contexto social.

¹² MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. São Paulo: atlas, 2017, p. 102.

Ao longo das últimas décadas o avanço tecnológico se deu de forma muito rápida a ponto de colocar os operados do direito diante de situações ainda sem previsão legal. O desafio de atualizar o sistema jurídico atinge diversas nações tornando o assunto tema de debate para estabelecer em meio a tecnologia e o direito a ponderação adequada para as normas.

Nesse debate, primeiramente constata-se que a tecnologia tomou espaços inimagináveis na sociedade trazendo aspectos positivos e negativos, ao passo que contribui para a praticidade do cotidiano, mas também faz com que os usuários estejam vulneráveis a riscos invisíveis. Menciona-se o sistema “*Backdoors*”, que será explicado adiante, como um exemplo cristalino de risco invisível, uma vez que existe uma espionagem digital.

Fato é que a privacidade e a comunicação são direitos inerentes a pessoa humana, portanto em primeiro lugar é importante garantir e valorizar a preservação da privacidade e do sigilo sobre a vida privada, sendo a quebra de sigilo algo secundário e não o ponto mais relevante para solucionar.

No entanto, a controvérsia atual se estrutura na inversão dessa premissa. O que não pode ser aceito, isso porque a privacidade é direito fundamental amparado fortemente pela CRFB/88. Esse debate é também dividido em âmbito filosófico-jurídico, dispendo de vertentes variadas entre os jusnaturalistas, os positivistas e os idealistas.

Paulo Gustavo Gonet Branco, esclarece¹³:

[...] para os jusnaturalistas, os direitos do homem são imperativos do direito natural, anteriores e superiores à vontade do Estado. Já para os positivistas, os direitos do homem são faculdades outorgadas pela lei e reguladas por ela. Para os idealistas, os direitos humanos são ideias, princípios abstratos que a realidade vai acolhendo ao longo do tempo, ao passo que, para os realistas, seriam o resultado direto de lutas sociais e políticas.

Sob a vertente do jusnaturalismo, compreendendo o direito fundamental como aquele que nasce com o homem, sendo intrínseco a ele e anterior as normas impostas por tudo aquilo que não é natural, pode-se afirmar que a privacidade detém de fato prioridade. Não significa dizer ser um direito absoluto, como se comprova com a possibilidade excepcional de interceptar conteúdo de comunicações em aparelhos que não dispõem da criptografia. Nota-se a excepcionalidade de um direito constitucionalmente garantido, mas é importante frisar que se aplica a casos específicos.

¹³ Ibidem., p.139.

Como é o caso do *Whatsapp* em que é protegido por criptografia, deve prevalecer o direito à privacidade, tendo em vista que a interceptação nesse *app* coloca em risco o sigilo de todos os outros usuários. Como mencionado no primeiro capítulo, o MCI visa a proteção dos usuários da internet, no que tange a interceptação telefônica a premissa é semelhante.

Para Paulo Gustavo Gonet Branco¹⁴:

O sigilo das comunicações é não só um corolário da garantia da livre expressão de pensamento; exprime também aspecto tradicional do direito à privacidade e à intimidade. A quebra da confidencialidade da comunicação significa frustrar o direito do emissor de escolher o destinatário do conteúdo da sua comunicação.[...] A reclusão periódica à vida privada é uma necessidade de todo homem, para a sua própria saúde mental. Além disso, sem privacidade, não há condições propícias para o desenvolvimento livre da personalidade. Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracassos à crítica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muito menos como o indivíduo se autoavaliar, medir perspectivas e traçar metas.

Mais do que preceito jurídico, sob a ótica de Gonet Branco, a privacidade é caracterizada pelos sentimentos, desenvoltura, autoconhecimento, superação, reforçando ainda mais o aspecto jusnaturalista sobre a privacidade. O autor¹⁵ frisa ainda que “Uma das limitações à liberdade de comunicação social é o respeito devido ao direito à Privacidade [...]” previsto no art. 5º, X da CRFB/88¹⁶, sendo esse direito citado expressamente também no art. 220 como limite à liberdade dos meios de comunicação.

A privacidade em primeiro plano é amparada também pela Organização das Nações Unidas e foi tema de Assembleia Geral com finalidade de discutir sobre “*The right to privacy in the digital age*”¹⁷ em que se estabelece diretrizes sobre os direitos da privacidade na era digital.

No que tange aos riscos invisíveis da era digital, esse é outro argumento robusto, pois é importante refletir sobre a privacidade protegida por criptografia para além da comunicação, levando-a para outras áreas do cotidiano como por exemplo, aplicativos bancários e banco de dados do setor público.

¹⁴ Ibidem., p. 307.

¹⁵ Ibidem., p. 294.

¹⁶ O inciso X do artigo 5º da CRFB/88, dispõe que: X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

¹⁷ ASSEMBLEIA GERAL DA ONU, op. cit., nota 08.

Assim, a criptografia existe como um avanço social, pois genericamente de acordo com a era digital requer-se mais proteção à privacidade do que a fragilização dos meios que a tornam seguro. Em sentido técnico, o estudo realizado pelo Center for Strategic and International Studies, no artigo “*The effect of Encryption on Lawful Access to Communications and Data*”¹⁸ ressalta o inquestionável avanço técnico que é a criptografia e a importância dela para a sociedade como um todo inclusive para o direito.

No entanto, coloca também como matéria desafiadora para a área jurídica, contrapondo que com o avanço tecnológico edificou-se a necessidade de proteção aos indivíduos e a criptografia foi excelente nesse aspecto, mas grupos com intenções criminosas como extremistas islâmicos e Al Qaeda’s também se beneficiam. A nível nacional também pode-se mencionar as organizações criminosas como Comando Vermelho (CV) e Primeiro Comando da Capital (PCC).

Certamente existe conflito entre a plena proteção da comunicação e a possibilidade de eventual quebra de sigilo, mas todos os estudos apontam para a preservação da privacidade. O estudo realizado pelo centro supracitado tem como um dos títulos “*The encryption debate and backdoors*”, “O debate sobre criptografia e *backdoors*”¹⁹, e pontua o seguinte²⁰:

[...] o termo backdoor implica em acesso clandestino e falta de responsabilização por ele. O que as agências policiais querem é o uso de criptografia recuperável que possa permitir acesso legal com a supervisão apropriada. o problema é que exigir recuperação é caro e complexo para implementar.[...] Nossa conclusão básica é que os benefícios de exigir o acesso a dados criptografados não superariam os custos. O acesso da polícia aos dados criptografados é um problema, mas a magnitude do desafio ainda não é significativa o suficiente para justificar os mandatos de descryptografia.

Assim, compreende-se *Backdoors* como um termo para se referir a “porta dos fundos”. É uma porta clandestina aberta no sistema, não documentada, que permite ao criador ter acesso a ele. Para o estudo supracitado o fato de ser um sistema de alto custo e

¹⁸ CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. *The effect of Encryption on Lawful Access to Communications and Data*. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE. Acesso em: 05 jul. 2020.

¹⁹ [...] the term backdoor implies surreptitious access and a lack of accountability. what law enforcement agencies want is the use of recoverable encryption that can permit lawful access with appropriate oversight. the problem is that mandating recoverability is costly and complex to implement. [...] our basic conclusion is that the benefits of mandating access to encrypted data would not outweigh the costs. Law enforcement access to encrypted data is an issue, but the magnitude of the challenge is not yet significant enough to justify decryption mandates.

²⁰ CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, op. cit., nota 18.

difícil de ser implantado pesa mais do que os problemas a serem solucionados com a inovação, frisa-se ainda a inexistência de algo relevante o bastante a ponto de gerar a quebra da criptografia.

Nesse sentido, a única conclusão possível sobre a quebra do sigilo das comunicações na era digital é de que a privacidade deve ser protegida enquanto não houver mecanismo de interceptação exclusiva de usuários previamente determinados sem que viole a privacidade dos outros. É certo também que, em virtude dos meios tecnológicos serem predominantes no cenário atual, requer-se maior zelo pela privacidade e proteção da comunicação, o que é mais vantajoso de acordo com o contexto debatido.

3. A RELEVÂNCIA DA REGULAMENTAÇÃO DA PROVA DIGITAL NO ORDENAMENTO JURÍDICO BRASILEIRO

A prova digital ainda não é um instituto positivado no ordenamento jurídico, em virtude do rápido avanço tecnológico, algumas esferas do direito passaram a carecer de normas regulamentadoras. Esse é o caso do Código de Processo Penal no que tange a requisição de provas e a falta de previsão legal da prova digital.

Prova em contexto genérico revela a busca pela construção da verdade, tendo os seus diversos meios de constituição ao longo da história de acordo com cada momento. Nesse sentido Pacelli lembra dos juízes de Deuses²¹ “o acusado submetia-se a determinada provação física, ou suplício, de cuja, superação, quando vitorioso, se lhe reconhecia a veracidade de sua pretensão [...]”. Esse exemplo contextualiza perfeitamente a influência do tempo na materialização do que pode ser considerado prova.

Tourinho Filho cita os seguintes exemplos do sistema *ordálico*²²:

Havia a prova da água fria: jogado o indiciado à água, se submergisse, era inocente, se viesse à tona seria culpado [...] A do ferro em brasa: o pretenso culpado, com os pés descalços, teria que passar por uma chapa de ferro em brasa. Se nada lhe acontecesse, seria inocente; se se queimasse, sua culpa seria manifesta [...]

A produção de prova é muito representativa de acordo com cada contexto histórico, sendo inquestionável a existência de uma nova espécie de prova ainda não regulamentada, isso porque a era atual é inovadora no quesito técnico da prova. Gustavo Henrique de

²¹ PACHELLI, Eugenio. *Curso de Processo Penal*. 21. ed. rev., atual. e ampl. São Paulo: Atlas, 2017. p. 174.

²² TOURINHO apud PACHELLI, Eugenio. *Curso de Processo Penal*. São Paulo: Atlas, 2017. p.174.

Vasconcellos Cavalcanti²³, conceitua a prova digital como “refere-se àquelas provas dispostas em uma sequência de bits e consignada em uma base física eletrônica. Uma prova digital, portanto, é um elemento digital/eletrônico capaz de dar ciência de um fato a alguém.”.

Compara-se a prova documental, a qual remete a dados e informações materializados em documentos físicos. A época em que se estabeleceu essa espécie de prova era impensado a possibilidade de documento probatório virtual, como é o caso de banco de dados, onde é armazenada uma gama de informações.

Renato Brasileiro, em sentido semelhante conceitua a prova documental sob a ótica restrita e ampla²⁴:

O conceito de documento pode ser abordado de forma estrita ou de modo amplo. Numa concepção mais restrita, considera-se documento (de *doceo*, ensinar, mostrar, indicar) qualquer escrito, instrumento ou papel, público ou particular (CPP, art. 232, *caput*). Pode-se defini-lo, assim, como toda a peça escrita que condensa graficamente o pensamento de alguém, podendo provar um fato ou a realização de algum ato dotado de relevância jurídica. Numa concepção mais ampla, e com base em uma interpretação progressiva, tem-se como documento qualquer objeto representativo de um fato ou ato relevante, conceito no qual podemos incluir fotografias, filmes, desenhos, esquemas, e-mails, figuras digitalizadas, planilhas, croquis, etc. Em ambas as concepções, apresenta-se como característica essencial do documento a relevância jurídica, a ser compreendida como a possibilidade da expressão do pensamento nele contido gerar consequências no plano jurídico.

A diferença entre o sentido restrito e o amplo é reveladora da evolução dos meios de prova, referindo-se o autor a “interpretação progressiva” para justificá-la, destaque-se o e-mail como um objeto de prova representativo do cenário atual. Certamente o não reconhecimento da espécie “prova digital” no Código de Processo Penal não implica em dispensa de provas quando forem de teor digital.

No entanto, é de suma importância a inclusão dessa nova espécie no título VII do CPP²⁵ sobre “provas”, acrescentando as diretrizes da prova digital, assim como já existe a prova documental, testemunhal, dentre outras. Isso porque, a regulamentação específica atualiza o sistema além de evitar equívocos na era digital, como tem acontecido com a aplicação inapropriada do MCI.

²³ CAVALCANTI, Gustavo Henrique de Vasconcellos. *Validade jurídica das provas digitais no processo administrativo disciplinar*. Disponível em: https://corregedorias.gov.br/assuntos/responsabilizacao-agentes-publicos/documentos/artigo_evidencias_digitais_no_pad.pdf. Acesso em: 05 jul. 2020.

²⁴ BRASILEIRO, Renato de Lima. *Manual de Processo Penal*. 8. ed. ver., ampl e atual.- Salvador: Juspodium, 2020, p. 788.

²⁵ BRASIL. *Código de Processo Penal de 1941*. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 06 jul. 2020.

Em razão dessa carência de previsão legal, não muito distante, houve debate ferrenho sobre a apreensão de provas consideradas “digitais”. Tendo em vista que diferentemente da prova documental em sentido estrito, a coleta de prova digital não exige que o colhedor permaneça com a posse do dispositivo detentor de informações. Por exemplo, ao realizar a busca e a apreensão de um computador em virtude das provas ali constantes, não é necessário a custódia desse objeto, uma vez que é possível fazer cópia dos dados necessários e posteriormente devolvê-lo ao proprietário sem restringir em grau máximo o direito de propriedade²⁶.

Nesse sentido, Renato Brasileiro conceitua apreensão da seguinte maneira²⁷:

A apreensão deve ser tida como medida de constrição, colocando sob custódia determinado objeto ou pessoa [...]. Conquanto a busca e apreensão esteja inserida no Código de Processo Penal como meio de prova (Capítulo XI do Título VII), sua verdadeira natureza jurídica é de meio de obtenção de prova (ou de investigação da prova). Isso porque consiste em um procedimento (em regra, extraprocessual) regulado por lei, com o objetivo de conseguir provas materiais, e que pode ser realizado por outros funcionários que não o juiz (v.g., policiais). Sua finalidade precípua não é a obtenção de elementos de prova, mas sim de fontes materiais de prova [...].

Esse é um exemplo cristalino de caso em que a regulamentação da prova digital é de extrema importância. Em razão do Código de Processo Penal ser da década de 40, carrega termos que não existem mais e carece de instrumentos atuais, como fotocópias e cartas, atualmente substituídas por outros meios da era digital²⁸.

Eis a relevância de sintonizar a realidade com o contexto jurídico atual, principalmente para evitar que ao atender a legislação em um ponto específico não seja violado outro, como é o caso da busca e apreensão de aparelhos eletrônicos para obtenção de provas. Nesse exemplo o direito de propriedade é colocado em segundo plano sem necessidade, uma vez que a coleta de dados pode ser realizada e transferida para um *pen drive* e o aparelho rapidamente devolvido.

Diante da necessidade de atualização, atualmente tramita na Câmara Legislativa Projeto de Lei nº 8045/2010 sobre o novo Código de Processo Penal, com inserção de institutos próprios da era digital, como o Título “Da Interceptação das Comunicações

²⁶ OHN, Paul; BRENNER, Susan. *The Yale Law Journal*: Fourth Amendment Seizures of Computer Data. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1378402. Acesso em 05 jul. 2020.

²⁷ BRASILEIRO, op. cit., p. 791.

²⁸ LOPES JUNIOR, Aury. *Direito processual penal*. 17. ed. São Paulo : Saraiva Educação, 2020, p. 794.

Telefônicas”, com previsão legal no Projeto de Lei, Capítulo III sobre “ OS MEIOS DE PROVA”²⁹.

Discute-se também a implementação do Título “Prova Digital”, mas ainda está pendente no Projeto de Lei. Fato é que, essa temática contribuiria de forma robusta tanto para o ordenamento jurídico, no contexto amplo, como também em sentido estrito referente à suspensão dos serviços de comunicação tendo em vista ser tema oriundo da era digital.

Portanto, verifica-se que o Código de Processo Penal de 1941, carece de normas para orientar juridicamente os casos concretos atuais, uma vez que o contexto histórico revela o novo prisma no quesito técnico da prova. Sendo um destes a regulamentação da prova digital a qual na era atual constitui pauta indispensável e urgente para as investigações e produção de provas, principalmente no que tange a custódia de aparelhos eletrônicos ao atingir o direito de propriedade.

CONCLUSÃO

Na presente pesquisa foi possível constatar que a suspensão dos serviços de comunicação por ordem judicial está acompanhada por fundamentos jurídicos usados de forma inapropriada e que também violam direitos amparados pela CRFB/88. Verificou-se que o sigilo das comunicações na era digital envolve questões técnicas que tornam a privacidade prioridade não só em âmbito jurídico, mas também no tecnológico. Além disso foi exposta a carência de normas direcionada a era digital no quesito de requisição de provas no Código de Processo Penal.

No primeiro capítulo contata-se que o debate sobre a suspensão dos serviços de comunicação recai sobre o texto legal, do qual não constitui permissão em hipótese alguma para imposição de sanções em decorrência do descumprimento de ordem judicial. Isso porque a Lei do Marco Civil da Internet tem como propósito a proteção dos usuários de internet, desse modo não pode ser usada em face destes violando o seu direito à privacidade e à comunicação. Apesar das diversas decisões aplicando inapropriadamente os dispositivos da referida lei o Supremo Tribunal Federal aponta no sentido de reforçar a aplicação correta dos dispositivos legais.

²⁹ BRASIL. Câmara dos Deputados. *Projeto de Lei nº 8045/2010*. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1638152&filename=Tramitacao-PL+8045/2010. Acesso em: 06 jul. 2020.

Outra constatação em torno das decisões de suspensão dos serviços de telecomunicação com fundamento na Lei nº 12.065/2014 é que por serem medidas violadoras da CRFB/88 em que são aplicados equivocadamente os artigos 7º, II e 12, III e IV, são dispositivos inconstitucionais.

No segundo capítulo, debatido sobre a quebra do sigilo das comunicações na era digital concluiu-se que a privacidade deve ser protegida enquanto não houver mecanismo de interceptação exclusiva de usuários previamente determinados sem que viole a privacidade dos outros. Observou-se que o custo e a complexidade da aplicação do sistema para viabilizar a quebra do sigilo é alto e que os problemas dos quais exigem essa violação não são significantes o suficiente para compensar o custo.

Além de demonstrar que, em virtude dos meios tecnológicos serem predominantes no cenário atual, requer-se maior zelo pela privacidade e proteção da comunicação, o que é mais vantajoso de acordo com o contexto debatido, já que existem riscos invisíveis tornando os usuários vulneráveis. Como exemplo cristalino, apontou-se o sistema *backdoors*, usado por um terceiro clandestinamente para acompanhar o que um usuário específico está acessando.

Frisou-se que a criptografia existe como um avanço tecnológico e jurídico, pois genericamente de acordo com a era digital requer-se mais proteção à privacidade do que a fragilização dos meios que a tornam segura. Essa tem sido a principal premissa no ajuste da aplicação apropriada do MCI, como é o entendimento do Ministro do Supremo Tribunal Federal Edson Fachin em voto proferido na defesa dos direitos fundamentais, ainda que a violação seja para fins de investigação criminal.

Por fim, no último capítulo tratou-se de apresentar a relevância da regulamentação da prova digital no ordenamento jurídico e constatou-se que essa positivação contribuiria de forma robusta para o ordenamento jurídico, tanto no contexto amplo, como também sem sentido estrito referente à suspensão dos serviços de comunicação tendo em vista ser tema oriundo da era digital.

A lacuna legal nesse prisma se explicou por contexto histórico, tendo em vista que o tempo é muito representativo na materialização do que é considerado “prova”, como é o caso do sistema *ordálico* citado por Tourinho filho. Além disso verificou-se que o Código de Processo Penal de 1941, carece de normas para orientar juridicamente os casos concretos atuais. Sendo um destes a regulamentação da prova digital, a qual na era atual, constitui pauta indispensável e urgente.

REFERÊNCIAS

ASSEMBLEIA GERAL DA ONU. *Declaração Universal dos Direitos Humanos*. Disponível em: <http://www.un.org/en/universal-declaration-human-rights/>. Acesso em: 03 jul. 2020.

_____. (2013). *The right to privacy in the digital age*. Disponível em: <https://undocs.org/A/RES/68/167>. Acesso em: 03 jul. 2020.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 8045/2010*. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?Codteor=1638152&filename=Tramitacao-PL+8045/2010. Acesso em: 06 jul. 2020.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 jul. 2020.

_____. *Código de Processo Penal de 1941*. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 06 jul. 2020.

_____. *Lei nº 12.965 de 2014*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 03 jul. 2020.

_____. Supremo Tribunal Federal. *ADI nº 5.527 e ADPF nº 403*. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>. Acesso em: 03 jul. 2020.

BRASILEIRO, Renato de Lima. *Manual de Processo Penal*. 8. ed. ver., ampl e atual.- Salvador: Juspodium, 2020.

CAVALCANTI, Gustavo Henrique de Vasconcellos. *Validade jurídica das provas digitais no processo administrativo disciplinar*. Disponível em: https://corregedorias.gov.br/assuntos/responsabilizacao-agentes-publicos/documentos/artigo_evidencias_digitais_no_pad.pdf. Acesso em: 05 jul. 2020.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. *The effect of Encryption on Lawful Access to Communications and Data*. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE. Acesso em: 05 jul. 2020.

LOPES JUNIOR, Aury. *Direito processual penal*. 17. ed. São Paulo : Saraiva Educação, 2020.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet,. *Curso de direito constitucional*. São Paulo: atlas, 2017.

MIT Libries. Disponível em: <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8&isAllowed=y>. Acesso em: 03 jul. 2020.

OHN, Paul; BRENNER, Susan. *The Yale Law Journal: Fourth Amendment Seizures of Computer Data*. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1378402. Acesso em: 05 jul. 2020.

PACELLI, Eugenio. *Curso de Processo Penal*. 21ª. ed. rev., atual. e ampl. – São Paulo: Atlas, 2017.

SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina. *Marco Civil da Internet: comentários a jurisprudência*. São Paulo: Revista do Tribunais, 2017.