USO EXCLUSIVO

Revista dos **TRIBUNAIS**

Ano 110 • vol. 1031 • setembro 2021

Medidas cautelares e meios de prova nos crimes cibernéticos

Precautionary measures and means of proof in cybercrimes

Acesse o QR Code e leia este artigo em Visual Law

Greice Patricia Fuller

Pós-Doutora em Direito na Universidad de Navarra /Espanha com bolsa da CAPES (2018). Doutora e Mestre em Direito das Relações Sociais, pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Especialista em Direito Espanhol para Juristas estrangeiros pela Universidad de Alcalá – Madrid (2017). Professora dos Cursos de Graduação das Faculdades de Direito e Pós-Graduação *Lato Sensu* de Direito Digital e Proteção de Dados e Direitos Difusos e Coletivos da Pontifícia Universidade Católica de São Paulo (PUC/SP). Professora do Programa de Mestrado em Direito da Sociedade da Informação e da Graduação do Centro Universitário das Faculdades Metropolitanas Unidas (FMU). Líder do Grupo de Pesquisa Efetivação jurídica estatal certificado pelo CNPq (Linha de pesquisa: Decisão Jurídica e monopólio do Estado): Programa de Mestrado em Direito da Sociedade da Informação FMU. (dgp.cnpq.br/dgp/espelhogrupo/2190779147769731)
greicepf@uol.com.br

João Marcelo Braga Fernandes Pedrosa

Mestrando em Direito na Sociedade da Informação pelas Faculdades Metropolitanas Unidas (FMU) (2020-2021). Pós-graduado (*lato sensu*, com título de especialista e opção em Magistério Superior) em Ciências Penais, Direito e Processo Penal pela Uniderp-LFG (2010). Graduado em Direito pela Universidade Candido Mendes no Estado do Rio de Janeiro (2008). Professor Universitário e de Cursos Jurídicos e Preparatórios para Exame de Ordem (OAB), nas disciplinas Direito Penal, Processual Penal, Criminologia e Medicina Legal. Delegado de Polícia do Estado de São Paulo.
joaomarcelo1@gmail.com

Áreas do Direito: Penal; Processual; Digital

Resumo: O presente artigo trata dos crimes cibernéticos ou eletrônicos, tendo como objetivo especificamente o tratamento de questões atinentes às medidas cautelares e aos meios de prova no que se relaciona a estes delitos. Preliminarmente, optou-se por realizar uma breve digressão histórica e teórica acerca da sociedade da informação e seus conceitos visando compreender a trajetória da informação, enquanto instrumento tanto na disseminação do conhecimento humano – eis que seria

Abstract: This article analyses cybercrimes, more specifically the issues related to precautionary measures and means of evidence in relation to these crimes. Preliminarily, it was decided to make a brief historical and theoretical digression about the information society and its concepts in order to understand the trajectory of information, as an instrument both in the dissemination of human knowledge, that would be imaginable, to obtain such a reach and capillarity of technological

Fuller, Greice Patricia; Pedrosa, João Marcelo Braga Fernandes. Medidas cautelares e meios de prova nos crimes cibernéticos. *Revista dos Tribunais*. vol. 1031. ano 110. p. 207-224. São Paulo: Ed. RT, setembro 2021.

USO EXCLUSIVO CJF

imaginável, obter tamanho alcance e capilaridade do avanço tecnológico e científico não fosse pela internet – quanto nos desafios à sociabilidade humana e à normatividade jurídica, uma vez que a dependência social aos meios tecnológicos e a proliferação da criminalidade cometida por meio informático são fenômenos incontornáveis da Sociedade de Informação. Após, aponta-se a evolução dos delitos para os meios digitais, inclusive salientando os seus conceitos e classificações. Conclui-se com a percepção de que o desenvolvimento tecnológico, a proliferação dos aparelhos e dispositivos eletrônicos e a massificação da Internet tornam imperativa uma permanente reflexão dogmática e multidisciplinar e estudo, sendo ainda indispensável a internalização do Tratado de Budapeste.

PALAVRAS-CHAVE: Crimes cibernéticos – Medidas cautelares – Meios de prova – Convenção de Budapeste.

advancement and scientific were it not for the internet, as for the challenges of human sociability and legal norms, since social dependence on technological means and the proliferation of criminality committed by means of information technology are unavoidable phenomena of the Information Society. Afterwards, the evolution of crimes towards digital media is pointed out, including their concepts and classifications. It concluses with the perception that technological development, the proliferation of electronic devices and devices and the widespread use of the Internet make a permanent reflection and study imperative, the only possible way to combat new forms of crime and cybercriminal phenomena, and internalization is indispensable of the Budapest Treaty.

KEYWORDS: Information society – Cybercrimes – Precautionary measures – Means of proof. – Budapest Convention.

SUMÁRIO: 1. Introdução. 2. Prólogo: a sociedade da informação em perspectiva. 3. A criminalidade informática: conceitos e classificações. 4. O cenário nacional: medidas cautelares e meios de provas nos crimes cibernéticos no Brasil 5. A convenção de Budapeste e o cenário internacional dos meios de prova em crimes cibernéticos. 6. Conclusões. 7. Referências.

1. INTRODUÇÃO

Inaugura-se, com o despertar deste novo tempo, uma nova sociedade, impulsionada por um novo estágio do modo de produção capitalista e, principalmente, pela disseminação em escala mundial a do desenvolvimento das novas tecnologias.

Não restam dúvidas de que hoje e, sobretudo no futuro, a vida humana continuará se expandindo sobre o ciberespaço e com isso os órgãos públicos, em especial aqueles destinados à solução de conflitos e em especial, à persecução criminal, como a Polícia Judiciária (investigativa), o Ministério Público, o Legislativo e o Judiciário, terão de estar preparados com mecanismos eficazes para atender as demandas que lhes serão impostas.

Assim, o presente estudo tem como escopo compreender a trajetória da informação, enquanto instrumento tendente a angariar, manter ou buscar poder na sociedade da informação, analisando, especialmente a realidade traduzida no século XXI quando a internet passou a ser utilizada habitualmente como instrumento da criminalidade. A partir

daí, pretende-se analisar algumas questões relacionadas à dogmática jurídico-penal, no que tange à prática de crimes cibernéticos, bem como a mecanismos atualmente adotados e cuja efetividade é analisada à luz de aspectos socioculturais, chegando-se a proposição de meios persecutórios que poderão ser adotados para uma produção de provas de maior extensão e profundida à formação da firme convicção judicial e consentânea com princípios garantísticos de bens jurídicos constitucionalmente tutelados, mas diuturnamente atacados pelos crimes praticados no seio da sociedade da informação.

A metodologia do artigo adota a técnica analítica, analisando-se aspectos de cunho constitucional-sociológico, no qual são analisados aspectos normativos sob o enfoque dialético, crítico-reflexivo e referencial teórico.

2. Prólogo: a sociedade da informação em perspectiva

Em uma análise objetiva, mas extremamente precisa, Castells afirma que no final dos anos 90, vários acontecimentos de importância histórica transformaram o cenário social da vida humana. Uma verdadeira revolução tecnológica concentrada nas tecnologias da informação e da comunicação passou a remodelar a base material da sociedade em ritmo acelerado, a tal ponto que o século XXI tem se apresentado ao mundo, como um estágio inexplorado do desenvolvimento histórico, econômico, cultural, social, jurídico e político, denominado pelo próprio autor como sociedade em rede.[1]

Muito embora seja fortemente difundida a visão de que o avanço tecnológico da sociedade em rede propicia propósitos positivos inegáveis, não se pode olvidar que, apesar disso, essa evolução também, dialeticamente, provoca alterações de cunho estrutural nas relações sociais humanas e desafios à normatividade jurídica, notadamente, penal e processual penal. Nas palavras do ex vice Secretário-Geral da ONU Jan Eliasson: "A tecnologia vem fazendo avanços tremendos contra a fome, as doenças e o desperdício de energia. Mas também fortalece o crime organizado e aumenta o espectro de ataques cibernéticos"[2].

Nota-se, dessa maneira, uma dualidade de aspectos, quais sejam, de um lado, o positivo tendo em vista que na atual sociedade de rede, toda a informação se desenha em marcas indeléveis no campo da cultura e na disseminação do conhecimento humano, através da celeridade e instrumentos de busca oferecidos pela internet – de outro, o negativo que perfaz um lado extremamente preocupante inerente à forma de como a internet vem sendo gerida pelo mercado consumerista, relações sociais e governos nacional e internacional.

1. CASTELLS, Manuel. A Era da Informação: economia, sociedade e cultura. v. I, a sociedade em rede. 6ª ed., São Paulo: Paz e Terra, 2002, p. 39.
2. ONU. 13º Congresso sobre o Crime da ONU: o impacto dos delitos no desenvolvimento. Disponível em UNITED NATION INFORMATION SERVICE: https://unis.unvienna.org/unis/events/2015/crime_congress.html. Acesso em: 26/10/2020.

> "Claro é que aliada à expansão das novas tecnologias, observa-se o desenvolvimento de uma intensa e complexa extensão de novas situações fáticas ainda desprovidas de regulamentação jurídica, especialmente, na área criminal, que acaba por ser dependente de conhecimentos muito precisos e técnicos sobre o mundo digital, impondo-se assim, o seu estudo de forma inclusive multidisciplinar. Ademais, o crescimento tecnológico percorre dimensões objetivamente mais rápidas em comparação ao desenvolvimento doutrinário e legislativo sobre o tema que requer o rompimento de barreiras dogmáticas em face dos institutos jurídicos penais e processuais penais propostos até o presente momento"[3].

Tomando-se por base os saltos tecnológicos e do conhecimento que marcaram o final do século XX e a transição para o XXI, nada impede que reconheçamos e desejemos o desenvolvimento do ser humano enquanto espécie, reconhecendo, até com certo destaque, o progresso social, cultural e educacional (com a inclusão digital), entretanto, não se pode perder de vista que nem sempre o processo envolvente das novas tecnologias carrega violações contumazes e severas aos direitos e garantias fundamentais previstos na Constituição Federal de 1988.

A dependência social aos meios tecnológicos e a proliferação da criminalidade cometida por meio informático são fenômenos incontornáveis e fáticos da Sociedade de Informação.

Torna-se indispensável, assim, analisar quais são os direitos que podem vir a ser violados no contexto das tecnologias informáticas e dos crimes eletrônicos e indagar se existem tipos penais específicos o suficiente no ordenamento jurídico-penal brasileiro a descrever taxativamente essas violações aos bens jurídicos que devem ser (penalmente) tutelados. Ou se, ao menos, as ofensas a estes bens criminalmente relevantes, poderiam ser subsumidas a tipos comuns previstos no Código Penal, como é o caso dos crimes patrimoniais como furto ou estelionato ou crimes contra a honra como a calúnia, a difamação ou a injúria.

Portanto, o cenário jurídico-penal que se encontra é que se de um lado há uma ausência bastante significativa de tipificações legais em relação aos crimes praticados no contexto da sociedade da informação e no âmbito da internet, que se quedam sem normatização, sem a devida apuração e responsabilização, por conseguinte; de outro, como entende Fuller, o Direito Penal não pode servir como instrumento de coerção, se não franqueado pela ideia de servir como *ultima ratio* para a tutela de bens jurídicos[4].

---

3. FULLER, Greice Patrícia. Crimes na sociedade da informação: uma nova realidade fenomênico-jurídica. In: LISBOA, Roberto Senise (coord.). O Direito na Sociedade da Informação. São Paulo: Almedina, 2020.
4. FULLER, Greice Patricia. Crimes na sociedade da informação: desafios a dogmática jurídico-penal em face dos direitos humanos. In: II Congresso Luso-brasileiro de direitos humanos na sociedade da informação. Maçao: Instituto Terra e Memória, 2017. Disponível em: [http://www.pacadnetwork.com/itm/images/sampledata/Domeniu/Area%20Domeniu%206%20Oosterbeek,%20Fiorillo%202017._Online_Version_final_Compressed.pdf]. Acesso em: 12/10/2020.

A partir das digressões acima, a investigação e a efetiva repressão dos crimes informáticos, máxime aqueles crimes praticados através da internet, constitui hoje um desafio para o Estado, pela forma dissimulada e potencialmente oculta que os encerra, designadamente quanto à sua autoria, à produção de elementos informativos de sua materialidade, mas, especialmente, pela capacidade de propagação nociva das ofensas praticadas neste ambiente de interligação das redes inerentes aos sistemas informáticos.

Contudo, é inegável a contribuição para o processo das provas armazenadas em suporte informático na investigação de qualquer crime, em especial, os virtuais, em um momento histórico em que a localização, as preferências, o círculo de amizades, as conversações, os elementos de trabalho, as fotografias, os vídeos, são dados recolhidos e armazenados pelos sistemas informáticos.

No plano judiciário atravessa-se, ainda, um período de grande indefinição quanto à margem de atuação constitucionalmente e legalmente permitida à investigação e persecução penal em confronto com o respeito pelos direitos fundamentais dos cidadãos. Dificuldade potencializada pelos inúmeros obstáculos na interpretação e aplicação do direito constituído relativo à prova digital em processo penal, fruto de uma desconcertante insistência do legislador em manter inalterado o quadro normativo-regulador da matéria, não só sistematicamente disperso em vários diplomas como também de conteúdo aparentemente conflitante – quando existente.

3. A criminalidade informática: conceitos e classificações

O conceito de criminalidade informática abarca 2 (duas) diferentes realidades criminológicas, a saber: os crimes praticados contra os sistemas informáticos, atualmente previstos e punidos em nosso sistema jurídico através do Código Penal e outras leis extravagantes. No Código Penal, mais certo nos artigos 313-A e 313-B, além do Art. 154-A todos do referido diploma legal, este último incluído pela Lei 12.737/2012 (popularmente conhecida como Lei Carolina Dieckman). Na legislação esparsa em tipos como o Art. 10 da Lei 9.296/96, que traz o crime de interceptação telefônica, informática ou telemática sem autorização judicial ou com objetivos não autorizados por lei.

E os crimes praticados por meio de um sistema informático, aqui englobando-se todo o crime perpetrado através de meios tecnológicos, mas que não tenha o sistema informático ou sistema telemático como objeto material da conduta delitiva, isto é, como objeto ou coisa sobre a qual recai a conduta criminosa. Para essa classificação – menos rebuscada e menos complexa – todos os crimes que utilizam a internet ou o sistema informático como meio estariam abrangidos pelo conceito de criminalidade informática. Assim, não só a divulgação não autorizada de imagem, cena de sexo ou pornográfica (Art. 218-C), os tipos de pornografia infantil previstos no ECA (Art. 241-A a Art. 241-E da Lei 8.069/90), além dos crimes contra a honra, patrimoniais e todas as falsidades cometidas através de meio eletrônico, entre muitos outros.

Fuller, Greice Patricia; Pedrosa, João Marcelo Braga Fernandes. Medidas cautelares e meios de prova nos crimes cibernéticos. *Revista dos Tribunais*. vol. 1031. ano 110. p. 207-224. São Paulo: Ed. RT, setembro 2021.

No Brasil, o tema encontra-se desenvolvido, no Boletim 101 do IBCCrim, no qual é utilizada a seguinte classificação para a criminalidade eletrônica: crime virtual puro (chamado por outros doutrinadores de "próprio") significa "toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas". Segundo o autor, além destes, há ainda os chamados crimes virtuais mistos, que são aqueles cujo uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático[5]. E por fim, há os crimes virtuais comuns, considerados como aqueles que se utilizam da internet apenas como instrumento ou meio para a realização do delito já tipificado pela lei penal, como é o caso dos artigos 122, 138, 139, 140, 147 e 171, todos do Código Penal.

E em que pese a redação utilizada pelo autor que preferiu a expressão "crimes virtuais", essa não soa como a melhor opção, uma vez que pode levar o intérprete a acreditar que trata-se de uma ofensa irreal, existente apenas em potência ou sem efeito real, isto é, que não existe efetivamente, é de se observar que os cibercrimes ou crimes informáticos existem e, mais do que isso, estabelecem novas formas de violação de bens jurídicos, cometidas através das tecnologias de informação e comunicação. E, por esse motivo, devem ser pensados novos tipos penais e reanalisados os tipos penais já existentes para que se busquem soluções político-criminais a este quadro[6].

Dentro desta perspectiva, os bens jurídicos que podem ser violados em face dos crimes cometidos na sociedade da informação são vários, e todos de estatura constitucional, podendo ser indicados, *v.g.*: os direitos à intimidade, à privacidade, à integridade física e a "integridade digital" dos dispositivos ou redes comunicacionais dos cidadãos. Além destes, os direitos à produção e criação literária, artística, o direito inerente à proibição de toda e qualquer forma de discriminação, em razão de raça, sexo, cor, religião, opinião ou qualquer outra condição ou circunstância pessoal ou social, bem como à ordem democrática de um país ou o direito ao segredo das comunicações[7] que também podem ser lesionados em face de ingerências não autorizadas de terceiros, violando a confidencialidade de determinada informação. Romeo Casabona ainda assevera, demais bens jurídicos como, a produção e criação literária, artística, científica e técnica e o direito inerente

5. PINHEIRO, R.C. 2001. Os crimes virtuais na esfera jurídica brasileira. In: Boletim IBCCrim, ano 8 (101), p. 19.
6. FULLER, Greice Patricia. Crimes na sociedade da informação: desafios a dogmática jurídico-penal em face dos direitos humanos. In: II Congresso Luso-brasileiro de direitos humanos na sociedade da informação. Maçao: Instituto Terra e Memória, 2017. Disponível em: [http://www.pacadnetwork.com/itm/images/sampledata/Domeniu/Area%20Domeniu%206%20Oosterbeek,%20Fiorillo%202017._Online_Version_final_Compressed.pdf]. Acesso em: 12/10/2020.
7. FULLER, Greice Patrícia. Crimes na sociedade da informação: uma nova realidade fenomênico-jurídica. In: LISBOA, Roberto Senise (coord.). O Direito na Sociedade da Informação. São Paulo: Almedina, 2020, p. 391.

à proibição de toda e qualquer forma de discriminação em razão de condição ou circunstância pessoal ou social[8].

Certo é que, afora aqueles que possuem previsão legal no Código Penal ou na legislação penal extravagante, em sua maioria crimes cibernéticos comuns, boa parte dos crimes eletrônicos próprios (puros) ou mistos, restam sem cobertura jurídico-penal, o que, por óbvio, dificulta, sobremaneira, a apuração dos referidos delitos em respeito ao princípio da legalidade estrita do direito penal. Isto ocorre pela dificuldade em apurar as condutas praticadas sob o manto do anonimato, praticadas sob um aspecto metafórico, na maioria das vezes a portas fechadas, através de um ambiente virtual que não se apresenta com um lugar de tentativa ou consumação no espaço físico, mas também em razão da falta de ferramentas disponíveis para a realização da apuração criminal neste ambiente que, como defende o filósofo francês Augé (1994)[9], trata-se de um "não-lugar".

Em alguns casos, observa-se a inexistência de legislação específica sobre o tema, entretanto, as situações referentes às práticas permitem subsunção, entre o fato e a norma, de forma indireta nos crimes já previstos no Código Penal, como é o caso de, em algumas hipóteses: a) contra a honra (artigos 138 a 140); b) constrangimento ilegal (artigo 146); c) ameaça (artigo 147) e d) participação em suicídio (artigo 122).

Ocorre que, devido à complexidade do sistema penal e de seus princípios norteadores, como é o caso da legalidade estrita, esta subsunção por via transversa ou indireta nem sempre será possível. Não sem razão, Fuller, em leitura sistemática do ordenamento penal, cotejando com a norma constitucional, salienta que: "se de um lado há a necessidade de contenção das condutas ilícito-tecnológicas, de outro, há lacunas em relação aos tipos penais e o uso de analogia *in malam partem* ofenderia frontalmente o princípio da legalidade estrita no chamado Estado Democrático de Direito"[10].

Não é preciso ir longe para se observar, com pesar, que um dos tipos penais mais basilares desse novo ecossistema e dessa nova realidade social, a invasão de dispositivo eletrônico, apenas teve a sua conduta criminosa definida legalmente no ano de 2012, através

8. CASABONA, Carlos María Romeo. La adaptación del Derecho Penal al desarrollo social y tecnológico. Granada: Comares, 2010, p. 305.
9. Um dos maiores problemas para a Doutrina que cuida da jurisdição e da competência no caso dos chamados crimes cibernéticos/eletrônicos, está no fato de que esses crimes são cometidos em um "espaço" que é: abstrato; sem identidade física; e ausência de fronteiras territoriais. Então, a tratar deste espaço, do chamado "cyber espaço", temos que levar em consideração o fato de que neste lugar (não-lugar), não vigoram conceitos de: soberania e competência territorial. Augé afirma que a rede promove a diluição das fronteiras geográficas, mas também a geração de novos territórios, identidades e práticas sociais. Lugares e Não lugares. (AUGÉ, 1994).
10. FULLER, Greice Patricia. Crimes na sociedade da informação: desafios a dogmática jurídico-penal em face dos direitos humanos. In: II Congresso Luso-brasileiro de direitos humanos na sociedade da informação. Maçao: Instituto Terra e Memória, 2017. Disponível em: [http://www.pacadnetwork.com/itm/images/sampledata/Domeniu/Area%20Domeniu%206%20Oosterbeek,%20Fiorillo%202017._Online_Version_final_Compressed.pdf]. Acesso em: 12/10/2020, p. 184.

USO EXCLUSIVO CUT

da chamada Lei Carolina Dieckman (Lei 12.737 de 30 de novembro de 2012). E foi necessária uma enorme comoção popular e clamor midiático, para que um caso envolvendo uma famosa atriz, desse ensejo à movimentação legislativa no sentido de regulamentar a referida conduta.

Outros crimes ainda mais graves demoraram ainda mais tempo para receber a devida atenção legislativa, como é o caso do Art. 218-C do Código Penal, publicado apenas em 2018. O crime em questão pune, entre outros casos, aquele que publica ou divulga, por qualquer meio – inclusive por meio de comunicação de massa ou sistema de informática ou telemática –, fotografia, vídeo ou outro registro audiovisual que contenha, sem o consentimento da vítima, cena de sexo, nudez ou pornografia, consistente na chamada "Pornografia de Vingança" (ou *Revenge Porn* na expressão em inglês). Antes da Lei n. 13.718, de 2018, que trouxe a referida conduta delitiva, esse caso, assim como inúmeros outros do nosso ordenamento jurídico, em razão da absoluta ausência de dispositivos próprios para os crimes cibernéticos, era enfrentado com adaptações, malabarismos ou contorcionismos jurídicos que muitas vezes não se sustentavam no curso de um longo e complexo processo judicial que visa avaliar todas as elementares e circunstâncias do delito, no momento da adequação do fato com sua previsão legalmente instituída.

Tudo isso, sem falar naqueles casos, ainda, ampla e solenemente ignorados pelo Poder Legislativo, como parece ser o caso, em situações menos complexas, das inúmeras modalidades de fraudes informáticas em crimes praticados contra o patrimônio das vítimas ou mesmo os casos dos chamados perseguidores (*stalkers* e *cyberstalkers* – no âmbito das relações doméstico-familiares), casos de *bullying* virtual (*cyberbullying);* ou mesmo, em casos mais complexos, como é o caso de crimes contra a humanidade, quais sejam: as novas modalidades de terrorismo ou guerra virtual, ciberterrorismo e ciberguerra (*cyberwar*), para os quais não há sequer forma oblíqua de encaixe ou adequação entre o fato e a norma penal.

4. O CENÁRIO NACIONAL: MEDIDAS CAUTELARES E MEIOS DE PROVAS NOS CRIMES CIBERNÉTICOS NO BRASIL

Demonstra-se dessa forma que as instituições públicas brasileiras trabalham com excessiva morosidade, sem que se digne a legislar sobre temas de grande envergadura e relevância, seja em razão da complexidade dos atos e ritos com que são desenvolvidos, seja por pura e simples falta de vontade política daqueles que comandam a máquina pública, frequentemente preocupados com outras questões relacionadas ao orçamento público, questões econômicas como aumento de seus próprios salários ou com a boa e velha disputa política do poder pelo poder. Em sendo assim, há que se admitir que é muito difícil, para não dizer absolutamente improvável, que o legislativo nacional possa produzir, na mesma velocidade em que as novas tecnologias evoluem, legislações que venham a regulamentar esses novos tempos e as novas realidades em que somos (e estamos) cada vez mais inseridos.

Sob este paradigma, é possível dizer com boa margem de certeza que não há – e, talvez em um prognóstico intuitivo sobre a realidade fática do desenvolvimento do ritmo das novas tecnologias nem nunca haverá – suficientes tipos penais no sistema jurídico-penal brasileiro que descrevam taxativamente violações aos bens jurídicos merecedores de reprimenda penal. Mais do que isso, é possível ainda afirmar que os meios de apuração, ou seja, as normas processuais que regulamentam as medidas cautelares e os meios de prova para crimes eletrônicos/cibernéticos também não acompanharão a evolução das novas tecnologias.

Nesse ponto da exposição, não se pode ignorar que de acordo com o Conselho Europeu da ONU, através a Convenção sobre o Cybercrime, também conhecida como Convenção de Budapeste, o cibercrime é a modalidade criminosa que mais cresce no mundo e já afeta milhões de pessoas em todo o planeta. E que estes crimes se manifestam de diferentes formas, como delitos relacionados à identidade, violações de direitos autorais, pornografia infantil, entre outros abusos. É, por isso mesmo, uma das maiores ameaças para esses cerca de 3 (três) bilhões de usuários da internet que, conscientes ou não, armazenam, produzem e difundem informação online.

Com o aumento da facilidade de cometer este tipo crime, agentes da lei encontram cada vez mais dificuldades para conter sua propagação frente aos desafios impostos pelos avanços tecnológicos. Em regra, países em desenvolvimento, como o Brasil, não têm a capacidade para combater os ataques virtuais e por isso contam com um índice mais alto de vítimas. Segundo a ONU, o crime cibernético cresce rapidamente em todo mundo e se tornou um negócio lucrativo, que pode ultrapassar a casa dos 3 (três) trilhões por ano em prejuízos. Neste contexto, a necessidade de políticas voltadas a proteção dos cidadãos nunca foi tão importante[11].

Apenas mencionando o Brasil, o crescente aumento na criminalidade cibernética, colocou o país como o segundo no mundo em casos de crimes dessa natureza, afetando cerca de 62.000.000 (sessenta e dois milhões) de pessoas e causando prejuízos na casa dos R$ 22.000.000 (vinte e dois milhões de dólares)[12]. E isto, é de se notar, sem que se esteja a tratar de uma criminalidade complexa, como é o caso das grandes organizações criminosas ou terroristas. Cada vez mais, autores delitivos, mesmo os de menor potencial lesivo e periculosidade tem explorado a velocidade, a conveniência, as ferramentas e o anonimato da rede mundial para praticar uma vastidão de atividades criminosas que desconhecem fronteiras e limites físicos, e representam novas ameaças a economia global.

11. ONU. 13º Congresso das Nações Unidas Sobre Prevenção de Delitos e Justiça Criminal. Data 12 a 19 de abril de 2015. Disponível em: [https://unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html]. Acesso em: 26/10/2020.
12. SUPERIOR TRIBUNAL DE JUSTIÇA. Crimes pela internet, novos desafios da jurisprudência. Disponível em: [http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx] A.cesso em 20/10/2020.

Basta imaginar um simples *hacker* que, de sua casa no Brasil, conecta-se, a servidores norte-americanos e invade sites de bancos em paraísos fiscais como a Suíça para subtrair milhões em valores monetários de diversas contas bancárias, depositando-os em uma conta clandestina em um banco da Rússia e, em seguida, convertendo esses valores em *bitcoins* em servidores na Alemanha para utilizar as moedas virtuais para comprar produtos exportados da China. O ilícito penal exemplificado, foi praticado por uma única pessoa isoladamente e sem a necessidade de grandes investimentos, porém, a sua investigação demandará esforços internacionais cooperativos incomuns e absolutamente irreais para os padrões nacionais.

Como acima mencionado, é perceptível que o Estado brasileiro responde de forma ainda ineficiente e despreparada, a crimes desta natureza, em face da existência de lacunas em nosso sistema processual penal e prescrições normativas para medidas cautelares ou meios de produção de prova que permitam uma apuração mais adequada dessas infrações informáticas. A título de exemplo, pode-se dizer que a apuração dos crimes cibernéticos no Brasil, apresenta-se quase à sua inteireza à base de adequações legislativas e mecanismos utilizados por via de adaptação, como acontece com as determinações judiciais para busca e apreensão de dados informáticos e/ou telemáticos. Basta para tanto observar as já famosas operações da Polícia Federal, *v.g.* Nestes casos, é corriqueiro observar quando das operações televisionadas, agentes da Polícia Federal carregando, em seus braços, CPUs e, por vezes, até monitores de computadores, o que revela um dado importante, qual seja: o de que quando é necessário localizar nos arquivos pessoais do investigado determinado documento ou prova, ao invés da utilização de uma ferramenta mais adequada, como o monitoramento ou a invasão do dispositivo eletrônico do autor do delito, as autoridades contam com a sorte ao somente tentar localizar algo naquele computador após a prisão, sendo obrigado a contar assim com a presteza do criminoso, de manter as provas do delito intactas em sua máquina.

A utilização dos meios tecnológicos deixa rastros nos sistemas operativos, informáticos e até mesmo na rede de forma geral. Muitos dados informáticos são armazenados no sistema de forma automática, sob a forma de *logs,* de ficheiros ou arquivos temporários (*temporary files*) ou caixa de mensagens, que ficam gravados no *hard drive* do dispositivo ou nas bases de dados do sistema. Outros tantos são armazenados pela vontade do utilizador. Por essa razão, ao utilizar um dispositivo, o utilizador conforma-se com a possibilidade desse armazenamento ocorrer, a não ser que tenha o cuidado de proceder a uma limpeza dos dados e pastas armazenados após a utilização.

Entretanto, o direito à intimidade, à reserva da vida privada e a proibição de acesso às comunicações privadas são direitos constitucionalmente garantidos aos cidadãos. E, por esse motivo, não podem sofrer restrição ou redução, salvo os casos devidamente autorizados por lei. É nesta senda que a atualização legislativa para a captura e obtenção de prova em meio digital torna-se imprescindível, uma vez que utilizar-se apenas de fórmulas pré-estabelecidas e criadas em um tempo que sequer se imaginava que este cenário existiria, já não é suficiente em face da realidade do século XXI.

De uma forma geral, o que se têm atual e comumente, no Brasil, como medidas cautelares e meios de produção de prova em crimes cibernéticos são as mesmas medidas que já existiam em 1941 no Código de Processo Penal e na década de 90, quando se refere às legislações esparsas. No código processual, o que se observa é basicamente a utilização de mandados de busca e apreensão para obtenção de provas em equipamentos eletrônicos ou em redes de computadores e/ou virtuais como, aliás, sempre se fez no processo penal quando para arquivos, pastas ou outros documentos físicos de interesse àquele processo, em regra, com fundamento no Art. 240, § 1º, *alínea* "h" do CPP. O que, como se sabe não se trata de medida totalmente hábil e eficaz no contexto da criminalidade digital, uma vez que estamos na era do *cloud computing* (da computação em nuvem) e é de se esperar que as provas dos delitos cometidos por intermédio dos computadores não fiquem armazenadas nestes dispositivos, mas em backups, em nuvens ou mesmo em servidores localizados em países estrangeiros.

Outra medida possível e que, cumpre salientar, sofreu atualização pontual, é a interceptação telefônica e de dados informáticos e telemáticos prevista na Lei 9.296/96. Convém ponderar de maneira crítico-pragmática, sem olvidar-se de aspectos científicos, do qual é dotado o Direito, que inicialmente, com o advento da lei, o que as autoridades competentes para a investigação criminal mais utilizavam era a interceptação das comunicações telefônicas, contudo, atualmente tais medidas apresentam, sua eficácia e uso reduzidos, a medida em que as comunicações são realizadas atualmente através de trocas de mensagens e conversações mantidas através de aplicativos *online* destinados a esta finalidade, tais como *WhatsApp., Facebook Messenger, Telegram*.

Claro é que não apresentam a finalidade precípua de servirem de provas à persecução penal, mas permitem o envio de mensagens de texto e voz, como o *Instagram* ou o *Snapchat,* isso sem falar nos aplicativos de ligações em voz sobre IP (*voip*) o que dificulta, sobremaneira, tanto a interceptação das comunicações seja em forma de texto ou voz, como a localização dessas informações em arquivos de backup, devido ao formato criptográfico de ponta a ponta realizada pelas empresas para preservar a intimidade de seus usuários, tal qual acontece com o *Facebook* (proprietário das mais importantes plataformas deste segmento – *WhatsApp, Facebook Messenger e Instagram*).

Como se observa do quadro acima narrado, a mera solicitação judicial para busca e apreensão de um computador ou outro aparelho eletrônico de propriedade do autor de um delito ou mesmo a interceptação das comunicações telefônicas ou telemáticas poderão não ser suficientes para localizar os indícios de autoria e a prova da materialidade delitiva que se pretende obter para a apuração criminal. Some-se a isto, a posição ainda indefinida dos Tribunais Superiores em relação à análise da licitude da prova obtida pela autoridade policial ou seus agentes, sem autorização judicial, mediante acesso a registro telefônico ou a agenda de contatos de celular apreendido no local do delito e estar-se-á diante da quase total impossibilidade de colheita de provas para os crimes eletrônicos ou cibernéticos, na atual perspectiva do cenário nacional, ao menos com as ferramentas que estão hoje instituídas como opção para a colheita de provas destes delitos.

Fuller, Greice Patricia; Pedrosa, João Marcelo Braga Fernandes. Medidas cautelares e meios de prova nos crimes cibernéticos. *Revista dos Tribunais*. vol. 1031. ano 110. p. 207-224. São Paulo: Ed. RT, setembro 2021.

Em outro cenário bem menos explorado e um tanto mais restrito, é possível observar que o legislador, em alguns casos propôs contornos mais modernos à apuração criminal e às medidas cautelares para produção de provas a determinados delitos. É o que se observa das disposições da Lei 12.850/2013, que trata das organizações criminosas e dispõe sobre a investigação criminal e os meios de obtenção da prova nas infrações penais sob este pano de fundo. Nesta senda, impõe o legislador nacional a possibilidade de, em qualquer fase da persecução penal, a obtenção, entre outras das provas consubstanciar-se no a) acesso a registros de ligações telefônicas e telemáticas; b) interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica e c) infiltração, por policiais, em atividade de investigação.

Neste último caso, previu o legislador no art. 10-A da Lei 12.850/2013, que será admitida a ação de "agentes de polícia infiltrados virtuais" na internet, com o fim de investigar os crimes previstos na lei e outros a eles conexos, praticados por organizações criminosas, previsão está trazida a lume pela Lei 13.964, de 2019. A inserção de usuário oculto, como chamada na prática, permitiria a autoridade policial – ou agente desta – observar e analisar a conduta do investigado em tempo real, verificando que tipo de conversas mantém e com quem se relaciona através de aplicativos como *Facebook e WhatsApp*., os locais que frequenta (*online* e *off-line)* e até mesmo se pratica os delitos de que está sendo acusado através das redes de computadores, "fornecendo" essas provas sem que haja tempo para excluir ou apagá-las de seus. Ocorre que mesmo havendo previsão para o referido meio de prova, é preciso notar que estas medidas estão disponíveis apenas para os delitos referentes às organizações criminosas e a outros a eles conexos, o que revela que outros casos, ainda que da mesma natureza ou de maior gravidade não poderão, caso não sejam praticados por organizações criminosas na forma do Art. 1º, §1º da Lei 12.850/2013 não terão à sua disposição as mesmas ferramentas.

Não por outro motivo, é que se faz necessário que tanto o Estado quanto o direito se atualizem e acompanhem esta nova realidade que nos traz a Sociedade da Informação. Não apenas em relação aos mecanismos policiais que precisam ser atualizados, mas também uma maior cooperação entre os órgãos, que são absolutamente indispensáveis para a persecução do delito, mas também é preciso conceber, ademais, que essa nova forma de ilicitude, advinda da criminalidade eletrônica, possui algumas características próprias e, por isso mesmo, demanda a adoção de uma nova dogmática jurídico-penal.

5. A CONVENÇÃO DE BUDAPESTE E O CENÁRIO INTERNACIONAL DOS MEIOS DE PROVA EM CRIMES CIBERNÉTICOS

A convenção de Budapeste consiste em um tratado firmado por diversos países no sentido de produção de provas realizadas de forma mais célere, através de mecanismos probatórios especialmente digitais e de contar com a denominada cooperação jurídica entre os seus signatários, para além de em seu preâmbulo enunciar que o delito informático consiste em "todo acto dirigido contra la confidencialidade, la integridade y

la disponibilidade de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos"[13]. Com isto, a cibersegurança – necessidade de existência de segurança nas ferramentas e instrumentos relativos às tecnologias da informação[14] – tem a potencialidade de ser mais efetivada, evitando os danos resultantes de crimes provocados no ciberespaço que possuem as notas da transnacionalidade e do anonimato.

Para fins de apuração criminal, observa-se que o Brasil encontra-se ainda em situação de defasagem em relação aos outros países, em especial no que concerne àqueles signatários da Convenção de Budapeste, para os quais, já possível registrar o surgimento de conceitos extremamente atuais em relação à colheita de prova em meio eletrônico ou virtual.

Entre os conceitos acima mencionados, cita-se *v.g.*, o conceito de prova digital voluntariamente disponibilizada e publicamente acessível ou prova digital coercivamente recolhida, seja pela via da solicitação seja por via de busca e apreensão (artigo 19), conservação expedita de dados informáticos armazenados (artigos 16 e 17), recolha em tempo real de dados telemáticos (artigo 20) e interceptação de dados (artigo 21).

No que se conecta aos conceitos de prova digital voluntariamente disponibilizada e publicamente acessível ou prova digital coercivamente recolhida, sabe-se que todos os cidadãos dispõem de instrumentos capazes de eliminar ou ocultar os dados informáticos armazenados pela sua utilização do sistema, e em geral, de legitimamente vedar o acesso a tais dados em dispositivos ou redes de computadores que controlam ou acessam.

Contudo, não o fazendo, o utilizador renúncia tacitamente à exclusiva disponibilidade dos dados. Assim sendo, o consentimento operante nestas hipóteses será semelhante àqueles casos em que se discute as provas invasivas e não invasivas[15].

Ora, se a prova é publicamente acessível ou voluntariamente disponibilizada, consistindo na mera inspeção ou análise superficial dos dados publicados ou disponibilizados online pelo usuário da rede, ainda que independente de autorização judicial, não haverá falar em ofensa as esferas da intimidade ou privacidade do usuário. Assim, nada impede,

13. CONSELHO DE EUROPA. Instrumento de Ratificación del Convênio sobre la ciberdelincuencia. Boletín Oficial del Estado núm. 226, 17/04/2010.

14. FULLER, Greice Patrícia. Cibersegurança: utopia ou realidade pragmática? In: PEREIRA, Claudio José Langrovia. Segurança Pública, instituições democráticas e seus elementos históricos, políticos e econômicos. São Paulo: Quartier Latin, 2019, p. 177.

15. Renato Brasileiro em seu Curso de Processo Penal, ao tratar do direito à não autoincriminação (*nemo tenetur se detegere*), professa a existência do direito de não produzir nenhuma prova incriminadora invasiva e nesse ponto, afirma ser importante tratar do que se entende por intervenções corporais, assim como o conceito de provas invasivas e não invasivas. Intervenções corporais (investigação corporal ou ingerência humana) são medidas de investigação que se realizam sobre o corpo das pessoas, sem a necessidade do consentimento destas, e por meio da coação direta se for preciso, com a finalidade de descobrir circunstâncias fáticas que sejam importantes para o processo, em relação às condições físicas ou psíquicas do sujeito que sofre as intervenções, ou objetos escondidos com ele. (LIMA, 2011, p. 925).

portanto, que o proprietário de um *smartphone* voluntariamente disponibilize à investigação o conteúdo de um SMS enviado pelo alvo na investigação que não a apagou depois de utilizar o aparelho.

Há, contudo, que distinguir, para efeitos processuais, a disponibilização da prova digital da disponibilização do acesso ao sistema informático onde está armazenada a prova em: a) prova digital voluntariamente disponibilizada ou publicamente acessível e prova digital coercivamente recolhida.

Nesse contexto, analisando a prova digital voluntariamente disponibilizada ou publicamente acessível estão em causa as situações em que o cedente publica informações ou faz chegar ao processo dados informáticos, quer sejam corporizados em reproduções mecânicas (CD's, DVD's, pen drives) ou em papel (impressões, prints, fotografias). Nestas situações aplica-se o regime geral da admissibilidade da prova documental, previsto no Código de Processo Penal, uma vez que não houve intervenção ativa dos órgãos de polícia (ou persecução) na pesquisa e recolha dessa prova. Ela foi, no fundo, "oferecida" às instâncias de controle formais e, como tal, nada impedirá a sua junção aos autos. Como se disse há pouco, não haverá ofensa à intimidade ou privacidade quando a própria parte abriu mão deste direito.

Nos casos acima grafados ocorre uma renúncia explícita do visado à eventual natureza sensível, pessoal ou íntima da informação ou comunicação. É legítima, portanto, a recolha de dados, sejam eles fotografias, mensagens de texto, vídeos, publicações com opiniões e informações pessoais, publicados nas redes sociais, por parte da polícia ou outros órgãos de apuração criminal, sem prévia autorização ou posterior validação judicial. Como boa prática e para prevenir futuros problemas de validade da obtenção da prova, é interessante haver descrição por parte da autoridade ou de seus agentes, no auto de diligência, do local (virtual) onde a prova foi encontrada (designadamente o endereço da web), as circunstâncias de tempo e lugar em que tal diligência ocorreu, bem como uma descrição sintética do tipo de prova obtida e da sua relevância aos autos.

Ademais, há a denominada prova digital coercivamente recolhida. Já nesta segunda hipótese, a prova não é nem voluntariamente disponibilizada nem publicamente acessível, mas sim fornecida mediante uma ordem pública emanada pela autoridade judiciária competente. Trata-se de um caso de disponibilização do acesso ao sistema informático onde está armazenada a prova, a sua recolha pressupõe uma atividade investigatória dos órgãos policiais. E mais do que isso, neste caso, a permissão de acesso, virá do proprietário do sistema informático onde encontra-se armazenada a prova digital e não do concreto titular de cada dado informático individualmente considerado.

Por essa razão, a pesquisa de prova digital em sistema informático que coercivamente recolhida deveria obedecer às regras semelhantes às da busca e apreensão, isto é, ordem da autoridade judiciária competente, manifestação do Ministério Público etc.

Considera-se, portanto, como nos casos de outros direitos constitucionalmente estabelecidos, somente se dispensará a prévia autorização da autoridade judiciária, independentemente da natureza dos dados obtidos, no caso de haver consentimento previamente

prestado pela parte cedente daqueles dados ou o responsável pelo sistema onde os mesmos se encontram, renunciando desta forma o seu direito à privacidade ou intimidade, fato este similar à famigerada autorização para ingresso em domicílio para buscas ou mandados de prisão.

A seguir, analisa-se a modalidade denominada de conservação expedita de dados informáticos armazenados. Neste caso, as autoridades competentes poderão exigir ou obter determinação judicial no sentido de obrigar-se na conservação de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem indícios de que eles são suscetíveis de perda ou alteração. Para a Convenção de Budapeste, em seus artigos 16 e 17, as autoridades terão à sua disposição medidas legislativas e/ou outras que se revelem necessárias para obrigar à determinada pessoa a conservar e proteger a integridade dos referidos dados durante um período de tempo tão longo quanto necessário, até um máximo de 90 (noventa) dias, podendo ser subsequentemente renovada.

Em caráter exemplificativo, pode-se citar o caso de empresas públicas ou privadas de controle de tráfego urbano, dotadas de câmeras para verificar a movimentação de veículos. Usualmente, as companhias de tráfego não possuem um tempo muito longo de gravação das imagens, que ficam disponíveis por cerca de 3 (três) a 5 (cinco) dias, quando passam a ser apagadas dando lugar às novas gravações que vão se sobrepondo às anteriores. Isso quando prazo não é ainda menor, como naqueles casos em que as imagens passam a ser substituídas por outras após 24 (vinte e quatro horas). Assim, caso a autoridade policial ou investigativa entenda necessária a manutenção ou salvaguarda das imagens de um determinado período de tempo de interesse para investigação, pode solicitar (ou obrigar) diretamente à companhia para que não se desfaça daquelas imagens, preservando-as fora do sistema ou gravando-as em outro dispositivo, para impedir que sejam apagadas e, com isso, a prova se perca. Seria também o caso das companhias telefônicas que atualmente possuem serviço de monitoramento e georreferenciamento de aparelhos celulares através das chamadas ERBs (Estações Rádio-Base).

Para que se possa melhor compreender o funcionamento desta ferramenta, pode-se dizer as ERBs funcionam como antenas utilizadas pelo serviço de telefonia celular, que servem para fazer a conexão entre o telefone e a rede da companhia telefônica. Estes equipamentos ficam costumeiramente espalhados pelas cidades e através deles a empresa de telecomunicação é capaz de dizer através de que antena um determinado número de telefone ou aparelho está utilizando a sua rede, sendo certo que para a melhor captação do sinal telefônica os aparelhos são programados para sempre conectar-se à torre mais próxima de onde o aparelho se encontra. Assim, se os órgãos de apuração pretendem traçar a rota percorrida por determinada pessoa, através das Estações Rádio Base é possível realizar a verificação de um trajeto aproximado ou ao menos dizer se o alvo transitou ou não por uma determinada localidade.

Como se observa, os referidos dispositivos legais da Convenção que possuem uma eficácia investigativa colaborativa, em especial se colocados em perspectiva com o

ordenamento jurídico brasileiro onde não apenas estas medidas não existem, como caso se pretenda "importá-las" visando a sua utilização, todas dependeriam de autorização judicial. Esta situação demandaria das autoridades policiais ou outros órgãos responsáveis por apurações impetrarem medidas cautelares inominadas solicitando dos magistrados as referidas providências, que caso autorizadas pelos juízes, após a manifestação do Ministério Público, ainda dependeriam da "boa vontade" e o "espírito colaborativo" das empresas em possibilitarem a colheitas das referidas provas, uma vez que não existem instrumentos coercitivos disponíveis, capazes de obrigar tais companhias a auxiliarem os órgãos de persecução.

6. CONCLUSÕES

Em uma realidade que se vai tornando cada vez mais complexa, o que acarreta, consequentemente, uma sociedade com mais, maiores e diferentes problemas, é da maior importância que o Direito consiga acompanhar em sua doutrina, jurisprudência e ordem normativa essa tendência. Importante salientar que mais do que ser capaz de acompanhar essa evolução de forma gradual, que as normas sejam adaptadas e readaptadas às distintas (e mais adversas) circunstâncias, de forma a que nunca percam a sua atualidade.

O desenvolvimento tecnológico, a proliferação dos aparelhos e dispositivos eletrônicos e a massificação da Internet tornam imperativa essa permanente reflexão e estudo, como condição imprescindível de combater novas formas de criminalidade e os fenômenos denominados cibercrimes. Com tais avanços tecnológicos, a prova digital vem ganhando crescente importância na realidade judiciária cotidiana, podendo-se encontrar e obter uma informação relevante para o desfecho de um processo-crime armazenada em um computador, uma nuvem, um pen-drive, um *smartphone*, um *smartwatch*, um *GPS* ou câmera fotográfica, enfim, em uma infinidade de aparelhos eletrônicos.

O ponto de controvérsia, então, não é outro senão a necessidade ou não de novas legislações para responder aos conflitos provocados pela Sociedade em Rede, em especial no que concerne aos crimes cibernéticos ou informáticos. E de tudo quanto foi exposto nesta pesquisa, o que se observa é que não é surpresa que as instituições públicas brasileiras – e de quase todo o mundo – trabalham com excessiva morosidade, grande parte das vezes, em razão da complexidade dos atos e ritos com que são desenvolvidos.

Faz-se, portanto, necessário que tanto o Estado quanto o direito se atualizem e acompanhem esta nova realidade que nos traz a Sociedade da Informação. Concebendo, de forma premente que essa nova forma de ilicitude, advinda da criminalidade eletrônica, possui características próprias e por isso demandará a adoção de uma nova dogmática jurídico-penal.

Neste sentido é que, visando um processo penal garantístico aos direitos fundamentais proclamados na Constituição Federal e mais eficaz à produção probatória, não se pode descuidar de uma colheita de provas que seja absolutamente atual e vinculada aos mais recentes mecanismos de digitais destinados à apuração criminal.

7. Referências

BARRETO JUNIOR, Irineu Francisco. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; DE LIMA; Cintia Rosa Pereira. (Org.). Direito & Internet III. São Paulo: Quartier Latin, 2015.

BRASIL. Lei Nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal. Disponível em: [http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm]. Acesso em: 10/11/ 2020.

BRASIL. Lei Nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Senado Federal, 2014. Disponível em: [http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm]. Acesso em: 10/11/2020.

CASABONA, Carlos María Romeo. La adaptación del Derecho Penal al desarrollo social y tecnológico. Granada: Comares, 2010.

CASTELLS, Manuel. A Era da Informação: economia, sociedade e cultura. Volume I, a sociedade em rede. 6ª ed., São Paulo: Paz e Terra, 2002, p. 39.

CONSELHO DE EUROPA. Instrumento de Ratificación del Convênio sobre la ciberdelincuencia. Boletín Oficial del Estado núm. 226, 17/04/2010.

FOLHA DE S. PAULO. Internet já tem quase 3 bilhões de usuários no mundo, diz ONU. Disponível em: [http://www1.folha.uol.com.br/tec/2014/11/1553088-internet-ja-tem-quase-3-bilhoes-de-usuarios-no-mundo-diz-onu.shtml]. Acesso em: 26.10.2020.

FULLER, Greice Patrícia. Crimes na sociedade da informação: uma nova realidade fenomênico-jurídica. In: LISBOA, Roberto Senise (coord.). O Direito na Sociedade da Informação. São Paulo: Almedina, 2020.

FULLER, Greice Patricia. Os delitos e as novas tecnologias em face da relação dialógica com os direitos humanos. In: SARLET, Ingo Wolfgang; WALDMAN, Ricardo Label (Orgs). Direitos humanos e fundamentais na era da informação. Porto Alegre, 2020.

FULLER, Greice Patrícia. Cibersegurança: utopia ou realidade pragmática? In: PEREIRA, Claudio José Langrovia. Segurança Pública, instituições democráticas e seus elementos históricos, políticos e econômicos. São Paulo: Quartier Latin, 2019.

FULLER, Greice Patricia. Crimes na sociedade da informação: desafios a dogmática jurídico-penal em face dos direitos humanos. In: II Congresso Luso-brasileiro de direitos humanos na sociedade da informação. Maçao: Instituto Terra e Memória, 2017. Disponível em: [http://www.pacadnetwork.com/itm/images/sampledata/Domeniu/Area%20Domeniu%206%20Oosterbeek,%20Fiorillo%202017._Online_Version_final_Compressed.pdf]. Acesso em: 12/10/2020.

GONZALES-CUELLAR SERRANO, Nicolas. Proporcionalidad y derechos fundamentales em el proceso penal. Madri: Colex, 1990. p. 290. In: FIORI, Ariane Trevisan (org.) A prova e a intervenção corporal: sua valoração no processo penal. Rio de Janeiro: Editora Lumen Juris, 2008.

LIMA, Renato Brasileiro de. Curso de Processo Penal, vol. I. – Niterói, RJ: Impetus, 2011.

ONU. 13º Congresso sobre o Crime da ONU: o impacto dos delitos no desenvolvimento. Disponível em UNITED NATION INFORMATION SERVICE: [https://unis.unvienna.org/unis/events/2015/crime_congress.html]. Acesso em: 26.10.2020.

ONU. 13º Congresso das Nações Unidas Sobre Prevenção de Delitos e Justiça Criminal. Data 12 a 19 de abril de 2015. Disponível em: [https://unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html]. Acesso em: 26.10.2020.

PINHEIRO, R.C. 2001. Os crimes virtuais na esfera jurídica brasileira. In: Boletim IBCCrim, ano 8 (101).

SILVA, Kerolinne Barboza da Silva e CAVALCANTI, Handerson Gleber de Lima. Criminalidade na era da informação: definições sobre criminalidade complexa. Revista de Direito, Governança e Novas Tecnologias. Curitiba, v. 2, n. 2, Jul./Dez. 2016.

SUPERIOR TRIBUNAL DE JUSTIÇA. Crimes pela internet, novos desafios da jurisprudência. Disponível em: [http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx]. Acesso em: 20.10.2020.

Pesquisas do Editorial

Veja também Doutrina relacionada ao tema

- "Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal, de Eduardo Bolsoni Riboli – *RBCCrim* 156/91-139 (DTR\2019\31666).

Veja também Jurisprudência relacionada ao tema

- *RT* 937/180 (JRP\2013\12156).

USO EXCLUSIVO CJF