CRIMES DIGITAIS: RESPONSABILIZAÇÃO E ALTERNATIVAS PARA A TIPIFICAÇÃO PENAL

Marina Helou Giraldeli Toni[1]
marina.giraldeli@outlook.com

Sérgio Augusto Frederico[2]
frederic@femanet.com

RESUMO: Este é o artigo final da pesquisa para o Programa de Iniciação Científica no ano de 2020, de tal modo que foi possível constatar a importância de adequar a legislação e os mecanismos de investigação conforme os avanços tecnológicos, haja vista que as lacunas legislativas ensejam o uso da analogia "*in malam partem",* o que representa uma violação às garantias fundamentais. Foi possível abordar também, novos fenômenos que se apresentam a temática, bem como a procedibilidade na investigação consoante às alterações acrescentadas pela Lei 13.964/2019. Por fim, salienta-se que a presente pesquisa, foi elaborada sob o viés da intervenção penal mínima, tendo em vista que muitas das condutas cometidas no âmbito digital já se encontram positivadas no ordenamento jurídico.

PALAVRAS-CHAVE: Crimes Digitais; Tipificação Penal; Direito Penal.

ABSTRACT: This is the final article of the research for the Scientific Initiation Program in the year of 2020, in such a way that it was possible to ascertain the importance to modernize the legislation and the investigation mechanisms according to the tecnologic advances, considering that the legislation gaps enable the use of the analogy "in malam partem", which represents a violation to the fundamentals garantees. It was also possible to approach new phenomena that presents the thematic, like the procedibility in the investigation consonant to the added alterations by the Law 13.964/2019. Lastly, it is noted that the present research was elaborated under the bias of the minimum penal intervention, having in view that many conduits committed in the digital scope are already affirmed in the current legal ordering.

KEYWORDS: Digital Crimes; Penal typification; Penal Law

---

[1] Graduanda em Direito pela FEMA/Assis. Orientanda.
[2] Mestre em Direito pela Instituição Toledo de Ensino de Bauru-SP, Advogado e Professor do curso de Direito da FEMA/Assis. Orientador.

1. Problemática atual

Segundo a *"Norton Cyber Security"*[3], o Brasil ocupa o segundo lugar com maior número de casos de crimes digitais, e os prejuízos estimados, já somam US$ 22 bilhões. As possíveis justificativas para o crescimento vertiginoso dessa modalidade de criminalidade, é a vulnerabilidade dos dispositivos eletrônicos ocasionada pelo desconhecimento acerca das formas de proteção de dados e da sensação de anonimato experimentada por usuários mal intencionados. Além disso, é notório que a legislação se mostra insuficiente em face aos novos desafios impostos pela "era digital".

Há de se destacar também, que o fenômeno da criminalidade virtual sobrevém naturalmente dada a multifuncionalidade da internet, influindo diretamente nas relações econômicas que passam a ser exercidas no plano virtual a nível global, se tornando um ambiente altamente atrativo para o estabelecimento de um modelo de criminalidade.

2. Crimes em espécie e suas particularidades

2.1. Crimes contra a honra

Os crimes contra a honra se consubstanciam em três tipos penais, sendo estes a calúnia, difamação e a injúria, e atualmente ganham destaque nos índices de criminalidade virtual. A calúnia, prevista no art. 138 do CP, configura a falsa imputação de um fato determinado como um crime a outrem, com pena prevista de seis meses a dois anos e multa. A difamação (Art. 139) por sua vez, ocorre quando o sujeito ativo da ação fere a honra objetiva da vítima, isto é, propaga um fato ofensivo à sua reputação, verídico ou não, e sua pena cominada é de três meses a um ano de detenção e multa. Encerrando o rol dos crimes contra a honra, temos a injúria, tipo penal que visa a proteção da honra subjetiva, punindo aquele que ofende a dignidade alheia se utilizando de adjetivos negativos com um a seis meses de detenção e multa. Segundo Fernando Capez , "O valor ofensivo da injúria deve ser aferido de acordo com o tempo, o lugar, as circunstâncias em que é proferida, até mesmo o sexo do ofendido deve ser levado em consideração". Não obstante, a internet nos últimos anos se tornou o principal meio de difusão de ideias e formas de expressão, sobretudo políticas, e é nesse contexto que surge as "*fake news"*, termo cunhado durante o curso da campanha eleitoral americana

---

3 https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm

que representou um novo paradigma na forma de influenciar a opinião pública e alterar a percepção da realidade, direcionando ataques providos de inverdades a opositores políticos, que normalmente podem ser enquadrados em uma das modalidades de crimes contra a honra. Qualquer tentativa de regulação do ciberespaço, levanta questionamentos acerca dos limites da intervenção estatal, e os possíveis cercamentos a liberdade de expressão, seja através da criminalização de condutas ou por estabelecer padrões de comportamento no ciberespaço.

Há controvérsias no que diz respeito ao limite da lei penal e a amplitude da garantia constitucional da liberdade de expressão, prevista no Art. 5º, IV (liberdade de pensamento), IX (Liberdade de expressão) e no Art. 220, § 1º (Liberdade de Imprensa), compreendendo a proteção da livre expressão e a liberdade de informação como um princípio derivado. Entretanto, a honra também é abarcada pela proteção constitucional como lei fundamental (art. 5º, X), o que requer a ponderação por parte do magistrado defronte a uma situação evidente de violação da honra perpetrada na internet, caberá ao juízo competente determinar a retirada do conteúdo, mediante requisição ao provedor de conexão e de aplicação, sob pena de se responsabilizar civilmente perante a vítima.

Quanto a responsabilidade do autor, sopesando sua culpabilidade e a gravidade dos fatos imputados, em conformidade com a proporcionalidade e a razoabilidade, será fixada na sentença penal condenatória o valor indenizatório, já que a princípio são crimes de pequeno potencial ofensivo.

2.2. Fraude e estelionato

Ambas as condutas estão tipificadas no art. 171 do Código Penal, e consistem na obtenção de vantagem ilícita para si ou para outrem, induzindo a vítima ao erro mediante artifício, ardil, ou outro meio fraudulento. Pode-se dizer que o crime de estelionato é praticado com a contribuição da vítima sem que ela saiba que está expondo seu patrimônio ao risco, ao passo que o autor a induz ao ou a mantém no erro, ensejando obrigatoriamente no prejuízo econômico.

Com o advento das relações comerciais pela internet, os chamados *E-commerces*, bem como a prestação de serviços, os criminosos e organizações criminosas passaram a se especializar e utilizar softwares sofisticados, a fim de forjar URLS, promover links falsos (conduta conhecida como *phishing*), além de adentrarem nos sistemas com a finalidade de se apropriarem de dados pessoais e bancários. De acordo com a DFNDR Lab, laboratório especializado em cibercrimes, apenas no Brasil

no período de abril a setembro de 2017, mais de 70 milhões de pessoas caíram em golpes online.

No que tange a obtenção de vantagem econômica, além dos tipos de fraudes supracitadas, temos a figura do "r*ansomware"*, dentre outras condutas complexas que carecem de maiores especificações no texto legal, que consiste no sequestro de dados por meio da sugestão de links atrativos, e no momento em que são acessados, os criminosos invadem o dispositivo eletrônico de modo a bloquear seu funcionamento e posteriormente determinam um valor de resgate para o desbloqueio. Tal conduta mencionada foi introduzida na legislação penal através da lei 12.737/12 pela redação do Art. 154-A, § 2º, entretanto, o artigo mencionado carece de especificações, bem como uma melhor definição do verbo do tipo penal "invadir", sob pena de dirimir em partes a responsabilização penal.

2.3. Articulação para tráfico de pessoas

O ordenamento jurídico brasileiro acolhe a conduta do tráfico de pessoas no Art. 149-A, que sofreu alterações pela Lei 13.344/16. Dentre essas mudanças, o legislador admitiu a figura do tráfico privilegiado, caso o autor seja primário e não integre organização criminosa e acrescentou a hipótese do tráfico de pessoa com a finalidade de retirar órgãos e tecidos destinados ao mercado negro, além de uma agravante inserida no § 1º, inciso I.

Conforme estudos apontados pela OMT[4] (Organização Mundial do Trabalho), 79% das vítimas são destinadas à prostituição, ao comércio de órgãos e a exploração de trabalho escravo em latifúndios, oficinas de costura e na construção civil.

Não é de hoje que a internet se mostra como um meio eficaz para o aliciamento de vítimas destinadas principalmente à exploração sexual. Comumente a articulação é orquestrada por uma organização criminosa, que no quesito responsabilização, incide o concurso material com os crimes previstos na Lei 12.850/13. Entretanto, não é uma tarefa simples localizar os aliciadores durante o procedimento investigativo, pois estes utilizam se de recursos altamente complexos a fim de camuflar o IP (endereço composto por números capaz de identificar o provedor, bem como o local de acesso) e habitualmente os criminosos desenvolvem suas atividades em camadas profundas da internet, como a "*deep web"* e *"dark web".*

2.4. A pornografia infantil

[4] http://circuitomt.com.br/editorias/cidades/73841-trafico-humano-pessoas-viram-produtos-pela-web.html

A circulação de pornografia infantil, que hoje simboliza uma verdadeira indústria altamente lucrativa, configura uma das maiores violações aos direitos fundamentais das crianças e adolescentes, e atualmente representa uma problemática mundial, pois o comércio de imagens e vídeos está interligado a uma rede transnacional.

A última alteração legislativa presente na Lei 11.829/2008, trouxe uma redação elucidativa em relação ao crime de produção e propagação da pornografia infantil no ECA, que previa apenas o oferecimento de serviços e imagens de cunho pornográfico na rede de computadores. No art. 241 a 241-E, o legislador incluiu na disposição "A" do referido artigo, os verbos oferecer, trocar, disponibilizar, transmitir, distribuir publicar e divulgar, também foi acrescentada a criminalização do mero arquivamento, posse e armazenamento de imagens e vídeos. Logo, é cabível a devida diferenciação texto legal do sujeito receptor do conteúdo pornografico dos sujeitos ativos produtores e propagadores da pornografia infantil, que se valem de tais conteúdos para obter proveito econômico.

2.5. A figura do estupro no âmbito digital

Tal conduta, prevista nos arts. 213 e 217-A (se tratando de vulnerável), se materializa no âmbito virtual comumente através da extorsão e da chantagem, onde o agente exige que a vítima disponibilize imagens e vídeos ou que se exponha em tempo real, com o objetivo de satisfazer a sua lascívia, que por sua vez ameaça a vítima de tal modo que não há outra escolha a não ser ceder o conteúdo requisitado.

Não raro vemos condenações nesse sentido, sobretudo se tratando de crianças e adolescentes, entretanto, cabem algumas ponderações no tocante a aplicabilidade desses tipos penais pré-existentes.

Os Tribunais Superiores em seus entendimentos acerca da temática, consoante a doutrina, descartam a necessidade da conjunção carnal para a caracterização do estupro de vulnerável.

Alem disso, em respeito ao princípio da especialidade, havendo qualquer tipo de violencia ou grave ameaça, não se aplica a desclassificação para o tipo penal da importunação sexual, que compreende também a ocorrência de atos libidinosos, o que em tese permitiria uma aplicação extensiva do dispositivo referente ao estupro.

Entretanto, no âmbito virtual, não constatando a ocorrência de violência, sobretudo nos casos em que a vítima é impúbere, fase na qual comportam uma

suscetibilidade maior as influências externas, há possibilidade de desclassificação para o art. 215-A. E nessa toada, recentemente o TJSP[5], em contraposição a corrente majoritária, reconheceu a aplicabilidade do referido artigo quando não houver conjunção carnal, em um caso de molestação. Fato é que o referido precedente impossibilitaria a adequação do art. 217-A a situações ocorridas na internet

.

3. Aspectos técnicos

A internet consiste em um sistema que interliga a rede mundial de dispositivos móveis, visando o compartilhamento de informações, utilizando sistemas de buscas por meio da chamada "*Web"*, uma rede vasta responsável por armazenar dados e endereçar websites possibilitando a busca e o rastreamento de informações. A web por sua vez constitui um espaço amplo, dividido em camadas que inclusive são intangíveis pelo sistema usual de buscas, como a tão conhecida "*Deep Web"* e *"Dark Web"* além de suas subdivisões.

A camada corriqueiramente acessada pelos internautas, é denominada como Surface Web, onde as URLS são transformadas em números (DNS), formando o "*Internet Protocol"*, responsável pelo percurso dos dados até as páginas desejadas, viabilizando o rastreamento e a obtenção de dados em uma eventual investigação.

No que diz respeito a "*Darknet"*, esta é acessada por um navegador específico, o TOR, que é capaz de assegurar o anonimato dos acessantes, impossibilitando a localização e o rastreio de páginas e usuários por meio da criptografia, baseada em quatro pilares:

> 1- Confidencialidade: apenas o destinatário deverá ter acesso a chave que decifra a mensagem encriptada; 2- Integridade: o destinatário deverá ter a capacidade de saber se a mensagem sofreu alterações durante a transmissão; 3- Autenticidade: o destinatário deverá conseguir identificar o emissor da mensagem; 4- Irretratabilidade: o emissor não poderá conseguir negar o autor da mensagem (emissor). (DUARTE e MEALHA, 2016, p. 12)

Com a criptografia de ponta utilizada sobretudo na "*Dark Web"* (camada abaixo da "*Deep Web"*), os criminosos se eximem de qualquer responsabilização. Usualmente, mesmo sendo usada para fins legítimos, visto que possui um banco de dados acadêmico e científico vasto, a "*Darknet"* é palco de crimes como a venda de órgãos, contratações de assassinos de aluguel e um amplo consumo da pornografia infantil.

[5] https://www.conjur.com.br/2020-nov-02/estupro-vulneravel-ocorre-quando-conjuncao-carnal-tj-sp

4. Evolução do Direito Digital

A internet ganha força na década de 1970 nos EUA durante o contexto da guerra fria, onde houve a necessidade de interligar informações e dados entre os centros de pesquisa militares e rapidamente, foi adaptada de modo a proporcionar comunicabilidade entre órgãos estatais, centros de pesquisa e laboratórios por meio da leitura de documentos codificados.

Entretanto, o surgimento da criminalidade virtual se torna aparente no mesmo período, devido a gradativa substituição dos meios convencionais de transmissão e armazenamento de informações sigilosas por parte dos governos, dando azo as primeiras condutas criminosas na internet, a espionagem e a invasão de dispositivos. Só em 1976 a comunidade internacional começou a se mobilizar a fim de discutir possíveis caminhos para a compreensão desse fenômeno na Conferência de Aspectos Criminológicos do Crime Eletrônico em Estrasburgo, na França.

Estudiosos sobre o tema estimam que a primeira conduta de "*hacking"* ocorreu em 1978, na Universidade de Oxford, onde um aluno invadiu a rede de computadores local e copiou um banco de provas, porém, até o momento não havia nenhum dispositivo legal que tratasse da temática (DAMÁSIO, 2016, p.20). Pouco tempo depois, a disseminação de vírus, veiculação da pornografia infantil e a invasão de sistemas, sobretudo pelos denominados "*hacktivists"* ganham força pelo mundo, e é diante dessa problemática que surge a primeira Lei de Fraudes e Abuso de Computadores nos EUA tutelando condutas criminosas em âmbito federal em 1986, passando por reiteradas alterações, incluindo a criminalização da distribuição de links maliciosos, ataques a sistemas, tráfego de senhas, retirada de informações privadas e por fim, incluiu as ofensas civis e ameaças.

No Brasil, verifica-se que o crime de ameaça teve seu marco inicial registrado em 1997, quando uma jornalista passou a receber diversos "*e-mails"*ofensivos à sua integridade moral e física. Na época, não havia qualquer previsão legal específica, porém no ano seguinte, no HC 76.689/PB, diante de um caso envolvendo a divulgação de material pornográfico infantil, o STF compreendeu a respeito da tipicidade que:

> Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para

> tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. (HC 76.689/PB, STF, 1a. Turma, 22/09/98, Min. Sepúlveda Pertence)

A despeito da contemporaneidade do tema, é certo que tipos penais pré-existentes já contemplam boa parte dos delitos informáticos, não sendo necessário a recriação desses dispositivos, assim, a atividade legislativa deve se debruçar a novas situações fáticas que ocorrem em decorrência do avanço tecnológico, criando tipificações específicas com a devida atenção a descrições elementares exageradamente extensivas.

5. Legislação brasileira

5.1. Lei 12.735/2012

A Lei 12.735/2012 conhecida como "Lei Azeredo", não trouxe nenhuma novidade no quesito incriminação, porém, modificou o inciso II do § 3º do Art. 20 da Lei 7.716/89, que regula os crimes raciais, possibilitando que as transmissões e publicações de símbolos, emblemas e propagandas de cunho nazista, sejam cessadas cautelarmente antes mesmo da abertura do inquérito policial, após uma análise prévia do conteúdo publicado.

Outra novidade relevante, é o Art. 4º da referida lei, que prevê a criação de órgãos da polícia judiciária especializados no combate de ações delituosas na rede de computadores, com o intuito de garantir maior celeridade dos procedimentos investigativos. No que pese a efetividade do Art. 4º, é notável que poucas Delegacias e departamentos especializados foram criados desde então, além disso, nada se fez para formar um corpo investigativo técnico e capacitado para dar a devida condução as investigações.

5.2. Lei "Carolina Dieckmann"

Após um episódio de vazamentos de fotos íntimas da atriz Carolina Dieckmann por meio de uma invasão ao seu computador, debates sobre a necessidade de se criminalizar condutas como o "*hacking"* e a disseminação de vírus foram suscitados, e nesse contexto, a fim de coibir condutas até então atípicas, surge a Lei 12.737/2012.

A principal novidade trazida pela lei, foi a inserção do Art. 154-A do CP:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

O artigo em análise passou a prever duas condutas, a primeira delas é a invasão de dispositivo informático com a finalidade exclusiva de obter, adulterar ou destruir o conteúdo encontrado. A especificidade da conduta supracitada acaba por deixar de contemplar a hipótese de acesso, ainda que indevido, a dispositivo alheio, visto que o verbo "invadir" pressupõe a existência de um Software de segurança, uma senha ou até mesmo um obstáculo físico no caso de dispositivos de armazenamento externo, sendo o mero acesso uma figura atípica.

Partindo desta premissa, surgem alguns questionamentos acerca do que pode ser considerado um dado ou uma informação, já que o texto legal não traz uma conceituação precisa. Na Tecnologia da informação, dado e informação possuem concepções distintas, enquanto o dado representa fatos ou conceitos ainda descontextualizados, a informação é o elo responsável por reunir um conjunto de dados e processá-los de modo a formar um significado. Contudo, pouco importa, em termos de aplicação da norma penal sobre a conduta, o conteúdo dos dados ou informações encontrados após a invasão, pois é nítido que o texto legal não estabelece parâmetros valorativos de quais espécies de dados ou informações estão sobre a égide da lei penal.

O legislador pretendeu punir também no § 1º, com pena correlata, aquele que produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de oportunizar a invasão do dispositivo, o que se dá através disseminação de *trojans* e *keyloggers*. Nos parágrafos subsequentes, a lei trata das majorações da pena caso a infração resulte no prejuízo econômico, na obtenção de conteúdos privados e sigilosos e quando o crime for cometido contra os representantes da esfera pública.

O tipo penal exige necessariamente o elemento doloso para a ambas as figuras, ou seja, a vontade livre e consciente de praticar os verbos elencados para que a conduta seja típica, independente do resultado. O dolo e a culpabilidade do agente só poderão ser apurados adequadamente mediante perícia técnica, a fim de atestar a relevância e conteúdo das informações alvo da invasão e como se deu no caso concreto, ademais, se trata de um crime informático que deixa vestígios, sendo obrigatório a realização de exame pericial sob pena de nulidade nos termos do Art. 158 do CPP. Vale salientar

também, que por vezes a invasão precede a prática de outros crimes, como uma atividade meio. A depender do caso concreto, poderá ser aplicado o princípio da consunção, assim o crime mais grave absorverá a conduta de menor potencial ofensivo que tenha sido cometida como um ato preparatório necessário a consecução do objetivo final. Nesse diapasão, se tratando de uma infração com pena cominada em até dois anos, a competência será do Juizado Especial Criminal, porém, havendo concurso de crimes, o processo se destinará ao juízo comum, procedendo somente com a representação do ofendido, salvo se o crime for cometido contra a administração pública de qualquer dos entes da federação ou contra empresas concessionárias de serviços públicos.

5.3. Marco Civil da Internet

Os objetivos centrais da Lei 12.965/2012 são o estabelecimento de normas e princípios que deverão nortear as práticas de bom uso da internet. Os principais pilares que regem sua constituição, estão pautados na liberdade de expressão e a privacidade dos usuários, em face dos inúmeros episódios envolvendo vazamento de dados pelas empresas e espionagem. Por ser um tanto quanto abrangente e genérica, a referida lei influi em diversas áreas do Direito brasileiro, e sua principal repercussão na seara criminal é justamente em relação a obtenção de registros de acesso junto aos provedores.

Em seu Art. 15, estabelece que qualquer registro referente ao conteúdo dos acessos, bem como dados relativos aos usuários, deverão ser obtidos através de uma ordem judicial, mesmo se tratando de requisição dos órgãos investigativos, fazendo uma ressalva em relação aos dados cadastrais (nome, filiação, endereço). O dispositivo legal também estabelece que esses dados e informações devem ser mantidos sob a posse do órgão investigativo pelo prazo máximo de 6 meses, podendo ser prorrogado pelo mesmo tempo com a devida determinação judicial. O estabelecimento de um prazo figura entre uma garantia essencial de que o conteúdo disponibilizado não seja desvirtuado posteriormente de suas reais funções em uma investigação, entretanto, representa ao mesmo tempo um impasse as autoridades policiais, tendo em vista a morosidade das etapas investigativas.

5.4. Lei Geral de Proteção de Dados

Inspirada na GDPR europeia, a LGPD traz consigo a mesma proposta: estabelecer normas e critérios relativos à governança de dados pelas empresas. A nova lei, não traz qualquer tipo de previsão no campo penal e processual penal, entretanto, em seu Art. 42, sedimenta a responsabilidade dos Administradores de empresas em eventuais incidentes, respondendo tanto pelas suas ações como omissões. A bem da verdade, essa previsão é relativa a esfera cível, mas estima-se que poderá se estender ao âmbito criminal e administrativo, tendo em vista o atual tratamento dado aos crimes empresariais. Além disso, comporta nesse bojo de responsabilização, àqueles responsáveis pelo cuidado dos dados como gestores e operadores.

Aqui se tem evidentemente a aplicação da teoria do domínio do fato na responsabilização dos agentes, no que tange a responsabilização dos atores, onde reside inúmeras controvérsias, pois há a pressuposição de que os administradores sempre terão conhecimento da prática delitiva ocorrida no interior da empresa, o que destoa da realidade de muitos estabelecimentos empresariais. Se trataria de responsabilização objetiva, o que em tese não encontra respaldo na sistemática de responsabilização penal brasileira.

6. Investigação criminal e cadeia de custódia da prova digital

Pode-se afirmar, que as provas nada mais são do que a reconstrução de um fato histórico, a fim de se imputar a culpabilidade ou a inocência de um indivíduo. A construção probatória se consubstancia na tentativa de apurar um conjunto de fatos pretéritos, muitas vezes modificados, na tentativa de dissimular elementos de autoria e materialidade.

A criminalidade informática de maior relevância para o direito penal, é um fenômeno praticado com uma racionalidade maior do que os demais delitos, nesse contexto, os possíveis vestígios ocasionados pela prática delitiva, até mesmo quando não houver tecnicidade por parte do criminoso, sofreram a tentativa de ocultação.

Os crimes digitais, sejam eles próprios, impróprios ou mistos, podem ser provados com qualquer tipo de prova, inclusive a testemunhal. Entretanto, aqui chama se atenção para a prova pericial, haja vista que esta é fundamental e obrigatória nos termos do art. 158 do CPP nos crimes que deixam vestígios.

Se tratando de uma modalidade de delito complexa, a perícia técnica realizada por peritos especializados, é um fator preponderante na colheita de elementos que comprovem a autoria e a materialidade principalmente. Em uma situação de flagrante

delito ou no curso da busca e apreensão, os peritos, especialistas ou não, devem cercar o local de modo a impedir que qualquer elemento alheio a cena do crime altere a propriedade das provas em potencial. Tal procedimento, previsto no art. 6º, I, do CPP, não difere das demais modalidades de delitos.

Após o cerceamento do local, resta a coleta adequada dos dispositivos ou da extração do conteúdo probatório das unidades de armazenamento, este procedimento poderá ser realizado somente pelo perito especialista.

O método empregado para extração de tal conteúdo, influi diretamente na prestabilidade da prova digital. Se tratando de dispositivos de armazenamento, estes são extremamente voláteis, tanto pela fragilidade material dos componentes como pela composição dos dados, que podem ser facilmente modificados durante o trato da prova pela autoridade investigativa, pois são compostos por sequências numéricas e qualquer modificação acidental, pode acarretar na imprestabilidade da prova (VIANNA, p. 77).

Tal problemática só será dirimida com a adoção de procedimentos específicos para a obtenção de provas digitais. Nesse sentido, mesmo se tratando de disposição genérica, desconsiderando as nuances dos crimes digitais, a previsão da cadeia de custódia da prova, novidade trazida com o advento da Lei 13.964/2019, deve impor maior rigor na construção probatória.

Compreende-se que com a alteração no art. 158 do CPP, diante da inobservância do procedimento previsto no referido artigo, a prova passa a ser considerada imprestável para figurar como um elemento de cognição na fase processual. Conforme ensina Renato Brasileiro Lima (2020, p. 253):

> A cadeia de custódia visa assegurar a idoneidade dos objetos e bens apreendidos, de modo a evitar qualquer tipo de dúvida quanto à sua origem e caminho percorrido durante a investigação criminal e o subsequente processo criminal. Em outras palavras, se a acusação pretende apresentar evidências físicas em juízo (v.g., arma do crime), deve estar disposta a mostrar que o objeto apresentado é o mesmo que foi apreendido na data dos fatos.

Um exemplo que ilustra a aplicabilidade desta nova disposição, é no procedimento que se compreende como ideal na extração de informações de dispositivos móveis e de armazenamento, que comportam a mesma técnica.

Em uma situação hipotética envolvendo o crime de transmissão de material pornográfico infantil, primordialmente deverá haver a *(1) preservação do local* em que ocorreu a prática delitiva, bem como todo e qualquer que tenha relação direta, *(2)*

colheita do material pelo corpo de polícia ou perícia, de modo a acondicioná-lo da maneira correta para que o dispositivo não danifique, e por fim, a *(3) extração* do conteúdo através de cópia dos dados armazenados ou se tratando de conteúdo presente em páginas (websites) mediante requisição aos provedores a fim de ter acesso ao material de forma integral, e em alguns casos, pelo rastreamento do Internet Protocol (IP).

No que tange a potenciais provas ou vestígios, o art. 158-B ainda prevê disposições relativas a prestabilidade dos indícios, e para que haja uma sequência lógica que conecte o conteúdo apreendido ao autor, adequada às condições gerais de admissibilidade da prova, o artigo compreende desde o reconhecimento do elemento probatório e seu isolamento, até seu armazenamento adequado e posteriormente ao seu descarte. Importante destacar que tais elementos probatórios obtidos em sede de inquérito policial, deverão respeitar a cadeia de custódia a fim de manter sua integridade, visto que esta não se resume apenas na satisfação da pretensão acusatória.

Portanto, conclui-se que a quebra da cadeia de custódia representaria também a quebra da confiabilidade da prova, configurando sua ilicitude. Não obstante, através do HC 160.662, a 6ª Câmara Criminal do STJ reconheceu que a ausência de detalhamento no procedimento de obtenção de prova, sobretudo na interceptação telefônica, deflagra uma violação ao contraditório e a ampla defesa, pois a obscuridade poderá estar imbuída de ilegalidades, e portanto, tais provas deverão ser desentranhadas do processo.

Conclusão

Por todo exposto, foi possível constatar que mera tipificação de condutas na seara não surte efeitos concretos, portanto deve ser feita pontualmente abarcando condutas que realmente representam um maior potencial lesivo. A inclusão de algumas condutas específicas na legislação penal, tem o condão adequar a legislação a nova realidade que essa parcela da criminalidade se insere.

Outrora, a questão controvertida suscitada precede a ausência de dispositivos penais específicos, que pouco ou nada influem na redução dessa modalidade de criminalidade, ademais, a tutela penal de tipos específicos que já se assemelham a condutas pré existentes, representaria um inchaço legislativo gigantesco, além de desvirtuar as reais finalidades do direito penal.

Salienta-se que a primeira lei incriminadora criada, é anterior a quaisquer tentativas de se estabelecer normas de uso na internet e de segurança de dados, sendo

que sua aplicabilidade é praticamente inócua tendo em vista que os tipos penais já existentes acabam por suprimir a responsabilização pelo art. 154-A. Assim, conclui-se que, questões relativas à segurança e proteção de dados devem ser aperfeiçoadas de imediato, bem como os padrões de uso da internet, e em última análise, quando conveniente, aplicar a tutela penal.

Referências bibliográficas

BITTENCOURT, Cezar Roberto. **Tratado de Direito Penal.v.1**. São Paulo: Editora Saraiva, 2018.

Brasil é o segundo país no mundo com maior número de crimes cibernéticos. **UOL**, 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em jul/2020.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Crimes cibernéticos** / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF,

CAPEZ, Fernando **Curso de direito penal**, volume 2, parte especial dos crimes contra a pessoa a dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212) / Fernando Capez. — 12. ed. — São Paulo : Saraiva, 2012.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva, 2011.

DUARTE, David. **Introdução a "Deep Web" -** David Duarte; Tiago Mealha - Monte de Caparica, Portugal: IET/CICS.NOVA, 2016. ISBN: 1646-8929

Estupro de vulnerável só ocorre quando há conjunção carnal, diz TJ-SP. **Conjur**, 2020. Disponível em: https://www.conjur.com.br/2020-nov-02/estupro-vulneravel-ocorre-quando-conjuncao-carnal-tj-sp. Acesso em nov/2020.

JESUS, Damásio de. **Manual de crimes informáticos**. Damásio de Jesus, José Antonio Milagre. – São Paulo: Saraiva, 2016.

LIMA, Renato Brasileiro de. **Pacote Anticrime: Comentários à Lei N. 13.964/19 - Artigo por Artigo** / Renato Brasileiro de Lima - Salvador: Editora JusPodivm, 2020.

592 p.

MARQUES, Airton. Tráfico humano, pessoas viram produtos pela web. **Circuito Mato Grosso**, 2015. Disponível em: http://circuitomt.com.br/editorias/cidades/73841-trafico-humano-pessoas-viram-produtos-pela-web.html. Acesso em ago/2020.

VIANNA, Túlio. **Crimes informáticos** / Túlio Vianna ; Felipe Machado – Belo Horizonte : Fórum, 2013.