



**DOS CRIMES VIRTUAIS, DA OBTENÇÃO DAS PROVAS E AS TENDÊNCIAS  
JURÍDICAS DECORRENTES DA EVOLUÇÃO TECNOLÓGICA.**

**OF VIRTUAL CRIMES, OF OBTAINING EVIDENCE AND LEGAL TRENDS  
ARISING OUT OF THE TECHNOLOGICAL EVOLUTION.**

**\*SAMARA SILVA PINTO**

**RESUMO:** O presente trabalho aborda a obtenção de provas no meio cibernético na esfera processual penal e da validade dessas provas no ordenamento jurídico brasileiro, ou seja, quais são os meios de provas que podemos obter por meios das redes sociais e demais acessos virtuais na visão do Processo Penal Brasileiro, além das tendências de inovações para acompanhar o avanço tecnológico.

**Palavras-chave:** Direito Processual Penal. Provas no Processo Penal. Crimes Cibernéticos. Obtenção de provas no processo penal. Inovações jurídicas nos crimes virtuais.

**ABSTRACT:** The present work deals with the obtaining of cybernetic evidence in the criminal procedural sphere and the validity of these tests in the Brazilian legal system, that is, what are the means of evidence that can be obtained by means of social networks and other virtual accesses in the process view Criminal law, in addition to the trends of innovations to accompany the technological.

**Keywords: Criminal Procedural Law. Evidence in Criminal Procedure. Cyber Crimes. Taking of evidence in criminal proceedings. Legal innovations in virtual crimes.**

## **1 - Introdução**

A evolução tecnológica influenciou e continua influenciando em diversos fatores da comunicação na sociedade, como por exemplo, o surgimento da *internet* que viabiliza a utilização das redes sociais como forma de entretenimento, informação e comunicação. Essa evolução tecnológica, que atinge principalmente o mundo da comunicação e informação nos dias atuais, já está disseminada mundialmente.

Nas últimas décadas, a utilização da *internet* não para de crescer, tornando-se o principal e mais utilizado meio de comunicação. Por meio dela, há interligação de comunicação entre pessoas, comunidades, acesso a diversas informações atuais e em tempo real, acesso rápido e fácil de comunicação e cada vez mais barato.

Mas, a utilização da *internet* não só trouxe pontos positivos para a sociedade, como também deixou de ser apenas uma forma de entretenimento e comunicação positiva, tornando-se um instrumento de práticas delituosas, caracterizando uma nova e ameaçadora forma de práticas ilícitas mediante meios de comunicação, dentre elas as redes sociais, onde as pessoas encontram-se mais conectadas.

Com a popularização da *internet* em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a *internet* é um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito; os crimes virtuais.<sup>1</sup>

---

<sup>1</sup> PINHEIRO, Reginaldo Cesar. Os crimes virtuais na esfera jurídica brasileira. Boletim IBCCrim, ano 8, n. 101, p. 18

Inúmeros são os benefícios trazidos com o surgimento da *internet*, porém esse avanço está correndo ao lado da utilização ilimitada e indiscriminada desse meio virtual, favorecendo os acontecimentos de crimes virtuais e assim dando alerta aos olhos da jurisdição na esfera Processual Penal.

Com todo esse mecanismo da tecnologia, a rede social insere-se efetivamente nas diversas áreas dentro do mundo social, político e jurídico, e, mencionado no aspecto jurídico, pode-se dizer que as redes sociais estão sendo de fundamental importância para a colaboração e obtenção de provas, sejam elas por meio do *facebook*, *instagram*, ou outros meios, tanto no aspecto de provas nos delitos ocorridos ou não pelo meio virtual.

Nesse mesmo contexto, verifica-se que o Estado como protetor dos direitos deve rever a questão jurídica das provas e dos meios de sua obtenção no Processo Penal Brasileiro para se adequar às inovações científicas e tecnológicas, garantindo um processo penal com resultados que cumpram as garantias constitucionais.

Sendo assim, a sociedade vem se adaptando e se moldando ao uso das redes sociais em vários aspectos, comunicação, trabalho profissional, relacionamentos, estudos, abrindo fronteiras ilimitadas de conhecimento sobre tudo que acontece no mundo, tendo em suas “mãos” um instrumento não só de acesso ao saber, mas também uma maior facilidade em agir no anonimato.

Assim, faz-se importante que o Poder Judiciário também se iguale a estas evoluções, adaptações e moldes sobre a tecnologia de informação, como forma de conhecimento, prevenção, vigilância, intervenção junto ao aprimoramento da legislação que concerne sobre o assunto, valendo-se dos benefícios gerados em prol de uma sociedade civilizada.

Contudo, nesse sentido o autor Leonardi traz seu entendimento sobre o tema. “No entanto se desejarmos que a nova fronteira digital se torne realmente civilizada, precisamos compreender como o sistema jurídico deve ser aplicado a esse novo domínio da interação humana”<sup>2</sup>.

Nota-se que para o Sistema Jurídico há vários passos a serem estabelecidos para investigação dos crimes virtuais, como por exemplo, a

---

<sup>2</sup> LEONARDI, Marcel. Tutela e Privacidade na Internet. São Paulo: Saraiva, 2012. p.29

identificação dos autores por meio de análise de tráfego de dados que chegará ao endereço do IP (*Internet Protocol*)<sup>3</sup> do computador.

As provas no Processo Penal Brasileiro são de fundamental importância para a convicção do juiz, ou seja, elas são as peças chave para sua deliberação.

Portanto, se o mundo se encontra influenciado pelos efeitos virtuais, as provas obtidas por meio virtual terão de ter a mesma eficiência como qualquer outro tipo de prova vigente na nossa legislação.

O avanço tecnológico inseriu as redes sociais e outros meios virtuais como pilares de relevantes aspectos no mundo atual. Na atualidade, são raras as pessoas que não se conectam a internet. Como menciona o autor Marcelo Crespo: “Essa evolução não trouxe somente benefícios para a sociedade, mas também permitiu que a criminalidade se apresentasse sob novas formas até então desconhecidas”<sup>4</sup>

Assim, o entendimento de Leonardi: “Quer gostemos ou não, novas tecnologias de informação continuarão a proliferar, oferecendo mais conveniências e mais riscos para a vida humana”<sup>5</sup>.

Portanto, as redes sociais, como um novo meio de obtenção de provas, emparelham as novas possibilidades probatórias possíveis através do desenvolvimento científico e tecnológico. Esclarecendo que a evolução do Processo Penal Brasileiro é urgente para tornar-se mais ágil, justo e eficiente para apuração criminal, com a utilização de provas mais confiáveis e modernas.

Nessa perspectiva, a obtenção de provas por meio de rede social seria um meio de prova cabal advindo do avanço tecnológico, ou seja, os crimes estão acontecendo virtualmente, então as provas concretas, terão de vir também pelo meio virtual, como por exemplo, captura de telas de conversa, fotos, vídeos ou outros documentos correlacionados, não significando que seja regra, e aceitável a prova que advém apenas do meio virtual:

Deste modo, para que essas provas virtuais sejam colhidas de forma

---

<sup>3</sup> Para que a comunicação entre os computadores na internet se estabeleça é necessário que cada conexão de computador à rede esteja identificada. O responsável por essa identificação é o protocolo IP (*Internet Protocol*).

<sup>4</sup> CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Editora Saraiva, 2011. p. 27.

<sup>5</sup> LEONARDI, Marcel. Tutela e Privacidade na Internet. São Paulo: Saraiva, 2012. p.38

integral, deve-se de ter materiais suficientes para a conservação e defesa das provas a fim de não serem modificadas no trâmite da investigação. Assim sendo, faz-se necessários alguns questionamentos, são eles: Como utilizar meios adequados (equipamentos de alta tecnologia ou programas para identificar as pessoas que utilizam redes sociais e sítios de relacionamento) para o colhimento das provas, como habilitar, capacitar profissionais especializados para o assunto, como inserir na legislação forma eficaz para combater o crescente número de crimes virtuais.

A Lei 12.965/2014 criada recentemente, que se refere ao marco civil da *internet*, prevê como regra geral que a quebra de sigilo de dados e do provedor de internet seja submetida ao controle jurisdicional e ao procedimento de requisição judicial, isso significa que os provedores de aplicações de *internet* somente são obrigados a fornecer tais dados mediante ordem judicial que apreciem o preenchimento dos requisitos legais para a quebra de sigilo.

A lei em questão, em regra geral, é principiológica, não mencionando punições mais rígidas quanto ao cometimento de crimes e nem soluções para obtenção de provas por meio virtual.

Assim sendo, essa lei não traz esclarecimentos, muito menos soluções eficazes para a coleta de provas nos crimes virtuais, dificultando a obtenção das provas. Acredita-se que não se identifica um autor de crime virtual apenas pelo IP, mas sim pelos conteúdos inseridos em redes sociais pelo suposto infrator. Esses conteúdos como forma de provas no processo penal precisam ser analisados de forma célere, logo, todo o trâmite de solicitação de autorização judicial prejudicaria o alcance de tais provas.

A necessidade de autorização judicial, presente na lei, existe para não haver embate com o direito de intimidade e de privacidade do indivíduo, contrapondo a questão posta sobre os crimes virtuais que é a de interesse coletivo, interesse da sociedade, o que prevaleceriam sobre os direitos individuais verificado neste contexto.

## **2 - Dos crimes cibernéticos**

O termo *cibercrime* ou *cybercrime* em inglês apareceu em uma reunião de um subgrupo do G-08 (grupo composto pelos sete países mais ricos do

mundo). Essa reunião abordava justamente as maneiras e os métodos utilizados para combater as práticas ilícitas por meio da *internet*.<sup>6</sup>

Para definir o que seja o crime virtual trazemos conceitos de alguns estudiosos no assunto.

Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.<sup>7</sup>

O crime cibernético é qualquer conduta ilegal realizada no meio jurídico, ou seja, são condutas típicas, antijurídicas e culpáveis, praticadas utilizando sistemas de informática ou contra eles<sup>8</sup>.

Os crimes cibernéticos referem-se a todos os delitos cometidos utilizando computadores ou *internet*, por meio de uma rede pública, privada ou doméstica. Os objetivos desses crimes são diversos e variam de acordo com os interesses de cada infrator. Além disso, as formas de cometer também são diversas e podem atingir apenas um usuário, vários usuários, ou a população em geral.

Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como *cibercrime*. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital.<sup>9</sup>

---

<sup>6</sup> Disponível em: <<https://cibercrimes.wordpress.com/2011/03/24/mas-afinal-o-que-ecibercrime/>> Acesso em: 15 maio de 2017.

<sup>7</sup> RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. JusNavigandi, Teresina, a. 6, n. 58, ago. 2002

<sup>8</sup> MENDES, Maria Eugencia Gonçalves. VIEIRA, Natália Borges. Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica. 2012. Disponível em: <<http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridicobrasileiro-e-a-necessidade-de-legislacao-especifica-2>>. Acesso em: 12 de fev. 2017. <sup>9</sup> CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. 1. ed. Rio de Janeiro: Brasport, 2014, pg. 03

Os levantamentos<sup>9</sup> têm mostrado que o Brasil ocupa lugar de destaque no cenário global de *ciber Crimes*. Em 2016, 42,4 milhões de brasileiros foram vítimas de crimes virtuais, os ataques virtuais são cada vez mais frequentes, sofisticados, instáveis e difíceis de combater, havendo necessidade de aprimoramento nos mecanismos, investimentos e estudos para combater esses crimes em seus diversos alvos.

Já em 2017, estudo realizado pela empresa de segurança Palo Alto Networks afirmou que o Brasil é o segundo país da América Latina que mais sofre com o crime cibernético, com 31% das atividades maliciosas ocorrendo em seu território, enquanto que o México é responsável pela liderança da lista com o total de 54%<sup>10</sup>.

De acordo com o autor Sandro D'Amaro Nogueira, "O rol dos crimes cometidos por meio eletrônico é extenso. Dentre eles: os crimes contra honra – injúria, calúnia e difamação os furtos, pedofilia - e etc."<sup>11</sup>.

No limiar dessa evolução tecnológica é possível constatar que, atualmente, o Código Penal de 1940 tende a lidar com situações criminosas que vão além do plano físico. Hoje, o agente delituoso não necessita ir às ruas para cometer determinados ilícitos como furto, racismo, crimes contra a honra, tráfico de drogas, dentre outros.

É por diversos motivos a propagação crescente do número de crimes virtuais na *internet*. Os criminosos que acessam a rede mundial de computadores se utilizam de técnicas para ocultar sua verdadeira identidade e conduta, podendo assim, assumir qualquer identidade que não a sua.

Ou seja, a prática de crimes virtuais é muito comum justamente pela ilusão de que o computador não poderá revelar a identidade dos envolvidos, pela desinibição causada pelo anonimato, além disso, muitos acreditam que a punição ainda é muito branda, ou mesmo inexistente, fazendo com que os números de crimes virtuais cresçam a cada ano.

Como observa o Professor Renato Opice Blum do curso de Direito Digital da Insper, "há um aumento proporcional (ao crescimento da quantidade de

---

<sup>9</sup> Disponível em <<http://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam42-milhoes-de-brasileiros,70001644185>> Acesso em: 17 maio de 2017.

<sup>10</sup> Disponível em <<http://tecnologia.ig.com.br/2017-03-31/crime-cibernetico.html>> Acesso em: 20 maio de 2017

<sup>11</sup> NOGUEIRA, Sandro D'Amaro. *Crimes de Informática*. Leme: BH Editora, 2009, p. 36.

usuários conectados) no número desses crimes. E, do ponto de vista legal, há um aumento no número de processos e de decisões judiciais.”<sup>12</sup>

E os problemas dos chamados *ciber Crimes* vão além da velocidade com que os crimes se multiplicam, pois, há também a dificuldade de identificação de autoria e obtenção de prova desses crimes.

Na visão de Daniel Burg, a internet facilita a impunidade uma vez que a investigação é mais complicada e muitas vezes quando é identificado o autor, já ocorreu a prescrição. “o crime pode ser cometido por alguém que está em outro país, com leis completamente diferentes”<sup>13</sup>.

Segundo Maciel Colli,: “o anonimato *on-line* fornece uma liberdade inatingível no mundo real”<sup>14</sup>

O anonimato traz uma dificuldade para identificação da autoria de um crime virtual, mas a identificação do IP do computador é de fácil acesso.

Ao se considerar a possibilidade de identificação do computador, esse anonimato *on-line* torna-se relativo. A princípio, o anonimato *on-line* é apenas aparente, porque o mais anônimo dos sujeitos poderá ter o seu computador identificado ao se conectar à rede mundial de computadores, através do endereço IP atribuído ao computador quando da conexão.<sup>15</sup>

Com o grande número de usuários nas redes sociais, muitas interações como postagem, comentários, vídeos, áudios e outros aqui não mencionados, acabam sendo considerados crimes. Muitas pessoas acabam utilizando as redes sociais para cometer algum tipo de delito. Abaixo segue um rol de crimes<sup>16</sup> que costumam ser praticados nas redes sociais:

- **Calúnia:** Caluniar alguém, imputando-lhe falsamente fato definido como crime, previsto no artigo 138 do Código Penal Brasileiro.

<sup>12</sup> Disponível em <<https://www.insper.edu.br/noticias/brasil-e-o-5o-do-mundo-em-fraudesdigitais/>> Acesso em: 15 de jun. de 2017.

<sup>13</sup> Disponível em <<http://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialistacrimes-virtuais>> Acesso em: 08 maio de 2017.

<sup>14</sup> COLLI, Maciel. *Ciber Crimes. Limites e perspectivas à investigação policial de crimes cibernéticos*. Curitiba: Juruá Editora, 2010. p. 45

<sup>15</sup> COSTA, Levi Roberto; PEIXOTO, Hélio Pereira. Um método para sistematização do processo investigatório de análise da informação digital Fomentando a cognição na atividade policial. 2011

<sup>16</sup> Disponível <[http://www.planalto.gov.br/ccivil\\_03/leis/L8069.htm](http://www.planalto.gov.br/ccivil_03/leis/L8069.htm)> Acesso em: 19 jun. de 2017



- **Injúria:** Injuriar alguém, ofendendo-lhe a dignidade ou o decoro, previsto no artigo 140 do código penal Brasileiro.
- **Difamação:** Associar uma pessoa a um acontecimento que possa denegrir a sua imagem; Difamar alguém, imputando-lhe fato ofensivo à sua reputação, previsto no artigo 139 do Código Penal Brasileiro.
- **Divulgação de material confidencial:** Revelar segredos de terceiros, bem como materiais íntimos, como fotos e documentos; Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem, previsto no artigo 153 do Código Penal Brasileiro.
- **Ato obsceno:** Disponibilizar algum conteúdo que ofenda a terceiros, como por exemplo, divulgar fotos obscenas em salas de bate papo, fóruns, que não sejam destinados a esses fins; Praticar ato obsceno em lugar público, ou aberto ou exposto ao público, previsto no artigo 233 do Código Penal Brasileiro.
- **Apologia ao crime:** Criar comunidades que ensinem a burlar normas ou mesmo que divulguem atos ilícitos já realizados; Fazer, publicamente, apologia de fato criminoso ou de autor de crime, previsto no artigo 287 do Código Penal Brasileiro.
- **Perfil falso:** Criar uma falsa identidade nas redes sociais; Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem, previsto no artigo 307 do Código Penal Brasileiro.
- **Tráfico de drogas:** Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar, previsto no artigo 33 da Lei nº 11.343/2006.
- **Invasão de dispositivo informático:** 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, que está previsto no artigo 154 –A do código penal, esse artigo foi introduzido recentemente por meio da Lei 12.737/2012, apelidada como Lei Carolina Dieckmann.

Ressalta-se que há um projeto de lei nº 4093/2015 da Câmara dos Deputados, para alterar a redação do artigo 154-A com objetivo de ampliar a abrangência do crime de invasão de dispositivo informático, pois a redação do artigo 154-A não está previsto o alcance do tipo penal para aqueles que invadem, sem autorização, dispositivo informático que não possui mecanismo de segurança.

- **Pedofilia, Estupro de vulnerável e similares:** Troca de informações e imagens de crianças ou adolescentes. Assim, temos no CP os crimes contra a dignidade sexual, possuindo capítulo específico acerca dos crimes sexuais contra vulneráveis: art. 217-A do CP – estupro de vulnerável; art. 218 do CP – mediação de menor de 14 anos para satisfazer a lascívia de outrem; art. 218-A do CP – satisfação da lascívia mediante a presença de menor de 14 anos; 218-B do CP – favorecimento da prostituição ou outra forma de exploração sexual de criança, adolescente ou vulnerável.

O Estatuto da Criança e do Adolescente -ECA também trata de crimes envolvendo a pedofilia:

Art. 240 do ECA – utilização de criança ou adolescente em cena pornográfica ou de sexo explícito;

Art. 241 do ECA – comércio de material pedófilo; art. 241-A do ECA – difusão de pedofilia;

Art. 241-B do ECA – posse de material pornográfico;

Art. 241-C do ECA – simulacro de pedofilia;

Art. 241-D do ECA – aliciamento de menores.

Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão “cena de sexo explícito ou pornográfica” compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou

exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais<sup>17</sup>.

É importante ressaltar que nos crimes de estupro e estupro de vulneráveis por meio virtual é perfeitamente possível de se concretizar, imagine por exemplo, uma pessoa, via *webcam*, mostra a outra pessoa que uma pessoa de sua família está em seu poder e, ameaçando matá-la com uma arma de fogo e apontada para sua cabeça, pede para que tire a roupa (do outro lado da tela) com o intuito de satisfazer sua lascívia (desejo sexual), masturbando-se;

No caso citado houve constrangimento mediante grave ameaça para a prática de um ato libidinoso (diverso da conjunção carnal), impossibilitando a vítima de optar por sua liberdade de pensamento, escolha, vontade e/ou ação. Percebemos, claramente no exemplo citado, que a tipicidade para o crime de estupro se consumou.

Não resta nenhuma margem de dúvidas sobre a quantidade expressiva de crimes executados diariamente por meio da *internet*. Portanto, há dúvidas quanto ao que se fazer quando alguém é acometido por um crime virtual, a quem recorrer, sobre quais provas a serem utilizadas, como obter tais provas, como levar ao conhecimento da Polícia.

Nesse diapasão, o Processo Penal Brasileiro não acompanhou essa evolução dos crimes eletrônicos, no sentido de não haver legislação específica suficiente esclarecendo e dando forma à validade de provas obtidas por meio de redes sociais e nem mesmo existindo uma evolução e aprimoramento de equipes especializadas para identificar e investigar esses crimes.

### **3- As Provas no Processo Penal**

O assunto prova é um dos temas mais importantes da ciência do processo no âmbito jurídico, neste caso no Processo Penal, uma vez que a prova é um dos pressupostos fundamentais para atingir a verdade, sendo o principal meio para convencer o juiz que deverá prolatar sentença mais justa possível e de acordo com que entender ser a verdade dos fatos.

---

<sup>17</sup> Disponível em <[http://www.planalto.gov.br/ccivil\\_03/leis/L8069.htm](http://www.planalto.gov.br/ccivil_03/leis/L8069.htm)> Acesso em: 20 jun. de 2017.

Além da importância das provas no Processo Penal, vale mencionar a importância dos meios de provas admitidos dentro desse processo, ou seja, como podem ser manejados e quais os mecanismos que podem ser utilizados para colher tais provas.

Neste contexto, em busca da verdade do fato, é possível a utilização da *internet* como meio de prova, pois suas páginas (imagens) podem ser impressas, tornando-se assim documentos de prova em processos judiciais.

As provas obtidas conduzem o juiz a formar sua convicção a respeito dos fatos, ou seja, pode-se dizer que os meios de provas é todo o instrumento que se destina a levar ao processo um elemento, uma informação a ser utilizada pelo juiz para formar uma convicção acerca dos fatos alegados pelas partes. Pode ser um fato, alegações, documentos, imagens, algum parecer que auxilie, direta ou indiretamente no desvendar da verdade dos fatos. Preconiza o artigo 232 do Código de Processo Penal: "Consideram-se documentos quaisquer escritos, instrumentos ou papéis públicos ou particulares. Parágrafo único. À fotografia do documento, devidamente autenticada, se dará o mesmo valor do original"<sup>18</sup>

A adequada utilização das provas traz previsões importantes na prática dos atos processuais penais, sendo favorável no auxílio da prestação jurisdicional.

Os meios de prova utilizados referem-se ao modo pelos quais as provas podem ser obtidas, sendo que o rol dos meios de prova apresentado pelo Código de Processo Penal é exemplificativo, permitindo admissão de outros meios além daqueles apresentados pela Lei Penal, desde que seja sempre observada a busca da verdade e da legalidade.

Pode-se mencionar que nos crimes cibernético, alguns meios de provas são mais utilizados pelo ordenamento jurídico brasileiro como, por exemplo, a perícia que pode ser feita nos computadores utilizados pelos supostos autores do crime, neste caso, é mais utilizada quando se identifica o IP do computador, mas não há certeza da autoria, pois terceiros poderiam ter acessado o computador.

---

<sup>18</sup> Disponível em <<http://www.jusbrasil.com.br/topicos/10660113/paragrafo-1-artigo-232-dodecreto-lei-n-3689-de-03-de-outubro-de-1941>>. Acesso em: 30 maio de 2017.

Outros meios de prova seriam a interceptação de correios eletrônicos e a quebra de sigilo de sítios de relacionamento, tais como *Orkut*, *Facebook*, *Instagram*, entre outros. Por esses meios citados, não podemos afirmar que a identificação da autoria do crime seria concretizada, porém a identificação torna-se mais possível.

Meio de prova é todo fato, documento ou alegação que possa servir, direta ou indiretamente, à busca da verdade real dentro do processo. Em outras palavras, é instrumento utilizado pelo juiz para formar a sua convicção acerca dos fatos alegados pelas partes.<sup>19</sup>

O Código adotou o conceito de documento em sentido estrito. No sentido amplo, podemos dizer que:

é toda base materialmente disposta a concentrar e expressar um pensamento, uma idéia ou qualquer manifestação de vontade do ser humano, que sirva para demonstrar e provar um fato ou acontecimento juridicamente relevante” De acordo com essa interpretação, então, são considerados documentos: vídeos, fotos, CDs etc.<sup>20</sup>

Portanto, deverá integrar o conceito de documento, o correio eletrônico, os documentos produzidos eletronicamente, páginas de redes sociais, como *Orkut*, *Facebook*, *instagram*, vídeos, conversas de *whatsapp*, *printscrenn de telas de conversar ou de fotos, dentre outros aqui não mencionados, pois estes apresentam documentos escritos, áudios, imagens, informações, caracterizando um meio de ambiente virtual.*

### 3.1- Das Provas Virtuais/ Eletrônicas

---

<sup>19</sup> BONFIM, Edilson Mougnot. Curso de processo penal. 3.ed. rev., atual e ampl. São Paulo: Saraiva, 2008. Pg. 307-308

<sup>20</sup> NUCCI, Guilherme de Souza. Manual de Processo Penal e Execução Penal. 6ª Ed., rev., at. e ampl. RT.2010. pag.497

A utilização de documentos eletrônicos para otimizar a mera comunicação entre órgãos públicos ou firmar contratos, tende a ter menor resistência quanto a sua veracidade, todavia, no Processo Penal parece haver uma resistência um pouco maior quanto à utilização dos documentos eletrônicos como meio de prova, que se deve ao receio de gerar condenações baseadas em provas cuja autenticidade e veridicidade são aferidas a partir de técnicas novas como a criptografia<sup>22</sup>.

As redes sociais estão em destaque no contexto de provas eletrônicas, sendo uma prova documental, qualquer objeto ou escrito que possa ser levado ao conhecimento do Magistrado, e que possa ser utilizado como prova, assim como mensagens de texto, correios eletrônicos, fotos e vídeos, que podem ser analisados como forma de provas, como *prints* ou capturas de telas, que funcionam como uma cópia autenticada das postagens, fotos, ligações, conversas que podem servir para comprovar crimes como ameaça, calúnia, difamação, injúria racial, entre outros.

No Brasil já existem julgados de Tribunais<sup>23</sup> que consideram legítimas as provas originadas das redes sociais, mesmo ainda não existindo uma lei específica que discipline sua utilização como provas em processos judiciais. Não há um manual específico quanto ao procedimento eletrônico, em relação ao caminho a que percorrem os documentos eletrônicos, páginas de sites e etc, a fim de que se saiba exatamente qual o caminho de tais documentos, quem o acessou e se houve a possibilidade de alterá-lo, e como isso ocorreu.

As provas virtuais é um assunto muito delicado e que precisa de aprofundamento para tentar driblar os crimes virtuais, ou seja as provas de um crime virtual são muito sensíveis, num clicar de *mouse* as provas podem ser destruídas pelo autor ou terceiros.

---

<sup>22</sup> Disponível em <[https://www.oficinadanet.com.br/artigo/443/o\\_que\\_e\\_criptografia](https://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia)>. Acesso em: 22 maio 2017.

<sup>23</sup> RIO GRANDE DO SUL. Tribunal de Justiça. Habeas Corpus nº. 70059192351, da 2ª Câmara Criminal. Rel. Min. Marco Aurélio de Oliveira Canosa. Porto Alegre. Julgado em 10 de julho de 2014, publicado no DJ em 22 de agosto de 2014. Disponível em: <[http://www.tjrs.jus.br/busca/search?q=facebook++meio+de+prova+penal&proxystylesheet=tjrs\\_index&client=tjrs\\_index&filter=0&getfields=\\* &aba=juris&entsp=a\\_\\_politicassite&wc=200&wc\\_mc=1&oe=UTF-Acesso em: 20 jul. 2017](http://www.tjrs.jus.br/busca/search?q=facebook++meio+de+prova+penal&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=* &aba=juris&entsp=a__politicassite&wc=200&wc_mc=1&oe=UTF-Acesso em: 20 jul. 2017)>.

Contudo, faz-se importante o Estado rever a valoração das provas e dos meios de obtenção delas no Processo Penal Brasileiro devido às evoluções tecnológicas envolvidas no mundo de hoje.

Ou seja, nesse vasto mundo cibernético, a prova digital deverá ser colhida de forma célere, cumprindo todos os cuidados necessários, sob pena de perder integridade do seu conteúdo.

Entende-se, que a perda de sua integridade, por serem provas de cunho sensível, que há obstáculos quanto à utilização dessas provas em processos judiciais, do outro lado, reitere-se, que mesmo as provas documentais físicas estão sujeitas a problemas de veracidade e autenticidade também, e, tendo em vista a construção epistêmica do processo, reconhece-se que todas as provas estão sujeitas a falhas na tentativa de reconstrução da verdade, não é porque a prova é obtida por meio eletrônico que ela terá pouca veracidade.

Nesse sentido, os óbices encontrados ao longo da investigação criminal, bem como do eventual processo penal, vão desde a identificação de um possível autor e sua localização, que identificar o IP – protocolo de internet – que identifica a máquina de onde partiu a conduta – o que não significa, necessariamente, identificar o sujeito criminoso, passando pela validade e licitude e provas colhidas.

Por fim, as dificuldades de rastreamento das condutas do suposto autor do crime, essa última é o grande obstáculo para aqueles crimes praticados no meio virtual, pois o perecimento de informações é rápido.

Assim, o investigador deverá considerar a prova pela sua natureza efêmera, o que dificulta a sua conservação num dispositivo eletrônico-digital que permite aumentar o seu período de utilização investigativa, para além do naturalmente considerado.

Para tanto é necessário meio mais eficaz para obtenção das provas virtuais, como equipes multidisciplinares, entre policiais com especialidade para tanto, empresas de rede sociais, agentes infiltrados, sistemas específicos, necessário também o aperfeiçoamento de recursos humanos no setor de segurança nesse meio ambiente virtual, estímulo ao crescimento das atividades de informática. Assim há possibilidade de obter as provas de forma célere e eficaz, com possibilidades maiores de achar o suposto infrator do delito.

### 3.2- Da Admissão das Provas nos Crimes Virtuais

Como mencionado em tópico anterior, as provas são a parte mais importante de um processo, seja em qualquer âmbito do Direito. E se na atualidade tem-se as redes sociais, por meio da internet, como meio de comunicação de maior utilidade, nota-se que as provas virtuais também estão sendo meios de prova de grande relevância dentro do Processo Penal Brasileiro.

Nesse sentido, o Estado deve rever a questão das provas virtuais e dos meios de obtenção destas no Processo Penal Brasileiro? Uma pergunta de relevância, pelo fato de não termos qualificação, seja com profissionais capacitados, seja por legislações eficientes, aprimoradas e específicas.

Dessa forma, torna-se necessária a atuação do Estado no sentido de coibir esse tipo de conduta, sendo necessária a criação de tipos penais ainda não previstos na legislação e que envolvam o mundo virtual, uma vez que não é permitido, em Direito Penal, utilizar analogia em relação às tipificações já existentes<sup>21</sup>.

Assim, considerando o avanço tecnológico e aplicando tal evolução no processo penal, pode-se constatar a possibilidade de as redes sociais serem utilizadas como mecanismo de prova junto aos tribunais, embora não estando explicitamente prevista no Código de Processo Penal Brasileiro.

Portanto, faz-se necessário trazer à tona a discussão que tange acerca da utilização das provas no âmbito do Processo Penal, a obtenção delas por meio das redes sociais como meio de produção de provas, esclarecer a importância da validade dessas provas no processo judiciário e mostrar a devida atualização referente as inovações tecnológicas que o judiciário deva ter para a aceitação dessas provas.

Sob a ótica do Direito Processual Penal, entende-se que a admissão e a coleta da prova são elementos essenciais para chegar à autoria de um delito, verifica-se que os crimes virtuais são complexos de serem verificados quando

---

<sup>21</sup> POLEGATTI, B. C.; KAZMIERCZAK, L. F. Crimes Cibernéticos: O Desafio do Direito Penal na Era Digital. Ourinhos, 2012.



cometidos, e conseqüentemente a obtenção das provas desses delitos são de grande dificuldade.

Na atualidade, percebe-se que não há instrumentos eficientes para coleta de provas por meio virtual, mas deve-se utilizar de forma precisa as poucas ferramentas que encontram disponíveis. Para adentrar nos meios de coleta das provas nos crimes virtuais, será necessário conhecer como funciona o procedimento de usuário – *internet* – sigilo.

Supõem-se que o *Instagram* seja o responsável por manter os dados cadastrais do autor da ofensa, logo tem-se que enviar um ofício à empresa solicitando os dados do suposto autor do crime, o *instagram* apresenta os dados cadastrais, mas, com base no Marco Civil da *Internet*, se recusa a fornecer o IP (*internet protocol*), conteúdos e outros dados que necessitam de autorização judicial para serem obtidos.

Em regra, até o *instagram* enviar uma resposta ou informação solicitada, e a autoridade policial remeter o inquérito para o judiciário e ter a representação judicial, já se passou um longo e considerável tempo para o tipo de crime em questão.

A obtenção de provas nos crimes virtuais, talvez não seja alcançada por ter entraves como a necessidade de autorização judicial para uma empresa fornecer o conteúdo de um suposto delito.

Em contrapartida, há um importante instrumento dentro desse contexto tramitando no Senado Federal, o projeto de Lei nº 486 de 2013, que estabelece que os provedores terão de comunicar ao delegado de polícia eventuais práticas ilícitas.

para estabelecer que uma vez detectada a ocorrência de delitos praticados por intermédio da rede mundial de computadores, os provedores dos serviços de acesso e conteúdo utilizados no cometimento de tal ilícito deverão comunicá-lo ao delegado de polícia em até quarenta e oito horas, preservando as evidências que ensejaram a comunicação por até cento e oitenta dias.<sup>22</sup>

---

<sup>22</sup> [www25.senado.leg.br/web/atividade/materias/-/materia/101649](http://www25.senado.leg.br/web/atividade/materias/-/materia/101649)

De certa forma, a *internet* criou a impunidade para a prática de alguns crimes, assim sob a perspectiva da realidade dos crimes virtuais, a cada dia os números aumentam, sendo um crime por meio da *internet* e não um crime de *internet*.

Assim, nota-se a necessidade de que tribunais sejam mais flexíveis no sentido da devida valorização das provas virtuais para comprovação dos crimes, tendo em vista que são por essas provas que se chega mais perto da autoria e materialidade do suposto delito praticado por meio virtual.

#### **4.0- Da ineficiência de autorização judicial para obtenção das provas nos crimes cibernéticos.**

Os crimes e as provas virtuais têm certa sensibilidade de desaparecimento, ou seja, tem uma depreciação muito rápida por serem virtuais, acredita-se que até a solicitação e autorização judicial para a obtenção dessas provas, já houve o desaparecimento das mesmas, por isso a obtenção de provas virtuais no Processo Penal deveria ser de pronto, sendo que as autoridade policiais deveriam ter acesso imediato as tais provas, e o Ministério Público poderia ter o condão de autorizar a obtenção dessas provas.

O entrave do assunto em questão é que, depois da Lei do Marco Civil, o processo de investigação contra os crimes virtuais ficou ainda mais difícil.

O crime da internet não tem fronteira onde tudo se pode rastrear. No entanto, com a aprovação do Marco Civil<sup>23</sup>, os conteúdos virtuais dependem de ordem judicial.

Quanto ao conteúdo das comunicações privadas armazenadas nos servidores dos provedores, faz-se necessária a ordem judicial. Somente os dados cadastrais poderão ser obtidos sem autorização judicial, todas as demais informações deverão ter acesso autorizado via mandado do juiz, o que dificulta a investigação.

O Marco Civil da *internet*, no entanto, é muito mais principiológico do que regulamentador, pois na maior parte de seus dispositivos apenas reconhece os

---

<sup>23</sup> O Marco Civil da Internet, oficialmente chamado de Lei N° 12.965/14, é a lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado

direitos fundamentais estabelecidos na Constituição Federal de 1988, mas não traz nenhuma solução, muito menos proteção para as conexões via internet. Algumas empresas costumam não criar óbices às investigações de crimes eletrônicos que tenham sido supostamente realizados por meio de seus serviços, pelo que está disposto no entendimento do Superior Tribunal de Justiça:

CRIME CONTRA A HONRA. DADOS. IP. “A obtenção de dados do usuário de determinado *Internet Protocol* (IP) consistente tão só na identificação da propriedade e do endereço em que instalado o computador do qual partiu o escrito criminoso não está resguardada pelo sigilo de que cuida o art. 5º, XII, da CF/1988, nem pelo direito à intimidade, que não é absoluto, prescrito no inciso X daquele mesmo artigo. Inexiste, no caso, qualquer aspecto do “*modus vivendi*” da pessoa, o que não resulta constrangimento ilegal. Assim, a Turma ao prosseguir o julgamento, denegou a ordem. (HC 83.338-DF, Rel. Min. Hamilton Carvalhido, julgado em 29/09/2009.)<sup>24</sup>

Portanto, há no âmbito constitucional os direitos individuais e coletivos, sendo que, caso a polícia tenha acesso aos conteúdos e informações dos usuários sem autorização judicial, conduz que há um lesão no direito individual, questão que traz grande emblema, pois nesse caso o direito coletivo, que seria a busca pelo agente criminoso prevaleceria sobre o direito individual.

Desta forma, as empresas que costumam exigir autorização judicial e com tal atitude estariam acobertando com a criminalidade ao dar abrigo as suas condutas e dificultando o trabalho das investigações, há nas palavras do Ministro Hamilton Carvalhido do STJ em sua decisão que, “inexiste, no caso, qualquer aspecto do *modus vivendi* da pessoa, o que não resulta constrangimento ilegal<sup>25</sup>”.

---

<sup>24</sup> Disponível <[www.stf.jus.br/portal/processo/verProcessoPeca.asp?id=3960447&tipoApp=.pdf](http://www.stf.jus.br/portal/processo/verProcessoPeca.asp?id=3960447&tipoApp=.pdf)> Acesso em: 21 de jun. de 2017.

<sup>25</sup> Disponível em <[www.stj.jus.br/docs\\_internet/informativos/RTF/Inf0409.rtf](http://www.stj.jus.br/docs_internet/informativos/RTF/Inf0409.rtf)> Acesso em: 01 de jun. de 2017.

O Delegado de Polícia Civil de SP Dr. José Mariano de Araújo Filho demonstrou sua preocupação no sentido de que “não raro, após vencer a burocracia imposta pelas representações aos Juizes para obtenção de informações de endereços I.P, o investigador acaba surpreendido pelo fato de que o detentor de tais dados que os informa não mais os possuir em arquivo”<sup>26</sup> E tal preocupação prospera, e isso pelo simples motivo de não haver na legislação qualquer determinação no sentido de que as empresas que prestam quaisquer tipos de serviços pela e para a Internet tenham que armazenar seus dados por algum período de tempo, em 3 a 5 anos, como é o desejável. Assim, fica à mercê e na quase totalidade das investigações, o delegado por exemplo de enviar via ofício, caso a caso, solicitando que tais empresas preservem os dados solicitados para que possam ser utilizados em investigação criminal em curso.

Esta foi uma primeira abordagem em relação ao tema. Os profissionais que tenham envolvimento com a investigação de crimes informáticos devem se manifestar e debater tais assuntos de forma aberta para que haja conscientização das empresas envolvidas.

Para a efetiva investigação de tais crimes virtuais no Brasil, em sua grande maioria era necessária a produção de representação ao Poder Judiciário, a fim de que fosse determinada a quebra do sigilo dos dados cadastrais de determinado acesso a grande rede pelo IP identificado. Isso quando não era necessária uma primeira representação para sabermos o IP utilizado.

O crime virtual sendo um crime atual, nota-se a quantidade assustadora de ocorrências, em contrapartida nota-se a existência de uma pequena quantidade de investigadores e de policiais especializados. Juntos a demora ou atraso da autorização do Poder Judiciário e a falta de informações requisitadas pelas empresas para ter acesso aos conteúdos. Certo que, uma investigação que parece bastante simples, acaba sendo prejudicada pelo excesso de exigências legais.

É importante ressaltar, em certos casos, para que se proceda a investigação, faz-se mister a autorização judiciária para a quebra de dados,

---

<sup>26</sup> Disponível em <<https://br.linkedin.com/in/josé-mariano-araujo-filho-9378724a>.> Acesso em: 16 jun.de 2017.

conexão ou acesso, busca e apreensão de material de informática e até mesmo para que se possa proceder uma completa investigação.

No Brasil, para que se encontre o cadastro do investigado:

basta que faça a busca do seu domínio em <http://registro.br> que estão disponíveis os cadastros dos proprietários dos sites com terminação “.Br”, assim será encontrado endereço e telefone da pessoa que criou determinado site, bem como o endereço de IP de onde este está hospedado<sup>27</sup>

#### **4.1 – Das hipóteses de inovações jurídicas para diminuir os crimes virtuais**

A legislação brasileira ainda se mostra muito aquém do que deveria. Existe no ordenamento jurídico uma sucessão de leis esparsas que procuram tratar do tema, porém ainda não existe legislação específica que consolide uma taxatividade dos crimes cibernéticos, nem ao menos uma conceituação jurídica adequada.

Vale ressaltar que não apenas no direito processual penal são percebidas questões merecedoras de reflexão, mas também no direito material. O Marco Civil da Internet, regulado por meio da Lei nº 12.965/14, foi um grande avanço nesse sentido, porém existe ainda grave deficiência legislativa na tipificação dos delitos virtuais a fim de combater e evitar esses crimes.

É importante salientar que pelo fato do Direito Penal brasileiro não recepcionar a analogia *in malam partem*, é imprescindível que os tipos penais sejam bem definidos na legislação, caso contrário, a lei penal incriminadora não pode ser aplicada.

Portanto, as condutas chamadas de crimes virtuais (embora inexista legislação específica) encontra-se tipificada em textos legislativos existentes (Código Penal e legislação esparsa) e, ao

---

<sup>27</sup> WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos, Ameaças e procedimentos de investigação. Editora: Brasport. P. 23 a 37

contrário do que alguns autores afirmam, a aplicação da lei já existente a essas condutas não é caso de analogia, pois não são crimes novos, não são novos bens jurídicos necessitando de tutela penal, a novidade fica por conta do *modus operandi*, de como o criminoso tem feito uso das novas tecnologias, com foco na Internet, fazendo com que os estudiosos e os aplicadores do Direito tenham que renovar o seu pensamento.<sup>2829</sup>

Os órgãos de segurança têm utilizado as redes sociais para auxiliar nas investigações em determinados casos com a devida autorização judicial, infiltrando-se para conseguir evidências em crimes sexuais contra a criança e o adolescente<sup>30</sup>.

É importante ressaltar que a recente Lei 13.441/2017 prevê a infiltração de agentes de polícia na internet com o fim de investigar crimes contra dignidade sexual de crianças e adolescente, entretanto a Lei poderia em sua redação ter ampliado a abrangência quanto a infiltração dos agentes de polícia nos demais crimes virtuais, para lograr êxito quanto a busca da autoria dos crimes.

Recentemente, nos Estados Unidos, ocorreu a prisão de um jovem de 26 anos que descumpriu uma decisão em um caso de *cyberstalking* que determinava a restrição do contato de pessoas não apenas fisicamente, mas via *internet* também.<sup>31</sup>

“As novas tecnologias e seus desdobramentos beneficiam não apenas a produção de provas como também o andamento dos processos.”<sup>32</sup>

No caso de páginas falsas, postagens ofensivas em sites de relacionamento, publicação e escritas indevida, vídeos e fotos etc., o importante é ter o endereço (link) e também a página impressa do fato ocorrido.

---

<sup>28</sup> PINHEIRO, Emeline Piva. Crimes virtuais: uma análise da criminalidade informática e da resposta estatal. Disponível em:

<<http://www.egov.ufsc.br/portal/sites/default/files/anexos/29397-29415-1-PB.pdf>>. Acesso em: 29 de mar. 2017

<sup>30</sup> Disponível em <http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/486183CAMARA-APROVA-INFILTRACAO-DE-POLICIAL-NA-INTERNET-PARA-INVESTIGAR-PEDOFILIA.html> Acesso em: 10 de maio de 2017.

<sup>31</sup> Disponível em <http://emporiododireito.com.br/clicar-22-vezes-seguidas-no-facebookconfigurastalking-os-perseguidores-mais-do-que-virtuais-por-danielle-mariel-heil/> Acesso em 12 maio 2017.

<sup>32</sup> Disponível em <<http://emporiododireito.com.br/juiz-utiliza-whatsapp-para-notificar-partes/>> Acesso em: 14 maio 2017.

A mesma orientação cabe para os sítios de comércio eletrônico, que sempre exigem um cadastro dos usuários, tanto para venda quanto para compra. Neste caso, também é importante trazer o registro das conversas realizadas por correio eletrônico e/ou comunicadores instantâneos, como tipos de protocolo.

Já no caso de correio eletrônico com conteúdo criminoso, o que não é incomum, além da página impressa, a pessoa deve levar junto o que chamamos de "cabeçalho do e-mail" ou "código fonte" da mensagem, guardando o correio eletrônico na sua caixa postal, ou seja, apagar o correio eletrônico não vai ajudar na identificação do criminoso.

Porém, infelizmente, a tecnologia avança de forma que não consegue ser alcançada pela legislação e diariamente novas possibilidades de cometimento de crimes pela internet surgem, a ausência de uma legislação específica para o crime virtual torna a punição problemática e dificulta na coleta e apresentação de provas.

Portanto, o Brasil não inseriu uma legislação eficiente para banir criminosos que cometem crimes virtuais, que de fato deveria ser uma legislação específica, detalhada e com penas mais rígidas, como por exemplo: cometer crime de calúnia no plano presencial que estabelece uma pena de detenção, de seis meses a dois anos, e multa, este previsto no Código Penal, e caso seja praticado por meio virtual, essa pena dobraria, e assim por diante aplicaria em todos os crimes cometidos virtualmente, hipóteses a serem analisadas para serem inseridas no Código Penal ou em alguma legislação específica sobre crimes virtuais.

Assim, como mencionado anteriormente, tais questões merecedoras de reflexão devem ser notadas tanto no direito processual como no direito material.

Assim, com legislações mais presentes e tendo uma penalidade mais rígida, amenizaria o grande crescimento de crimes virtuais, pois esses crimes são os crimes do momento, identificados como crime da atualidade.

Contudo, temos os chamados crimes do momento, mas não temos a legislação eficiente para aplicar nesses crimes virtuais, fazendo com que a cada dia o número de criminosos aumentem.

Outro ponto relevante a mencionar, são as carências do Poder Judiciário de aceitar provas advindas pelo meio virtual, ora, se os crimes estão

acontecendo dessa forma, não mais cabível que provas virtuais sejam aceitas para fim de apurar os fatos verdadeiros de um crime, identificando a autoria e a concretização da materialidade do delito.

Portanto, a investigação de crimes virtuais torna-se um pouco mais difícil, tendo em vista que devido às especialidades e meios para se alcançar o objetivo esperado, o agente investigador precisa ter um conhecimento mais aprofundado acerca da informática, porém, nem todos os agentes detêm tal conhecimento, para isso, torna-se imprescindível uma unidade na polícia para fazer um treinamento específico e atender a esses delitos especialmente.

Com todo contexto mencionado acima, não se esgotam por aqui as hipóteses de possibilidade para ajudar na busca de autores de crimes virtuais, podendo desde então criar equipes multidisciplinares, entre policiais especializados, leis mais rígidas, agentes infiltrados virtualmente, disque denúncia, comunicação *online*, esse último seria de grande relevância, pois os usuários que seriam vítimas dos crimes virtuais, acessariam via *internet* por meio de um link para comunicação de denúncias *online*, faria sua queixa e a partir de então os agentes especializados verificariam em tempo real o suposto delito, capturando provas no momento do delito, sem perder a integridade das provas com o passar do tempo.

As inovações legislativas no que se refere a provas virtuais dentro do Processo Penal Brasileiro permitiriam uma ampliação e eficiência de hipóteses de investigação criminal e de cooperação entre equipes multidisciplinar para serem tratadas tais matéria.

É de grande relevância haver um tópico específico dentro do Código de Processo Penal sobre o regime de obtenção de prova virtual, facilitando a admissão nos processos judiciais.

## 5- Conclusão

Entende-se que a globalização dentro dos fatores de comunicação, que foi o nosso ponto de partida para o atual trabalho, mostrou que a *internet* facilitou os crimes virtuais e como não há legislação eficiente atuais para tais crimes, há uma grande dificuldade nas investigações, estimulando a cada dia a impunidade,



para tanto, uma análise de estudos e técnicas jurídicas precisam ser reformuladas e aperfeiçoadas, para diminuir esse ritmo de práticas de crimes praticados virtualmente pelo Brasil e no mundo.

Para alcançar e prosseguir com a possibilidade de diminuir os crimes virtuais, é de grande relevância ter avanços referentes aos meios de obtenção de provas, para concretizar a autoria e a materialização dos crimes, como por exemplo o que dispõe a Lei 13.441/2017, que prevê a infiltração de agentes policiais na internet a fim de investigar crimes contra dignidade sexual de crianças e adolescentes, porém poderia nesta Lei ter ampliado quanto a infiltração dos agentes de policias também para os demais crimes virtuais.

É certo que, apesar das dificuldades, acredita-se que o trabalho de investigação e a devida condenação desses criminosos podem ser facilitados se houver investimentos, tanto em pessoal e treinamento, ou seja, pessoas altamente qualificadas no mundo da informática para realização das investigações e perícias, quanto as leis de hoje que são mal redigidas e não levam em consideração o modo como acontecem os crimes na *internet*.

Como mencionado, as provas de crimes cometidos por meio virtual são de fácil desaparecimento, e por isto as investigações e coletas de provas tem de ser o mais rápido possível, não necessitando de autorização judicial para coleta de provas nos crimes virtuais. Nesse quesito de não haver autorização judicial para obtenção de provas, vale mencionar que não seria genérica o acesso para verificar conteúdos suspeitos, apenas equipes credenciadas e especializadas dentro do poder executivo e judiciário teriam acesso aos conteúdos.

A legislação brasileira referente aos crimes virtuais não está adequada e, muitas vezes, o crime prescreve sem que haja uma punição dos autores do delito. Avanços significativo nas investigações seriam um mecanismo que ajudaria na busca dos criminosos, mas a tecnologia avançou e a legislação não o acompanhou.

Nos crimes contra a honra, por exemplo, há uma enorme dificuldade para se identificar o autor de ofensas realizadas na *internet*, e sem a identificação, seja do IP do computador, do conteúdo, das provas, e etc- sequer é possível oferecer queixa-crime. Questiona-se que grande maioria dos autores que cometem delitos por meio virtual ficam impunes, devido a ineficiência das investigações policiais, dos recursos disponíveis e das legislações vigentes, que

são ineficazes para estruturar uma busca para autoria dos delituosos, verifica-se que quando não se pune os criminosos por algum crime, aquela prática se torna contínua.

Pelo estudo apresentado em questão, no âmbito da investigação criminal, abordou uma grande preocupação com as características das provas virtuais, sendo essas provas um mecanismo de grande importância para verificar autorias dos crimes cibernéticos dentro do direito processual penal.

Contudo, os meios de provas utilizados atualmente, considerados válidos pelo ordenamento jurídico brasileiro, para que seja demonstrada a autoria e materialidade de um crime virtual são: a perícia realizada no computador utilizado pelo agente criminoso, a interceptação de correios eletrônicos e a quebra de sigilo de sítios de relacionamento, tais como *Orkut*, *Facebook*, *Instagram*, entre outros. Mas não significa que com essas ferramentas descritas acima seja alcançado o objetivo maior, que é a identificação da autoria.

No entanto, há necessidade de instrumentos eficientes para verificar a identificação dos autores dos crimes virtuais que precisam ser renovadas, como por exemplo: agentes infiltrados virtualmente, aperfeiçoamento de recursos humanos para o setor de segurança e informática, programas prioritários de defasa a informação, estímulo ao crescimento das atividades de inteligência da informática, integração das empresas de redes sociais e de comunicação com as polícias de investigação das delegacias especializadas em crimes virtuais, capacitação e materiais para as equipes, criação de equipes multidisciplinares entre polícias, empresas e judiciário, uma criação de disque denúncia *online* de crimes virtuais, que serão acessados em tempo real pelos agentes de investigação, que poderão obter provas e materialidade em segundos, não deixando que as provas se dispersem com um clicar do mouse, ainda mais, pode se inserir na legislação brasileira, penalidades mais severas quando crimes forem praticados virtualmente, ou seja, aplicar em dobro aqueles crimes que forem praticados por meio da *internet*.

Questiona-se o acesso aos conteúdos virtuais sem autorização judicial, violaria o direito a intimidade, é certo que a importância do direito à privacidade é tão relevante que a própria pessoa, ainda que deseje, não pode renunciar ou abdicar dele. Isto porque, segundo a Constituição Federal (artigo 5º, X), são invioláveis a intimidade, a vida privada, a honra e a imagem, assegurado o direito

à indenização pelo dano material ou moral decorrente de sua violação, mas o que causa uma contradição quanto a essa questão é: o que é de maior relevância, um direito individual ou um direito coletivo? Vale mencionar que o desvendar dos criminosos é um direito da sociedade perante o Estado, revelando que o direito coletivo nesse caso, se sobressai ao direito individual. Portanto, este estudo mostra que o assunto tratado se encontra em um estágio inicial, devendo ainda evoluir da mesma maneira que a *Internet* evolui a cada dia.

O regime regulador da prova digital necessitará de uma intervenção legislativamente coerente e cientificamente sustentável, sendo fundamental a implementação de um novo modelo regulador para crimes virtuais, capaz de conjugar as mudanças tecnológicas e a expansão dos crimes.

Muitas são as formas passíveis de serem utilizadas com o objetivo de combater este tipo de criminalidade virtual, tais como a criação de leis que tipifiquem estas condutas e regulamentem os meios de provas, facilitando a investigação e a punição dos delinquentes virtuais. Havendo maior coerção, os criminosos pensarão duas vezes antes de usar a *internet* como ferramenta para a prática de crimes, pois não estarão mais abrigados sob o manto da impunidade e do anonimato.

## 6 – Referências

BRASIL. Câmara Dos Deputados. **infiltração de policial na internet**. Disponível em: <<http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/486183CAMARA-APROVA-INFILTRACAO-DE-POLICIAL-NA-INTERNET-PARA-INVESTIGAR-PEDOFILIA.html>>. Acesso em: 10 maio de 2017.

BRASIL. Tribunal de Justiça do Rio Grande do Sul. **Habeas Corpus nº. 70059192351**, da 2ª Câmara Criminal. Rel. Min. Marco Aurélio de Oliveira Canosa. Porto Alegre. Julgado em 10 de julho de 2014, publicado no DJ em 22 de agosto de 2014. Disponível em: <<http://www.tjrs.jus.br/busca/search?q=facebook++meio+de+prova+penal&proxy>>

stylesheet=tjrs\_index&client=tjrs\_index&filter=0&getfields=\*&aba=juris&entsp=a  
\_\_politica-site&wc=200&wc\_mc=1&oe=UTF-8&ie=UTF-  
8&ud=1&lr=lang\_pt&sort=date%3AD%3AS%3Ad1&as\_qj=facebook+utilizado+c  
omo+meio+de+prova+penal&site=ementario&as\_epq=&as\_oq=&as\_eq=&as\_q  
=#main\_res\_juris. Acesso em: 20 jul. 2017.

BRASIL. Senado Federal. **Atividade e materiais**. Disponível em:  
<[www25.senado.leg.br/web/atividade/materias/-/materia/101649](http://www25.senado.leg.br/web/atividade/materias/-/materia/101649)>. Acesso em:  
21 de julho de 2017.

BRASIL. Superior Tribunal de Justiça, **informativo nº 0409**. Disponível  
em: <[www.stj.jus.br/docs\\_internet/informativos/RTF/Inf0409.rtf](http://www.stj.jus.br/docs_internet/informativos/RTF/Inf0409.rtf)>. Acesso em:  
01 de junho de 2017.

BONFIM, Edilson Mougenot. **Curso de processo penal**. 3.ed. rev. São Paulo:  
Saraiva, 2008.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. 1. ed. Rio de  
Janeiro: Brasport, 2014.

COLLI, Maciel. Cibercrimes. **Limites e perspectivas à investigação policial  
de crimes cibernéticos**. Curitiba: Juruá Editora, 2010.

CONJUR, **crimes virtuais**. Disponível em: <<http://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg--especialistacrimes-virtuais>>. Acesso em 08 de maio  
de 2017.

COSTA, Levi Roberto; PEIXOTO, Hélio Pereira. **Um método para  
sistematização do processo investigatório de análise da informação  
digital Fomentando a cognição na atividade policial**. 2011. Disponível em:  
<<http://www.icofcs.org/2010/ICoFCS2010-FULL.pdf#page=20>>. Acesso em: 24  
maio. 2017.

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

DELEGADO DE POLICIA, **Crime por meio eletrônico**. Disponível em: <<http://mariano.delegadodepolicia.com/tag/invesrigacao-crime-por-meioeletronico/page/17/>>. Acesso em: 03 jun. de 2017.

EMPORIO DO DIREITO, **Perseguidores mais que virtuais**. Disponível em: <<http://emporiododireito.com.br/clicar-22-vezes-seguidas-no-facebookconfigurastalking-os-perseguidores-mais-do-que-virtuais-por-danielle-marielheil/>>. Acesso em: 12 maio 2017.

INSPER EDU, **mundo em fraudes digitais**. Disponível em: <<https://www.insper.edu.br/noticias/brasil-e-o-5o-do-mundo-em-fraudes-digitais/>>. Acesso em: 15 de junho de 2017.

JUS BRASIL, **decreto lei nº 3689/1941**. Disponível em: <<http://www.jusbrasil.com.br/topicos/10660113/paragrafo-1-artigo-232-dodecreto-lei-n-3689-de-03-de-outubro-de-1941>>. Acesso em: 30 de maio de 2017.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012.

MENDES, Maria Eugencia Gonçalves. VIEIRA, Natália Borges. **Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica**. 2012.

NOGUEIRA, Sandro D'Amaro. **Crimes de Informática**. Leme: BH Editora, 2009.

NUCCI, Guilherme de Souza. **Manual de Processo Penal e Execução Penal**. 6ª Ed. 2010.

OFICINA DA NET, **criptografia**. Disponível em: <[https://www.oficinadanet.com.br/artigo/443/o\\_que\\_e\\_criptografia.](https://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia.)>. Acesso em: 22 de maio de 2017.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. Disponível em:

<http://www.egov.ufsc.br/portal/sites/default/files/anexos/29397-29415-1-PB.pdf>.

Acesso em: 05 de mar. 2017

PINHEIRO, Reginaldo Cesar. **Os crimes virtuais na esfera jurídica brasileira**. Boletim IBCCrim, abr. 2001.

PLANALTO, **Lei nº 8069**. Disponível em:

<[http://www.planalto.gov.br/ccivil\\_03/leis/L8069.htm](http://www.planalto.gov.br/ccivil_03/leis/L8069.htm)>. Acesso em: 19 de junho de 2017.

POLEGATTI, B. C.; KAZMIERCZAK, L. F. **Crimes Cibernéticos: O Desafio do Direito Penal na Era Digital**. Ourinhos, 2012.

TECNOLOGIA IG, **crime cibernético**. Disponível em:

<<http://tecnologia.ig.com.br/2017-03-31/crime-cibernetico.html>>. Acesso em: 20 de maio de 2017.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos, Ameaças e procedimentos de investigação**. Editora: Brasport.

WORD PRESS, **Cibercrime**. Disponível em:

<<http://economia.estadao.com.br/noticias/releases-ae,crimesvirtuais-afetam-42-milhoes-de-brasileiros,70001644185>>. Acesso em: 17 de maio de 2017.