MEIOS DE PRODUÇÃO DE PROVA ATRAVÉS DO SISTEMA DE REDES E SUA UTILIZAÇÃO NO SISTEMA PENAL BRASILEIRO

CORREIA, Maria Helena.[1]
HELENE, Paulo Henrique.[2]

RESUMO

O presente trabalho traz aspectos relevantes sobre a produção de provas por meio do sistema de redes de dados, buscando abordar o problema de forma ampla e, sobretudo, orientando os usuários destes meios a se prevenirem de eventuais crimes que podem ser praticados online. Apresenta, ainda, formas de produção e autenticação de provas, como por exemplo, a ata notarial, para que as evidências possam ser utilizadas em eventual processo de investigação criminal. O objetivo principal é conscientizar os leitores sobre os problemas que podem ocorrer a partir de simples descuidos ao utilizar do computador no seu dia-a-dia, e as formas de utilizá-lo ao seu favor.

PALAVRAS-CHAVE: Internet, Provas, Processo, Crime.

ABSTRACT:

This paper brings important aspects about the production of evidence through the network system, searching to approach the problem broadly and, mostly, guiding users of these means to prevent possible crimes that can be practiced online. Also, it presents forms of production and authentication of evidences, as notarial records, so that evidence can be used in any criminal investigation process. The main objective is to make readers aware of the problems that can occur from a simple carelessness when using the computer, and ways to use it in their favor.
KEYWORDS: Internet, Evidence, Process, Crime.

1. INTRODUÇÃO

O objetivo do presente trabalho traz aspectos relevantes sobre os acontecimentos ilegais que ocorrem dentro dos sistemas de redes *online*.

Ainda existe grande vulnerabilidade dos usuários que acessam os sites através da *internet*, pois acabam se tornando vítimas fáceis dos agentes que utilizam o mesmo sistema para aplicarem golpes contra o patrimônio ou a honra, e que geralmente não são localizados para serem punidos, devido à dificuldade que se tem em localizá-los.

O tema deste trabalho será norteado sobre aspectos relevantes do Direito Penal, do Direito Processual Penal e, subsidiariamente, do Direito Digital. A utilização destes institutos legais auxiliará na compreensão e possível solução da problemática da matéria tratada.

Dentro do viés temático que liga o direito e a *internet*, há grandes consequências quando estas se unem. É evidente que pouco se fala sobre a dificuldade na responsabilização dos criminosos

[1]Acadêmica do 9° período do curso de Direito do Centro Universitário FAG. E-mail: mariahelenacorre@gmail.com.
[2]Docente orientador. E-mail: paulo2h@hotmail.com

diante da vulnerabilidade do usufruidor do sistema, aquele que, por vezes, se encontra exposto aos perigos que podem ser adquiridos juntamente com a sua utilização dos recursos *online*.

Há uma grande relevância jurídica ao falar deste assunto, pois a sociedade espera uma maior proteção e uma justificativa acerca dos crimes praticados através da *internet*, visto que, na maioria dos casos, o responsável não é localizado, e este ato ilícito acaba ficando com uma punição vaga, deixando um sentimento de insegurança e indignação social. Por sua vez, a população requer cada vez mais segurança, em razão da realidade econômico-social ser outra, e o direito procura acompanhar as novas lides para que exista uma repreensão válida a estas situações de forma célere.

É de extrema necessidade esta discussão, uma vez que estes atos criminosos cometidos por meio da rede de sistemas fazem vítimas a todo momento. Em decorrência da dificuldade de localização dos autores e da escassa informação da sociedade sobre as formas de prevenção dos crimes (e eventual formação de provas para embasar um futuro processo penal), os agentes dificilmente são punidos.

Ademais, diante da diversidade cultural brasileira, pode-se perceber que pessoas de baixo e alto nível de conhecimento já passaram ou ainda vão passar por situações como a acima descrita, e há uma grande necessidade de localização e responsabilização dos indivíduos que praticam estes atos criminosos.

Deste modo, devem ser estudados pontos categóricos sobre o tema, a fim de tentar encontrar possibilidades de localização, punição e outras resoluções alternativas, desta forma poderá haver efetividade na aplicação das leis que já dispõem sobre o assunto.

Portanto, o problema do presente trabalho norteia-se na utilização do sistema de redes para a localização dos criminosos que praticam ilícitos por este meio, tendo como objetivo principal analisar os modos de confecção de provas que tendem a facilitar este processo de busca, acarretando na responsabilização destes indivíduos.

2. A COMUNICAÇÃO GLOBAL E O ESTADO-NAÇÃO

Com o advento da globalização mundial e das crescentes atividades de demandas virtuais e sistematização dos procedimentos, reduziram-se ainda mais a tolerância das ações criminosas que tomam conta dos setores de informatização em seu sentido *lato*.

ISSN 2318-0633

O Estado vem sendo cada vez mais pressionado a legislar e controlar as lides que envolvem ilícitos cometidos através do sistema de redes, ocorre que diante de tanto avanço tecnológico, e com as variadas formas de integração entre tribos, a União perdeu uma porcentagem de força em seu poderio sobre as comunicações, principalmente as que se espalham pela rede de computadores, situação que acaba trazendo um significativo aumento na prática destes delitos.

Nesta vertente, o sociólogo espanhol Oliván (1999) brilhantemente relata que, através da globalização, o crime organizado tomou novos rumos, passando a ser uma ameaça sinceramente grave e de difícil solução pelos Estados, que muitas vezes se veem presos a pensamentos e mecanismos.

Ferreira (2001, p. 208) também descreveu muito bem toda esta situação encarada por nosso Estado e ordenamento jurídico:

> O Código Penal brasileiro [...] não se mostra suficiente e adequado para suprir as necessidades nesse setor e coibir os abusos que se verificam de forma crescente e diversificada, com a constituição de novas modalidades de ofensas e interesses legítimos, no plano individual e social, que ao Estado cumpre coibir sobretudo através do direito penal, se os conflitos não puderem ser solucionados de outra forma, como dispõe a boa doutrina, segundo o princípio da subsidiariedade.

Ressalta-se que, apesar de todo poder concentrado nos órgãos estatais a fim de punir, não é qualquer ação cometida na área da informática que será tutelada pelo Direito Penal Digital, pois deverá haver a utilização da *internet* para a sua consumação, como será visto mais adiante, cabendo observar qual é o bem jurídico tutelado e o meio utilizado.

Neste sentido, apesar de já ocorrer um grande movimento nos setores jurídicos ao que tange a proteção e tipificação de condutas ilícitas cometidas nas redes de computadores, ainda há muito que se trabalhar neste quesito, para que a responsabilização saia do campo abstrato e se torne mais efetiva.

É o que relata a advogada e especialista em Direito Digital, Patricia Peck Pinheiro (2010, p. 65-66):

> [...] devem ser criados novos princípios de relacionamento, ou seja, diretrizes gerais sobre alguns requisitos básicos que deveriam ser entendidos por todos os usuários da rede, a resolução destas questões já possibilitaria segurança maior nas relações virtuais. O que é diferente de se criarem normas específicas cuja aplicação e eficácia ficariam muito limitadas no tempo e no espaço.

ISSN 2318-0633

Quando se trata de relacionamento virtual a comunicação pode ser mais difícil do que realmente aparenta ser, pois se trata de uma grande rede de computadores interligados, envolvendo nações, culturas morais e éticas totalmente diferentes umas das outras. Como bem descreveu a doutrinadora supracitada, é necessário que novos princípios sejam estabelecidos e seguidos por todos que integram este sistema.

2.1 DIREITO PENAL E INFORMÁTICA

Direito Penal e a rede de computadores nunca antes estiveram tão interligados, e por este motivo, é de grande relevância a apreciação do instituto da responsabilização penal para o efetivo esclarecimento de suas características, aplicação e consequências a serem aplicadas ao caso concreto, visto que o crime eletrônico se utiliza do meio virtual para sua concretização.

Diante desta compreensão, Pinheiro (2010, p. 296) especifica:

> A maioria dos crimes cometidos na rede ocorre também no mundo real. A internet surge apenas como um facilitador, principalmente pelo anonimato que propicia. Portanto, as questões quanto ao conceito de crime, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital.

A responsabilidade penal advém da necessidade que o Estado possui em punir o agente capaz que se enquadrou em algum tipo penal através de uma ação ou omissão, causando um dano a outrem que deve ser reparado. Portanto, há requisitos penais a ser seguidos para que essa efetivação do poder estatal seja aplicada de forma correta e mais célere possível, como se observará mais precisamente nos próximos tópicos.

Neste sentido, Ferreira (2001, p. 210) muito bem retrata o raciocínio:

> Se considerarmos, de acordo com a moderna doutrina penal, que constitui **crime da informática toda ação típica**, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão, [...] e caracteriza os elementos necessários para a criminalização das condutas puníveis, podemos estabelecer uma ampla gama de relações sociais ou individuais que comportam a utilização da informática e a possibilidade dos abusos que se deseja coibir através das normas penais [grifos da autora].

ISSN 2318-0633

Ante ao que foi exposto, verifica-se que o Direito Penal tutela comportamentos humanos ativos ou omissivos que estejam tipificados em lei, atribuindo a responsabilidade penal ao agente através dos elementos da culpa ou do dolo, em respeito ao princípio da legalidade (FERREIRA, 2001).

A doutrina acima citada clama pela existência de um capítulo no código de Direito Penal totalmente voltado aos crimes praticados através do sistema informático, pois se trata de bens intangíveis que necessitam ser tutelados para que possa parar de utilizar analogias e haver um diploma legal mais forte e eficaz.

2.2 CRIME DIGITAL, ELETRÔNICO, INFORMÁTICO OU CIBERNÉTICO

O Direito Penal, ao regulamentar o crime, adotou a Teoria Analítica do Crime, dividindo-o em fato típico, ilícito e culpável.

Entende-se como fato ilícito tudo aquilo que inflige o direito de outrem, causando-lhe algum dano ao bem jurídico tutelado. Em sua obra, o doutrinador Guilherme de Souza Nucci se utiliza das palavras de Zaffaroni e Pierangeli para expor o conceito de que “a antijuridicidade é una, material porque invariavelmente implica afirmação de que um bem jurídico foi afetado, formal porque seu fundamento não pode ser encontrado fora da ordem jurídica” (NUCCI, 2008, p.238), e ainda complementa que nexo causal é aquele que liga a ilicitude ao dano final, sendo este último um tipo de resultado do fato ilícito, que após ter passado por uma causa, pode trazer prejuízos na esfera naturalística ou normativa.

O nexo causal é aquele liga a ilicitude ao dano final. Nas palavras do nobre doutrinador Nucci (2008, p. 196), “é o vínculo estabelecido entre a conduta do agente e o resultado por ele gerado, com relevância suficiente para formar o fato típico. Portanto, a relação de causalidade tem reflexos diretos na tipicidade e, para reconhecê-la, é preciso definir causa”.

Nesse sentido, pode-se entender como causa toda ação ou omissão que leva diretamente ao resultado danoso e que, sem a sua existência, não existiria o dever de reparação, já que o resultado danoso deve ser detectado mesmo que a sua contribuição seja mínima.

O dano é um tipo de resultado do fato ilícito, que, após ter passado por uma causa, pode trazer prejuízos na esfera naturalística ou normativa. O resultado naturalístico ocorre com a modificação

no mundo físico. Neste caso, só se pode falar em resultado quando houver efetivas mudanças passivas de serem percebidas. Por sua vez, resultado normativo configura-se pelo resultado no mundo jurídico, por meio de um dano efetivo ou dano em potencial (NUCCI, 2008). Portanto, entende-se como dano toda a conduta que possa gerar resultados negativos e que ferem algum interesse jurídico tutelado.

Para que haja a efetiva coação estatal sobre as condutas praticadas por criminosos por meio do sistema de redes, há a necessidade de que se respeitem alguns princípios norteadores do chamado Direito Penal Mínimo, ou seja, elementos que classifiquem a conduta como ilícita. Assim, considerando-se que o Direito Penal é uma esfera estatal de intervenção mínima, há critérios que devem ser respeitados para que a punição seja efetivada com maior precisão, pois a última medida a ser tomada é a restrição de liberdade do agente.

Nesse sentido, vale ressaltar que o princípio da culpabilidade defende que não haverá crime sem presença da culpa ou do dolo, assim como preceitua o doutrinador Jesus (2013, p. 53):

> *Nullum crimen sine culpa*. A pena só pode ser imposta a quem, agindo com dolo ou culpa, e merecendo juízo de reprovação, cometeu um fato típico e antijurídico. É um fenômeno individual: o juízo de reprovabilidade (culpabilidade), elaborado pelo juiz, recai sobre o sujeito imputável que, podendo agir de maneira diversa, tinha condições de alcançar o conhecimento da ilicitude do fato (potencial consciência da antijuridicidade). O juízo de culpabilidade, que serve de fundamento e medida da pena, repudia a responsabilidade penal objetiva (aplicação de pena sem dolo, culpa e culpabilidade).

Na doutrina, a utilização específica do referido princípio ainda não foi pacificada, mas, no entendimento do doutrinador Greco (2008), a culpabilidade está rodeada por três elementos basilares, quais sejam: ela serve como um elemento para a análise do crime, um princípio medidor da pena e um mediador da responsabilidade penal sem o elemento culpa.

Assim, o autor descreve a culpabilidade em sua obra nos seguintes termos:

> Trata-se de um juízo de reprovação social, incidente sobre o fato e seu autor, devendo o agente ser imputável, atuar com consciência potencial de ilicitude, bem como ter a possibilidade e a exigibilidade de atuar de outro modo, seguindo as regras impostas pelo Direito (teoria normativa pura, proveniente do finalismo). (GRECO, 2008, p. 281).

No que se refere especificamente ao crime digital, alguns autores denominam crimes de informática impróprios aqueles praticados com o uso da *internet* como um facilitador da conduta ilícita, mas que sem ela seriam normalmente praticados. De outro lado, chama-se de crimes de

ISSN 2318-0633

informática próprios aqueles que podem ser efetivados somente pelo sistema de redes (FERREIRA, 2001).

Logo, Greco (2008) ensina que deve haver requisitos subjetivos para a aplicação das punições penais, levando-se em consideração os elementos da responsabilidade penal. O elemento dolo é o que está presente na maioria dos fatos ilícitos praticados nas redes de computadores. Isso ocorre porque o dolo se limita à própria intenção do agente em causar dano a outrem.

Nesse viés, o doutrinador Jesus (2013, p. 327) entende que o dolo "integra a conduta, pelo que a ação e a omissão não constituem simples formas naturalísticas de comportamento, mas *ações* ou *omissões* dolosas" [grifos do autor].

Portanto, para a visão da Corrente Finalista, entende-se por conduta dolosa toda aquela eivada por interesse do agente na prática de determinada ação ou supressão que determina certo resultado.

Ferreira destaca que a maior incidência de crimes praticados nas redes encontra-se relacionada à esfera econômica:

> Embora seja viável a ocorrência do uso dos meios informáticos na prática de um grande número de infrações, que a cada dia inclui uma nova modalidade, a predominância desses fatos é detectada principalmente na área dos crimes contra o patrimônio, contra a liberdade individual e contra a propriedade imaterial, além de outros de natureza econômica. (2001, p. 220).

Após as explanações feitas acerca dos critérios utilizados para a tipificação e punição de um ilícito penal, pôde-se observar que o requisito identificador da conduta criminosa efetuada pelo agente na descrição do tipo penal, chamado de ato ilícito, é justamente o que impede a efetivação da punição estatal.

Novamente, utilizando-se das notáveis explicações da doutrinadora Pinheiro, observa-se que o vilão do Estado é ele próprio:

> Legislar sobre a matéria de crimes na era Digital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindo o inocente. […] Por isso, devemos acompanhar esta discussão toda no Legislativo, visto que é necessária (PINHEIRO, 2010, p. 294).

Com a efetiva mudança de paradigmas globais e com a chegada da era da informatização, surgiram novas condutas que merecem ser punidas a rigor de sua gravidade. Para tanto, há uma grande necessidade na atualização do Código Penal, Código de Processo Penal e Lei de Execuções

Penais brasileira, para que conste a matéria dos crimes eletrônicos de forma efetiva (PINHEIRO 2010).

Ante ao exposto, verifica-se que, apesar da situação não estar devidamente controlada, o Estado não ficou inerte diante dos referidos ataques, pois houve inovações jurídicas que propiciaram alguns ajustes. Porém, ainda há muito que ser regulado para que a punição seja efetiva e precisa.

> As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como à necessidade de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio. (PINHEIRO, p. 296-297).

Para tanto, enquanto não há delimitações específicas acerca das novas condutas praticadas por meio das redes de computadores, resta observar as legislações existentes e tentar aplicá-las da forma mais fungível possível, a fim de tentar punir os agentes causadores dos danos para possíveis responsabilizações pelos atos praticados.

2.3 OS PRINCIPAIS CRIMES PRATICADOS ATRAVÉS DA INTERNET E SUAS FONTES

Os crimes que ocorrem por intermédio virtual têm como agentes indivíduos que acreditam na impunidade deste meio. Apesar desta sensação que é transmitida, há várias condutas que já são tipificadas pelo Código Penal, e consequentemente serão punidas de acordo com o seu enquadramento no diploma legal, pois neste caso, altera-se somente o meio utilizado para a prática do crime.

Como dita o doutrinador Cassanti (2014), as ameaças contidas em mensagens através dos sistemas de redes, a agressão e desrespeito, são atitudes cada vez mais comuns nas redes sociais, tais como o Facebook, Twitter, YouTube ou blogs.

Segundo os dados trazidos na obra citada, a ocorrência de condutas criminosas praticadas através da internet é cada vez maior, e o Judiciário vem utilizando-se da legislação vigente para afastar a impunidade destes crimes, tais como o Código Penal, Código Civil, e as leis específicas regulamentadoras, por exemplo, a da Interceptação Telefônica e da Proteção Intelectual, sendo que, segundo dados demonstrados no livro, 95% dos delitos praticados já são tipificados no Código

ISSN 2318-0633

Penal, e os outros 5% restantes necessitam de previsão legal, pois se referem a condutas que só podem existir dentro do meio eletrônico.

Abaixo, consta quadro com o exemplo de alguns crimes praticados pelo meio eletrônico e, respectivamente, as leis que os regulamentam, de acordo com a citação do autor Cassanti (2014).

Quadro 1 – Crimes praticados por meio eletrônico e leis que regulamentam

Crime	**Lei**
Uso indevido da imagem	Art. 5º, inc. X, CF/88
Insultos	Art. 140, CP
Calúnia	Art. 138, CP
Difamação	Art. 139, CP
Ameaça	Art. 147, CP
Divulgação de segredo	Art. 153, CP
Furto	Art. 155, CP
Dano	Art. 163, CP
Cópia não autorizada	Art. 184, CP
Escárnio por motivo religioso	Art. 208, CP
Favorecimento à prostituição	Art. 228, CP
Ato obsceno	Art. 233, CP
Escrito ou objeto obsceno	Art. 234, CP
Incitação ao crime	Art. 286, CP
Apologia ao crime	Art. 287, CP
Falsa identidade	Art. 307, CP
Inserção de dados falsos em sistemas de informação	Art. 313-A, CP
Adulterar dados em sistemas de informações	Art. 313-B, CP
Preconceito ou discriminação	Art. 20, Lei 7.716/89
Pedofilia	Art. 214 e seguintes, CP
Crime contra a propriedade industrial	Art. 195, Lei 9.279/96
Crime de concorrência desleal	Art. 195, Lei 9.279/96
Interceptação de comunicações de informática	Art. 10º, Lei 9.296/96
Crimes contra software (pirataria)	Art. 12, Lei 9.609/98
Negligência	Arts. 932 e 1.634, CC
Roubo de perfil em comunidades e blogs	Remendo constitucional 12.888-2/07

Fonte: CASSANTI, 2014, p. 36.

ISSN 2318-0633

2.4 AS FONTES DE COLETA DE INFORMAÇÕES PELA INTERNET

Apesar de ainda pouco utilizadas, há fontes desenvolvidas na *internet* que buscam trazer maior segurança aos usuários *online.* Antes de adentrar especificamente em cada espécie, se faz necessária sua conceituação e a breve classificação dessas fontes.

Conforme conceituam Barreto, Wendt e Caselli (2017), adequa-se ao conceito de fontes os dados ou conhecimentos que sejam úteis ao aplicador de investigação ou inteligência para a criação de meios de provas.

Ainda, conforme amplamente demonstrado na obra citada, segundo a Doutrina Nacional de Inteligência e Segurança Pública (DNISP), a fonte

> é toda e qualquer representação de fato, situação, comunicação, notícia, documento, extrato de documento, fotografia, gravação, relato, denúncia, dentre outros, ainda não submetida, pelo profissional de ISP, à metodologia de Produção de Conhecimento" (BARRETO, WENDT e CASELLI, 2017, p. 17).

Portanto, verifica-se que o campo de atuação de uma fonte é vasto, devendo o aplicador do direito realizar buscas com grande afinco, tendo por finalidade a utilização destas para auxiliar em suas sustentações como meios de prova para a condenação ou absolvição do indivíduo.

De acordo com o doutrinador, entende-se por Inteligência Digital aquele procedimento que se utiliza da tecnologia com o fim de angariar dados para análise, e por consequência, uma ampla produção de conhecimentos sobre a inteligência aplicada na segurança pública, com a devida criação de provas que darão base as investigações policiais e a responsabilidade civil dos criminosos.

Neste viés, a DNISP traz como classificação sucinta de fontes abertas e fechadas, sendo as abertas aquelas tidas como livres, e de fontes fechadas as que são protegidas.

Diante de todo conteúdo acima elucidado, necessário se faz esclarecer que a obtenção de dados pode se dar por dois meios: a sistema humano e o sistema eletrônico, que neste trabalho serão elucidados com a finalidade de demonstrar a ambiguidade que eles trazem, pois podem servir de canal para o crime e para a solução destes, mesmo que pouco explorado.

ISSN 2318-0633

2.5 A INTELIGÊNCIA HUMANA E ELETRÔNICA COMO FONTES

O ser humano é dotado de sentimentos, que transparecem através de suas atitudes, e, por consequência, acabam deixando rastros de sua ação. Portanto, a localização de vestígios humanos para coleta de provas torna-se ainda mais fácil.

Nas palavras Barreto, Wendt e Caselli (2017, p. 37),

> O analista não necessita mais de vários dias para conseguir um dado útil. Basta apenas um simples acesso à web! Quem nunca postou alguma informação, dado ou fotografia na web? Para ser bem-sucedido, o profissional responsável pela coleta deve compreender um dos processos mais complexos da gestão de ativos – a natureza humana (BARRETO; WENDT; CASELLI, 2017, p. 37)..

Em outras palavras, vislumbra-se a facilidade que o profissional analista tem ao dominar os sistemas de redes, desta forma, através da coleta de dados deste meio é possível auferir provas que auxiliarão o judiciário em sua tomada de decisão. Por sua vez, este processo para a localização de dados através do próprio ser humano, denomina-se HUMINT (sigla para *Human Intelligence*), e que se bem explorada, trará grandes resultados em processos de investigações policiais.

Também citada por Barreto, outra fonte a ser explorada é a Inteligência Eletrônica (INTEL) que traz como base o próprio equipamento, ou seja, a depender do tipo de dispositivos tem-se diferenciados meios de captação de elementos, como é caso da Inteligência de Sinais, Dados e Imagens, citando que "(...) a leitura desses dados, sejam sinais eletrônicos, sejam imagens, vídeos ou dados derivados do meio eletrônico e digital, é extremamente importante para o profissional responsável de determinado caso". (BARRETO, WENDT e CASELLI, 2017, p. 37).

2.6 A INTELIGÊNCIA DE IMAGENS E DE DADOS

A Inteligência de Imagens (IMINT) soma-se ao grupo de fontes através da coleta de imagens processadas pelos mais diversos meios, a fim de convertê-las em instrumento probatório. Neste meio, podem ser citados como exemplos os satélites, os *sites*, os radares, os sensores, dentre outros.

Na opinião de Barreto, Wendt e Caselli (2017), não há mais a necessidade de deslocamento para a captação de imagens, pois o Google Street View, por exemplo, e os demais sites relacionados a mapas, informam em tempo real imagens de qualquer local do Brasil e do mundo.

Através desta breve classificação, nota-se a importância destas fontes para o desenrolar de um processo justo, pois ao anexar imagens ao processo, fica ainda mais evidente a caracterização do direito pleiteado e a sua concessão ou não ao sujeito que o invocou.

Por sua vez, há também a fonte de Inteligência de Dados, que ganhou grande repercussão com a promulgação da Lei de Interceptação Telefônica de n. 9.296/96 (BRASIL, 1996), tornando possível, entre outras, a interceptação de sistemas de informática.

A legalização deste instituto trouxe grande êxito na localização e punição de sociedades criminosas, auxiliando de forma memorável nas investigações policiais. Nesse sentido, elencaram Barreto, Wendt e Caselli (2017, p. 39):

> Os dados telemáticos são transmitidos de alguma forma, seja por cabeamentos, seja por sinal wireless, por exemplo. Embora possa ser uma miscelânea de situações de irregularidades na formação da rede de Internet no Brasil e no mundo, ela é bastante nova e tende a ser regulamentada, tanto por leis quanto por decretos.

Neste sentido, pode-se perceber que a era digital trouxe significativos benefícios a área probatória do Processo Penal, pois facilitou a adequação e conveniência das fontes, de uma forma clara, precisa e rápida para o aplicador do direito, mas infelizmente vem sendo pouco utilizada para combater crimes cibernéticos, assunto a ser mais explorado adiante.

2.7 COMO ANGARIAR E PRESERVAR PROVAS DO CRIME VIRTUAL

Ao contrário do que muitos pensam, há a possibilidade da própria vítima conservar as evidências do crime praticado contra ela, facilitando o trabalho dos investigadores na busca da responsabilização penal do indivíduo.

Cassanti (2014) elenca uma série de atitudes a serem tomadas que levarão ao êxito probatório no momento da investigação e da instrução processual. Em primeiro momento, deve-se buscar salvar em uma mídia (*pen-drive*, CD ou DVD, por exemplo), arquivos, e-mails, telas, páginas, ou qualquer outra forma de evidência que possa ser útil.

ISSN 2318-0633

Após a coleta de dados, é necessário que todo o conteúdo recolhido passe a ter mais validade jurídica, isto pode der feito através da ata notarial, no qual o tabelião ou preposto comprova a validade e as informações da prova, dando a ela fé pública, podendo ser mantido em lugar seguro, apropriado e sem data de validade em qualquer Tabelionato de Notas ou Registro Civil Cumulado com notas, sem a exigência de demais formalidades ou representação (CASSANTI, 2014).

Por fim, nunca se deve esquecer de registrar um Boletim de Ocorrência. A maioria dos Estados já denotam de delegacias especializadas em crimes virtuais, e ao comparecer a localização física pode ser que a vítima seja encaminhada a uma plataforma online para a prestação de sua ocorrência.

Segundo Cassanti (2014), outro meio eficaz para constituição de prova sólida é a identificação do criminoso através de seu IP, o número que identifica seu computador. Porém, este procedimento deve ser efetuado após uma solicitação de quebra de sigilo telemático feita pela polícia federal.

2.8 VALIDADE JURÍDICA DAS PROVAS COLHIDAS NO SISTEMA DE REDES

Quando o assunto é prova, muitos não sabem especificar a validade delas quando adquiridas por meios eletrônicos. Por esse motivo, cabe esclarecer que o judiciário já se manifestou no sentido de que, quando se tratar de provas colhidas através de site oficial, somente poderá ser invalidado se o órgão expedidor da informação assim o fizer, tornando-se de validade plena se certificada digitalmente.

Portanto, assim como citam Barreto, Wendt e Caselli (2017), a Lei n. 6.015/73 de Registros Públicos deve ser observada, pois ela quem trará os requisitos e características para que a prova tenha plena eficácia.

Outra lei que vale ser citada é a de nº 5.433/68, conhecida como a Lei de Microfilmagem. Ao observá-la e fazer um paralelo entre o Código de Processo Civil e o Código de Processo Penal, verifica-se que estes exigem, concomitantemente a utilização da foto negativa, quando esta for objeto de prova no processo, mas atualmente, com a modernização do meio, é um raciocínio lógico dizer que provas digitais serão aceitas, visto que não possuem as negativas, ademais, não necessitam.

O que o legislador quis confirmar através desta e de outras formalidades, na visão de Barreto, Wendt e Caselli (2017), é a necessidade da validação desta prova digital, a fim de que sua essência seja preservada, através de auditoria, perícia ou fé pública por meio do tabelião. O importante é preservar sua essência e verificar que todos os procedimentos para sua conservação foram observados, visto que não há previsão legal que proíba este meio de prova.

Os artigos 231 e 231, parágrafo único do Código de Processo Penal preceituam:

> Art. 231. Salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo.
> Art. 232. 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.

Portanto, é expressa a admissão de todos os meios legais de provas, exceto as ilícitas, cabendo ao julgador apreciar a prova em conjunto com o processo, e aferir a ela seu valor devido.

3. CONSIDERAÇÕES FINAIS

Olhando por vários ângulos, pode-se concluir que o sistema de redes pode ser utilizado tanto para o crime virtual, quanto para comprobação deste e dos demais praticados fora da *internet*. Portanto, quando bem utilizada, essa ferramenta pode trazer grandes benefícios para o sistema processual, pois os meios interligam-se e formam um bojo de conteúdo probatório extenso e que, se utilizado, clareia as vistas tanto do defensor, quanto do acusador.

Como dantes foram tratados dos delitos mais comuns praticados na *internet*, neste momento, para conclusão do trabalho, necessária se faz a numeração de alguns meios para a prevenção de ser o alvo destes crimes.

O próprio Governo Federal vislumbrando a necessidade de tratar este problema social, publicou uma cartilha no Portal Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), em que poderão ser encontradas várias dicas de prevenção.

Além de adquirir o devido conhecimento sobre o assunto, é necessário que o computador do usuário esteja sempre protegido. Os dados de um levantamento feito pela companhia de segurança digital McAfee, e publicados na obra Crimes Virtuais, Vítimas Reais (CASSANTI, 2014), no

ISSN 2318-0633

Brasil, 16% dos computadores não estão protegidos com antivírus contra ameaças virtuais e vírus, tornando-se presas fáceis nas mãos de *hackers*.

Todo o cuidado é pouco no momento de realizar compras na *internet*, além do navegador estar devidamente protegido, deve-se verificar a procedência dos sites e evitar colocar o número do catão ou senha de banco em endereços eletrônicos desconhecidos ou com procedência duvidosa, cuidando sempre com os *downloads*, e-mails, e demais arquivos a serem baixados no computador, e claro, sempre agir com bom senso, que é o detector de ameaças instalado em nossa consciência.

REFERÊNCIAS

BARRETO, A. G. B; WENDT, E.; CASELLI, G. **Investigação Criminal em Fontes abertas.** 2.ed. São Paulo: Brasport, 2017.

BRASIL, Decreto-lei n. 3.689 de 3 de outubro de 1941. **Código de Processo Penal.** Disponível em: <http://http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 16 de maio 2018.

_____. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 20 ago. 2017.

_____. Decreto-lei n. 2.848, de 7 de dezembro de 1940. **Código Penal.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 20 ago. 2017.

_____. Lei n° 5.433, de 8 de maio de 1968. **Regula a microfilmagem de documentos oficiais e dá outras providências**. Disponível em <http://www.planalto.gov.br/ ccivil_03/Leis/L5433.htm >. Acesso em 20 ago. 2017.

_____. Lei n° 6.015, de 31 de dezembro de 1973. **Dispõe sobre os registros públicos e dá outras providências**. Disponível em <http://www.planalto.gov.br/ccivil_03 /leis/L6015compilada.htm>. Acesso em 20 ago. 2017.

_____. Lei n° 9.296, de 24 de julho de 1996. **Regulamenta o inciso XII, parte final, do Art. 5º da Constituição Federal**. Disponível em <http://www.planalto.gov.br/ccivil_03/ Leis/l9296.htm>. Acesso em 20 ago. 2017.

_____. Lei n°10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/2002/l10406.htm>. Acesso em 20 ago. 2017.

_____. Lei nº 7.716, de 5 de janeiro de 1989. **Define os crimes resultantes de preconceito de raça ou de cor**. Disponível em < ttp://www.planalto.gov.br/ccivil_03/Leis/L7716.htm>. Acesso em 20 ago. 2017.

_____. Lei nº 9.279, de 14 de maio de 1996. **Regula direitos e obrigações relativos à propriedade industrial**. Disponível em <http://www.planalto.gov.br/ccivil_03/ Leis/l9279.htm>. Acesso em 20 ago. 2017.

_____. Lei nº 9.609, de 19 de fevereiro de 1998. **Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências**. Disponível em <http://www.planalto.gov.br/ccivil_03/LEIS/L9608.htm>. Acesso em 20 ago. 2017.

CASSANTI, M. O. **Crimes Virtuais, Vítimas Reais.** 1.ed. São Paulo: Brasport, 2014.

FERREIRA, I. S. A Criminalidade Informática. In: LUCCA, N.; SIMÃO FILHO, A. (Org.). **Direito e Internet**: Aspectos Jurídicos Relevantes. 1.ed. São Paulo: Edipró, 2001. cap. 7, p. 207-237.

GRECO, R. **Curso de Direito Penal.** 4.ed. Rio de Janeiro: Impetus, 2008.

JESUS, D. **Direito Penal**: Parte Geral. 32.ed. São Paulo: Saraiva, 2013.

NUCCI, G. S. **Manual de Direito Penal.** 4.ed. São Paulo: Revistas dos Tribunais, 2008.

OLIVÁN, M.C. Para o Estado: Rede: globalização econômica e instituições políticas na era da informação. In: PEREIRA, L. C. B.; WILHEIM, J.; SOLA, L. (Org). **Sociedade e Estado em Transformação**. 1.ed. Brasília: UNESP, 1999. cap. 5, p. 150-151.

PINHEIRO, P. P. **Direito Digital.** 4.ed. São Paulo: Saraiva, 2010.

ISSN 2318-0633