DIÁLOGOS E INTERFACES DO DIREITO

REVISTA CIENTÍFICA DO CURSO DE DIREITO
CENTRO UNIVERSITÁRIO FAG

CIBERCRIMES E A LEGISLAÇÃO BRASILEIRA

LORENZO, Larissa Papandreus.[1]
SCARAVELLI, Gabriela Piva.[2]

RESUMO

Este artigo tem por objetivo abordar os elementos referentes aos crimes cibernéticos, bem como as modificações que surgiram no Código Penal brasileiro e as consequências que o advento da tecnológica causou ao cenário jurídico. Busca analisar se as leis brasileiras existentes são capazes de amparar as vítimas do meio informatizado, o *modus operandi* utilizado pelos cibercriminosos, uso do anonimato para consumação do delito e a dificuldade de identificação. Este trabalho dá enfoque na possível análise do local do crime, e qual a competência jurídica para o julgamento, tendo em vista as dificuldades para sua percepção devido ao uso do anonimato e a facilidade de atingir diversas vítimas em variados locais, com apenas uma conduta. E ainda, discorrerá acerca de como o cenário internacional lida com tais circunstâncias, como no caso de convenções internacionais. Os meios metodológicos utilizados foram pesquisa bibliográfica, jurisprudencial, em leis e artigos jurídicos.

PALAVRAS-CHAVE: Direito digital, Cibercrime, Legislação brasileira.

CYBERCRIMES AND BRAZILIAN LAW

ABSTRACT

This article aims to address the elements related to cybercrimes, as well as the changes that arose in the Brazilian penal code and the consequences that the advent of technology has caused to the legal scenario. It seeks to analyze whether existing Brazilian laws are capable of sustaining the victims of the computerized environment, the modus operandi used by cybercriminals, the use of anonymity to consummate the crime and the difficulty of identification. This essay focuses on the possible analysis of the crime scene and what is the legal competence for the jugding in view of the difficulties for its perception due to the use of anonymity and ease of reaching several victims in various locations with only one conduct. Furthermore, it sought to discuss how the international scenario deals with such circumstances as in the case of international conventions. The methodological means used were bibliographical, jurisprudential research, in laws and legal articles

KEYWORDS: Digital law, Cybercrime, Brazilian law.

1 INTRODUÇÃO

Os crimes virtuais ou cibercrimes surgem como um mal moderno e cada vez mais dominante na sociedade atual, encontrando-se altamente dependente de tecnologias e das redes sociais. Com o surgimento da tecnologia e o advento da internet, surgiram novas espécies delitivas, com novas formas de se praticar crimes já existentes, foram tipificadas novas condutas criminosas, cujos crimes são praticados no meio virtual. O fato é que criminosos se aproveitam de um novo mundo, virtualmente construído, para cometer delitos graves e, tão danosos, quanto os crimes não virtuais.

[1]Acadêmica do curso de Direito do Centro Universitário – FAG. e-mail: larissa.aguiar@hotmail.com
[2]Docente orientadora do curso de Direito do Centro Universitário – FAG. e-mail: gabrielapivapiva@hotmail.com

Dada a relevância do tema, o enfoque deste artigo é analisar a evolução dos cibercrimes e a dificuldade da aplicação da legislação brasileira.

Os crimes virtuais tratam de condutas típicas e ilícitas praticadas por intermédio da internet com a intenção de se obter alguma vantagem indevida, tendo por objeto material ou meio de execução a rede virtual.

A internet se tornou o meio de comunicação mais utilizado dos últimos tempos, a sua popularização se deu entre os anos 80 e 90, e a partir disso, iniciaram-se os registros de crimes virtuais. Trata-se de um meio rico de informações e de fácil acessibilidade, trazendo, então, grandes impactos na seara do Direito. À vista disso, o Direito Digital busca uma harmonização entre a relação jurídica e o meio virtual para que haja uma responsabilização do autor pelos danos gerados.

Não há muitas legislações específicas, por isso, faz-se necessário o diálogo entre os ramos do direito, sendo eles, Penal, Processo Penal, Civil, Consumidor, tal como convenções internacionais, para que haja uma maior amplitude e proteção.

Ressalta-se que há uma grande instabilidade dos crimes virtuais, tendo em vista que qualquer ato pode ser rapidamente apagado e alterado, havendo assim, a ausência de provas contra o autor do crime e dificuldade quanto a sua identificação, ocasionando obstáculos na atuação policial perante tais casos. Os crimes cibernéticos são peculiares desde sua autoria e materialidade como na tipificação de seus institutos.

Destarte, é importante verificar se a atual legislação brasileira seria capaz de reduzir a ascensão dos cibercrimes e a possível forma para o combate. Há algumas legislações específicas que inovaram o cenário jurídico, como por exemplo, a lei 12.737/12 e a lei 12.965/14, que serão estudadas a seguir. Todavia, existem muitas lacunas, o que faz com que diversas condutas não sejam passíveis de punição ou então tipificadas de forma incompleta, causando uma dificuldade no combate efetivo dos cibercrimes. Os crimes cometidos em razão da tecnologia criptografada são de preocupação internacional, e trata-se de um problema comum a todos, necessitando da harmonia e união entre demais países interessados no combate e proteção.

Logo, busca-se fazer uma análise criteriosa sobre o tema Direito digital, como são praticados os crimes virtuais, e esclarecer possibilidades de aplicação do ordenamento jurídico diante do novo e moderno cenário de situações jurídicas. Além de delimitar a competência territorial para julgamento dos cibercrimes.

Os meios utilizados para a elaboração deste artigo são: pesquisas jurisprudenciais, doutrina, demais artigos jurídicos envolvendo o tema supracitado, convenções internacionais e a legislação brasileira.

2 CIBERCRIME

2.1 DIREITO DIGITAL

A respeito do tema Direito Digital, Pinheiro (2016) compreende que é a evolução do próprio Direito em si, e são os atuais profissionais do Direito que devem zelar por proteções, como por exemplo, o direito à imagem, à proteção do direito autoral, da segurança de informação, dos processos contra os hackers. Dessa forma, o Direito Digital é o responsável por estudar e criar os instrumentos que serão capazes de atender a esses anseios. Sendo assim, os atuais operadores do Direito, costumeiros por estarem inseridos em uma era informatizada e online, devem acompanhar essa evolução, e, cada vez mais, aprimorar-se no tema.

Conforme Alves (2009), compreende-se o Direito Digital como o resultado do Direito com a Ciência da Computação, advindo da tecnologia e do atual meio digital em que estamos presentes, consequentemente, faz-se necessário a garantia da validade jurídica das informações, transações e uso de certificados digitais. Para uma maior precisão na busca dos autores e da materialidade dos delitos praticados no meio virtual, é indispensável a união de ambas as áreas para observar a forense computacional.

No meio digital se tem rápidas transformações, o que acarreta em uma maior dificuldade para legislação, visto que qualquer que seja a lei que passe a tratar de um instituto jurídico novo, esta deve ser genérica o suficiente para suportar a flexibilidade e diversos formatos que possam vir a surgir de um único assunto. Por isso, o Direito digital aplica dentro de uma lógica jurídica um conjunto de princípios e soluções que são aplicados de modo difuso, este conhecido, como Direito Costumeiro, para que então possa se preencher lacunas. No Direito Costumeiro há uma série de elementos que amparam o Direito Digital, como a generalidade, uniformidade, continuidade, durabilidade e a notoriedade (PINHEIRO, 2016).

Conforme entendimento de Pinheiro, entende-se quais são as características do Direito Digital:

> As características do Direito Digital, portanto, são as seguintes: celeridade, dinamismo, autorregulamentação, poucas leis, base legal na prática costumeira, o uso de analogias e solução por arbitragem. Esses elementos tornam muito semelhante a *Lex Mercatoria*, uma vez que ela não está especificadamente disposta em um único ordenamento, tem alcance global e se adapta as leis internas de cada país de acordo com as regras gerais que regem as relações comerciais e com princípios universais do Direito como a boa – fé (PINHEIRO, 2016, p.82).

Por conseguinte, o Direito Digital é uma extensão e inovação do Direito, que está em ascensão no meio jurídico, este por sua vez, interliga a comunicação do sujeito com a era informatizada. A celeridade e popularidade que a internet propõe fez com que muitos atos físicos fossem substituídos pelos virtuais.

2.2 CRIMES VIRTUAIS / CIBERCRIMES

Os crimes virtuais surgiram e se desenvolveram ao mesmo passo do surgimento da internet, e vêm se aprimorando com o passar dos anos, tendo como objetivo, sempre, trazer prejuízos a outros usuários. Também chamados de eletrônicos ou cibernéticos, são aqueles cometidos utilizando-se de um espaço fictício, criado a partir de uma rede mundial, em sua maioria, de computadores, a Internet, onde o agente não necessariamente comete o delito em um território, nem a vítima, necessariamente, precisa ser abordada fisicamente (MIRANDA, 2013). De acordo com Palazzi, crime virtual significa:

> Qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados. Essa criminalidade apresenta algumas características, entre elas: transnacionalidade (veiculada virtualmente, todos os países têm acesso e fazem o uso da informação), universalidade (é um fenômeno de massa e não de elite) e ubiquidade (está presente nos setores privados e públicos) (2014, p. 54).

Conceituando crimes virtuais, Rossini (2004) destaca a denominação como delitos informáticos como de maior amplitude, envolvendo toda e qualquer conduta que guarde relação com os sistemas informáticos, não precisando, obrigatoriamente, que o crime tenha ocorrido na internet para a tipificação. Em suas palavras:

> A denominação “delitos informáticos” alcança não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas

> informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta sem imprescindível "conexão" à Rede Mundial de Computadores, ou qualquer outro ambiente telemático. Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da internet, também seria alcançada pelo que se denominou "delitos informáticos" (ROSSINI, 2004, p. 110).

Nos crimes virtuais, o computador ocupa lugar de destaque e, na maioria dos casos, é o meio utilizado para a prática dos delitos. Pode-se dizer, dessa forma, que este é o instrumento para a prática do crime virtual. Entretanto, o computador pode vir a ser um alvo ou, penalmente falando, o objeto danificado de uma vítima.

Além disso, são poucas as legislações específicas acerca do tema, Jesus e Milagre (2016) afirmam que há uma insegurança jurídica em questão de tecnologia, havendo, desse modo, riscos para a sociedade, ficando os indivíduos vulneráveis a criminalidade virtual. O Brasil está na 4ª posição de países com maior número de ameaças virtuais.

Uma das maiores preocupações que englobam os crimes virtuais é a facilidade do sujeito ativo na prática de seu crime, visto que este pode atingir centenas de vítimas de diferentes países, sem sequer sair de sua casa, além de muitas vezes poder optar pela forma de anonimato. Os crimes são variados, dentre eles cita-se o estelionato, invasão de privacidade, contrabando e até mesmo pornografia infantil.

Conforme Jesus e Milagre (2016), o perfil para do criminoso virtual brasileiro é mais criativo do que técnico, em vista disso, constantemente, os crimes ocorrem pela falta de educação online dos sujeitos passivos, bem como o despreparo das autoridades investigativas.

2.3 CLASSIFICAÇÃO DOS CRIMES VIRTUAIS/ CIBERCRIMES

São dos mais variados as nomeações dos delitos cometidos no meio virtual, e há necessidade de classificar as tipificações desses crimes. Vale ressaltar que existem várias classificações doutrinárias, sendo, portanto, amplamente discutido pelos autores.

Para Jesus e Milagre (2016), são quatro as classificações referentes aos crimes informáticos. Sendo que estes podem ser próprios, em que a própria tecnologia de informação é o bem jurídico ofendido; impróprio, no qual a tecnologia da informação é o meio que se utiliza para a prática dos

crimes que atinjam bens jurídicos tutelados pelo Código Penal Brasileiro; os crimes informáticos mistos, que dizem respeito aos crimes complexos, ou seja, além do bem jurídico do meio informatizado, a legislação também protege outros bens jurídicos; e por fim, o crime informático mediato ou indireto, em que pese se trata de delitos informáticos praticados para consumação de um delito não informático.

Para Higor Vinicius Nogueira Jorge (2012) e Emerson Wendt (2012), a classificação fica em ações prejudiciais atípicas e os crimes cibernéticos. As ações prejudiciais atípicas podem ser entendidas como condutas que causam transtorno para vítima através do meio digital, porém, não há tipificação na legislação. E os crimes cibernéticos, por sua vez, podem ser subdivididos em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos", sendo que este último faz parte dos crimes que necessitam do meio digital informático para concretização do crime (como por exemplo, o caso do crime descrito na Lei Carolina Dieckmann, crime de invasão de dispositivo informático). Dessa forma, os crimes cibernéticos abertos possuem a faculdade de serem praticados pelo meio digital informático, como os crimes de violação de direito do autor.

Já para Teixeira (2014), há três classificações que podem ser entendidas como puros, mistos e comuns. O puro é aquele em que o sujeito visa o sistema de informação em si, como por exemplo, deteriorar o próprio sistema de computação; já o misto utiliza-se necessariamente do sistema de informática para atingir um bem jurídico diverso; e por fim, os comuns, em que o sistema é um mero auxílio, mas não é imprescindível para que haja a consumação do delito.

2.4 IDENTIFICAÇÃO DO SUJEITO ATIVO

Por sujeito ativo pode-se entender que é aquele que cometeu o ilícito penal, habitualmente no meio virtual o sujeito ativo é conhecido como "Hackers". Para Marcelo Crespo (2011):

> A definição dada, por um hacker, a tal palavra é no sentido daquele que invade sistemas em benefício próprio, obtendo dados e informações alheias (documentos, programas, músicas etc.), mas sem danificar nada. São milhares os sites na internet que se intitulam hackers e muitos deles oferecem definições dessa terminologia. A definição mais aceita é que hacker é qualquer um que tenha grande conhecimento sobre computadores e faça invasões.

A identificação do sujeito passivo via de regra é fácil, visto que é a própria vítima. A problemática está em identificar o sujeito ativo, tendo em vista a facilidade em se ocultar. Para chegar ao sujeito passivo é necessário identificar o número do protocolo de comunicação da internet (conhecido como IP), para Pedro Pisa (2012) "*O IP (Internet Protocol) é o principal protocolo de comunicação da Internet. Ele é o responsável por endereçar e encaminhar os pacotes que trafegam pela rede mundial de computadores".*

À vista disso, se o protocolo for identificado, é possível que se localize o local acessado pelo cibercriminoso.

2.5 LEGISLAÇÕES ESPECÍFICAS PARA TIPIFICAÇÃO DOS CRIMES VIRTUAIS/ CIBERCRIMES/ CIBERCRIMES

Um dos maiores problemas acerca do tema é a adequação da legislação pátria diante os crimes virtuais, todavia, no ano de 2012, foram sancionadas duas leis que tipificam sobre os crimes online, a lei 12.735/12 e a lei 12.737/12, as quais alteraram o Código Penal e possibilitaram maior aplicabilidade de punições para os delitos. Dessa maneira, foi possível instituir penas para diversos cibercrimes, como invasão de computadores, disseminação de vírus ou códigos para roubos de senhas e o uso de cartões de crédito e débito sem a devida autorização do titular. Não obstante, em 2014 passou a vigorar a lei 12.965/14, conhecida como Marco Civil da Internet (BRASIL, 2012).

2.5.1 Análise da lei 12.735/12

A lei 12.735, de 30 de novembro de 2012, tipifica os crimes cometidos com o uso de sistema eletrônico, digital ou similar, dessa forma, os órgãos da polícia judiciária deverão estruturar setores especializados para combater a ação delituosa em rede de computadores, dispositivos de comunicação ou sistema informatizado (BRASIL, 2012).

Todavia, a lei apenas dispõe em seu texto a cooperação de órgãos públicos, nada dispondo sobre iniciativa particular. Conforme Jesus e Milagre :

> A lei estabelece em seu artigo 4º a possibilidade da polícia judiciária estruturar órgãos especializados no combate à ação delituosa em redes de computadores, dispositivos de

> comunicação ou sistemas informatizados. Nada fala em relação à cooperação da iniciativa privada, muito utilizada, por exemplo, nos Estados Unidos (JESUS e MILAGRE, 2016, p.77).

Ressalta-se que a presente lei alterou o Decreto - Lei nº 2.848 de 7 de dezembro de 1940 – Código Penal, e o Decreto- Lei nº 1.001 de 21 de outubro de 1969 – Código Militar, bem como trouxe alterações na Lei 7.716 de 5 de janeiro de 1989. Dentre as alterações, o artigo 5º alterou o inciso II do §3º do art. 20, da lei 7.716 de 5 de janeiro de 1989, e passou a ter a seguinte redação :

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência Nacional.
> Pena: reclusão de um a três anos e multa
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza
> Pena: reclusão de dois a cinco anos e multa.
> § 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência:
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio (BRASIL, 2012).

É a mais específica legislação sobre crimes digitais que se encontra em nosso ordenamento Legislativo, a qual determina que sejam instaladas delegacias especializadas capazes de ampliar a proteção e o amparo à sociedade.

2.5.2 Análise da lei 12.737/12

A lei 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, dispõe sobre a tipificação criminal de delitos informáticos, ela ganhou grande relevância na mídia devido ao caso da atriz que teve suas fotos íntimas vazadas em diversos sites eletrônicos pelo mundo todo. A referida lei acrescentou ao Código Penal os artigos 154 – A e 154 – B, bem como alterou os artigos 266 e 298 do mesmo Códex (BRASIL, 2012).

Conforme o Promotor de Justiça Ishida (2012), o artigo 154- A trouxe para o ordenamento jurídico o crime de “Invasão de Dispositivo Informático”, com a seguinte redação :

> **Art. 154**-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter,

> adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 2012).

Os crimes de "invasão de dispositivos informáticos" são os com punições mais brandas, as penas são de três meses a um ano de prisão e multa, já condutas mais severas, como obter pela invasão, contéudos de comunicações eletrônicas privadas e informações sigilosas, a pena pode variar de seis meses a dois anos de prisão, além de multa, incorre na mesma pena caso o delito envolver a divulgação e comercialização à terceiros, através de vendas ou repasse gratuito do conteúdo obtido com a invasão da privacidade, podendo a pena, neste último caso, ser elevada de um a dois terços (BRASIL, 2012).

O artigo 154 – B, por sua vez, afirma que os crimes definidos no artigo 154- A se procederão mediante representação, ou seja, ação pública condicionada. Porém, caso o crime seja cometido contra a administração pública direta ou indireta, de qualquer dos poderes da União, Estados e Distrito Federal ou Município ou contra empresas concessionárias de serviços públicos, a ação será pública incondicionada (BRASIL, 2012).

> **Art. 154**-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de servicos públicos (BRASIL,2012).

Além do mais, a lei trouxe alterações em dois artigos, o artigo 266 do Código Penal, incluindo o serviço telemático ou de informação de utilidade pública, e o artigo 298 do mesmo códex, em que se equiparou a documento particular o cartão de crédito ou de débito.

Conforme Paganotti (2013), até o ano de 2012, não havia no Brasil legislações que versavam sobre crimes cibernéticos, os magistrados se utilizavam do próprio Código Penal para tipificação, causando decisões contraditórias.

A lei 12.737/12 inovou ao trazer para o ordenamento jurídico novas tipificações acerca da Invasão de Dispositivo informático, a legislação foi oriunda de um projeto já existente no Congresso Nacional, mas devido a repercussão social que o caso da atriz trouxe, houve maior agilidade a rapidez na promulgação do sancionamento.

2.5.3 Análise da lei 12.965/14

A lei 12.965 de 23 de abril de 2014, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, e determina as diretrizes para atuação da União, Estados, do Distrito Federal e dos Municípios em relação à matéria (BRASIL, 2014).

Nos entendimentos de Araújo (2017), há conformidade da lei com a própria Constituição Federal, visto que trata de individualidade humana, bem como a privacidade e dignidade, busca sempre o bem comum e igualdade, garantindo a todos o direito à rede de internet. A liberdade de expressão, o direito à intimidade e privacidade estão em ênfase no Marco Civil, como cita Araújo:

> Como já observado acima, a preservação do direito à intimidade e à privacidade mereceu a devida salvaguarda no artigo 10 e seus parágrafos da Lei 12.965/2014, pelo que comunicações privadas transmitidas na Internet não podem ser divulgadas pelos provedores, salvo mediante ordem judicial (ARAÚJO, 2017, p.93).

O artigo 3º da lei estabelece os princípios do Marco Civil da internet, que disciplina o uso da internet no Brasil, dentre eles, vale ressaltar os principais, que são a garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; e a proteção à privacidade (BRASIL, 2014).

No artigo 7º do Marco Civil encontra-se os direitos dos usuários, como por exemplo, a inviolabilidade da intimidade e da vida privada, tal como a sua proteção pelo dano material ou moral decorrente de sua violação. Há também o direito de não fornecimento à terceiros de dados pessoais, salvo mediante consentimento livre, expresso e informado ou então nas hipóteses previstas em lei. (BRASIL, 2014).

Por esse motivo, os provedores que possibilitam o acesso de seus usuários com o meio digital, devem respeitar a privacidade de dados e registros, como exemplo de provadores do Brasil, pode-se citar a Embratel. Pinheiro (2010) afirma que os provedores são mais do que empresas que portam serviços, eles são responsáveis pela entrada dos usuários a rede, sendo, portanto, uma empresa relacionada à área de telecomunicação de grande importância.

Diante disso, o Marco Civil da Internet visa principalmente proteger a privacidade de todos, foi um avanço na neutralidade da rede, trazendo uma inovação, o qual apenas mediante ordem judicial poderá haver a publicação de dados de cada usuário existente em sites ou em redes sociais, o mesmo

se aplica à retirada de contéudo do meio virtual, com exceção as vítimas de violações de suas intimidades, pois estas podem de forma direta solicitar a retirada do conteúdo impróprio.

2.5.4 Análise da lei 13.718/ 2018

A legislação 13.718/2018 introduziu modificações nos crimes contra a dignidade sexual, como a importunação sexual e divulgação de cena de estupro, fazendo com que a natureza da ação penal de tais crimes se torne pública incondicionada (BRASIL 2018).

Introduziu no Código penal o artigo 218- C, o qual dispõe sobre os crimes de divulgação de cena de estupro/cena de estupro de vulnerável, cenas de apologia ao estupro e cena de sexo ou de pornografia:

> **Art. 218**-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia (BRASIL 2018).

Essa, por sua vez, foi mais uma inovação no ordenamento jurídico em tutela do bem jurídico que foi violado, qual seja a divulgação das cenas do estupro ou vídeos e fotos íntimas divulgadas, criminalizando a exposição íntima que não fora consentida. Conforme Oliveira e Andrade (2016), antes da criação do artigo, casos de exposição íntima sem consentimento eram tratados muitas vezes como calúnia e difamação, configurando crimes de ação privada.

2.6 TERRITORIALIDADE

Para Erik Ferreira (2016), a necessidade de combater os cibercrimes diz respeito à territorialidade/extraterritorialidade, é sabido que há mecanismos de investigações como a Interpol em seus sistemas de investigações, mas tendo em vista que há uma grande facilidade do autor do crime ocultar sua identificação, gerando uma grande dificuldade para os setores, como é o caso de

um criminoso que consegue de um país atingir a máquina de outro país, utilizando-se de um servidor que se encontra em um terceiro país.

O artigo 5º do Código Penal dispõe que se aplica a legislação brasileira, sem prejuízo das convenções, tratados e regras de Direito Internacional ao crime praticado no território nacional, desse modo, adota-se a teoria da territorialidade temperada, onde o Brasil, em respeito a cooperação internacional, abre uma lacuna no que se refere a sua exclusividade (BRASIL 1940).

O Código Penal Brasileiro adota a teoria da ubiquidade para determinar o lugar do crime, ela está prevista no artigo 6º do Código Penal: " Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". Assim, adota-se a regra do Código Penal (teoria mista ou da ubiquidade), tratando-se de crimes a distância, que são os que a conduta criminosa é praticada em um país e o resultado se produz em outro, como ocorre nos conflitos de Direito Penal internacional (BRASIL 1940).

Já em relação à competência, está prevista no artigo 70 do Código de Processo Penal, e define a competência pelo local em que houve a consumação ou no caso de tentativa, o local onde se praticou o último ato de execução (BRASIL 1940).

No entanto, a rede de internet possui um caráter internacional e está ao mesmo tempo em todo mundo, dificultando a identificação do local onde ocorreu o crime, não obstante, o autor dificilmente utiliza seu computador pessoal, além de utilizar contas usuárias falsas para a prática do delito.

Com a inovação do assunto, a jurisprudência dos Tribunais Superiores vem cada vez mais se consolidando em julgados para tratar de casos no âmbito digital. Como exemplo, tem-se o julgado a respeito do conflito de competência praticado por meio de redes sociais.

> Conflito de competência. Crime de ameaça praticado por whatsapp e facebook. Âmbito de aplicação da lei maria da penha. Delito formal. Consumação no local onde a vítima conhece das ameaças. Conflito de competência conhecido. Declarada a competência do juízo suscitado. 1. O crime de natureza formal, tal qual o tipo do art. 147 do Código Penal, se consuma no momento em que a vítima toma conhecimento da ameaça. 2. Segundo o art. 70, primeira parte, do Código de Processo Penal, "A competência será, de regra, determinada pelo lugar em que se consumar a infração". 3. No caso, a vítima tomou conhecimento das ameaças, proferidas via Whatsapp e pela rede social Facebook, na Comarca de Naviraí, por meio do seu celular, local de consumação do delito e de onde requereu medidas protetivas. 4. Independentemente do local em que praticadas as condutas de ameaça e da existência de fato anterior ocorrido na Comarca de Curitiba, deve-se compreender a medida protetiva como tutela inibitória que prestigia a sua finalidade de prevenção de riscos para a mulher, frente à possibilidade de violência doméstica e familiar. 5. Conflito conhecido para declarar a competência do Juízo da 1º Vara Criminal da Comarca de Naviraí/MS, ora suscitado. (STJ - CC: 156284 PR 2018/0008775-5, Relator:

> Ministro RIBEIRO DANTAS, Data de Julgamento: 28/02/2018, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 06/03/2018).

O relator ministro Ribeiro Dantas, ao julgar o conflito de competência do caso exposto, utilizou-se do artigo do Código de Processo Penal e estabeleceu que em regra a competência será determinada pelo lugar em que se consumar a infração.

No âmbito das fraudes praticadas pela internet, é importante mencionar conflito de competência nº 145.576, julgado pelo Superior Tribunal de Justiça :

> Conflito negativo de competência. Penal e processual penal. Furto mediante fraude. Transferência bancária via internet sem o consentimento da vítima. Consumação no local da agência onde o correntista possui a conta fraudada. Competência do juízo suscitado. 1. A Terceira Seção desta Corte Superior firmou o entendimento no sentido de que a subtração de valores de conta corrente, mediante transferência fraudulenta, utilizada para ludibriar o sistema informatizado de proteção de valores, mantidos sob guarda bancária, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do Código Penal - CP. 2. O delito em questão consuma-se no local da agência bancária onde o correntista fraudado possui a conta, nos termos do art. 70 do Código de Processo Penal - CPP; no caso, na Comarca de Barueri/SP. Conflito de competência conhecido para declarar competente o Juízo de Direito da 1ª Vara Criminal de Barueri/SP, o suscitado. (STJ - CC: 145576 MA 2016/0055604-1, Relator: Ministro JOEL ILAN PACIORNIK, Data de Julgamento: 13/04/2016, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 20/04/2016).

Em relação ao furto mediante fraude, praticado por transferência bancária pela internet, o Superior Tribunal de Justiça decidiu que o delito se consumou no local da agência bancária, onde o correntista fraudado possuía a conta.

2.7 CIBERCRIME SOB UM ASPECTO MUNDIAL

Tendo em vista que para o ordenamento jurídico brasileiro o tema supracitado ainda é novo, e as legislações não amparam todos os crimes virtuais, é importante fazer uma análise na área do Direito Internacional, como no caso de convenções.

2.7.1 Convenção sobre cibercrime

A Convenção sobre Cibercrime, também conhecida como Convenção de Budapeste, foi assinada em 23 de novembro de 2001, e estipula em seu preâmbulo que os Estados signatários com a intenção de unir seus membros e ampliar a proteção dos usuários contra a criminalidade no ciberespaço através da cooperação internacional.

A Convenção de Budapeste (2001) mostra evidente que através de uma cooperação se tenha um resultado mais rápido e eficaz as ações penais relativas a infrações no âmbito digital, visa-se a proteção dos usuários diante do atual cenário tecnológico em que estamos. A Convenção apresenta a intenção de impedir atos ilegais praticados e proteção dos direitos humanos.

Dentre as matérias tratadas na convenção, estão as relacionadas à confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos, infrações relacionadas a computadores, pornografia infantil, violação do direito de autor e direitos conexos (CONVENÇÃO DE BUDAPESTE, 2001).

De acordo com artigo postado por Grossmann (2018), o Ministério Público Federal revelou que o Brasil, até o momento, não é signatário da Convenção de Budapeste, mas apoia a adesão do país. A procuradora geral da República, Raquel Dodge (2018), enviou por ofício seu posicionamento positivo ao Ministério das Relações Exteriores em relação a adesão do Brasil à Convenção. Grosmann (2018) ressalta que o Brasil não é signatário da Convenção de Budapeste por conta de sua tradição diplomática de não aderir a acordos aos quais não foi convidado para discutir os termos.

Por conseguinte, compreende-se que o Brasil até agora não faz parte, contudo, mostra seu interesse em integrar a Convenção. Visto que há muitas omissões legislativas a respeito do tema, a União com demais países mostra-se positiva em relação à eficácia e o combate. Ao aderir a Convenção, o tratamento seria em um âmbito internacional de combate aos crimes digitais, havendo também, uma cooperação com os demais signatários que, igualmente, sofrem com as práticas ilícitas do meio e que possuem legislações distintas das brasileiras.

Sobre o Brasil, somente no ano de 2018, conforme relatório feito pela SafeNet (2019) – associação civil que combate crimes virtuais e a violação dos Direitos Humanos na internet- em parceria com o Ministério Público Federal, o número de cibercrimes cresceu 109,95 % em relação ao ano anterior, foram 133.732 queixas de delitos online, que variam desde ciberbullying, fraudes, golpes até pornografia infantil e incitação à violência.

Conforme relatório final da Comissão Parlamentar de Inquérito (CPI da Espionagem), a qual foi instaurada em 2013 pelo Senado Federal, é notório a fragilidade do Brasil frente a espionagem no meio digital, visto que o país possui baixíssima segurança cibernética, ocasionando dificuldade nos sistemas de defesa cibernética (SENADO FEDERAL, 2013).

.

3 CONSIDERAÇÕES FINAIS

Percebe-se que o Direito vem se moldando e se adequando ao novo cenário dos cibercrimes, o qual encontra diversas dificuldades acerca disso, é notório que a inovação criminológica por hora está bem à frente da legislação nacional e, por essa razão, ainda há muita insegurança no usuário. O Direito precisa acompanhar a evolução da sociedade que está em uma era informatizada, ressalta-se que os avanços tecnológicos tendem a crescer cada vez mais e junto com ele a criminalidade virtual, há uma rapidez na tecnologia enquanto os órgãos repressivos governamentais se encontram lentos.

O Marco Civil da internet (lei 12.965/14) é a mais ampla legislação em relação ao tema, foi um grande avanço para o usuário da internet, visto que tutela direitos fundamentais e versa sobre aspectos referentes à ciberespionagem, todavia, observa-se muitas lacunas e muitos fatos que carecem de regulamentação.

Algo de grande importância é fortalecer a cooperação entre diferentes Estados, como é o caso de convenções internacionais, seria de suma relevância o Brasil ratificar a Convenção de Budapeste para que o amparo e proteção aos usuários seja mais amplo e os usuários possam utilizar a rede com mais segurança, zelando também pela privacidade e a proteção dos crimes digitais.

Além da lacuna legislativa, outra problematização diz respeito à dificuldade que a polícia judiciária encontra em localizar o sujeito ativo da infração, bem como identificar a autoria e materialidade do crime, ocasionando muitas vezes na não punição do infrator, visto que faltam órgãos especializados para o combate e investigação, o sistema jurídico investigativo brasileiro carece de membros para esse tema. As provas digitais se alteram celeremente, é necessário que cheguem rapidamente ao alcance dos agentes investigativos para que os fatos não sejam perdidos e possa ser realizado uma investigação célere.

A respeito da territorialidade e a competência, conforme análise de julgados, o entendimento encontra-se no Código Penal e Código de Processo Penal, mas deve se levar muito em conta cada

caso concreto e suas peculiaridades, tendo em vista a facilidade de alteração das informações e provas do crime

Por fim, a prevenção pode ser vista como um importante vetor de sucesso, considerando que grande parte dos usuários são vulneráveis e não fazem noção do que pode acarretar o simples acesso ao meio virtual, várias vezes os usuários são crianças, que caso recebam orientação desde pequenas, podem tanto se proteger como não se tornarem futuros sujeitos ativos.

REFERÊNCIAS

ALVES, Marcelo de Camilo Tavares. **Direito Digital**. Goiânia, 2009.

ARAÚJO, Marcelo Barreto. **Comércio eletrônico, Marco civil da internet, Direito Digital**. Rio de Janeiro, 2017.

BLAT, Erick Ferreira. **Combate ao Crime Cibernético**. Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federal. Rio de Janeiro: M.Mallet Editora Ltda, 2016.

BRASIL. **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal.** Disponível em: http: www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986. Acesso em: 23 set. 2019.

BRASIL. **Código de Processo Penal**, decreto lei nº 3.689, de 03 de outubro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 08 mai. 2020.

_____. **Código Penal**, decreto lei nº 2.848, de 07 de Dezembro de 1940. Disponível em : http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 22 mai.2020.

_____, **Lei nº 12.965.** Brasília: Congresso Nacional, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 set. 2019.

_____, **Lei Ordinária nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante

uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 24 set. 2019.

_____, **Lei Ordinária nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 24 de set. 2019.

_____, **Lei Ordinária nº 13.718, de 24 de setembro de 2018**. Dispõe sobre a criminalização da exposição pornográfica não consentida; altera o Decreto – Lei nº 2.848, de 7 de desembro de 1940 – Código Penal; e da outras providencias. Disponível em : http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm . Acesso em: 22 de mai. 2020.

_____, Luís Osvaldo Grossmann. **Convergência digital**. Disponível em : https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=48450&sid=4. Acesso em: 8 mai. 2020.

CONVENÇÃO DE BUDAPESTE. **Crimes Cibernéticos.** 2018. Disponível em : https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=48450&sid=4. Acesso: 8 mai. 2020.

_____,. **Convenção sobre o cibercrime.** 2001. Disponível em : http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 31 out. 2019.

ISHIDA, Valter Kenji. **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal.** São Paulo. 2012.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

JESUS, Damásio E.de. **Direito Penal**. São Paulo: Saraiva, 2003.

MIRANDA, Marcelo Baeta**. Abordagem dinâmica aos crimes via Internet. Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 4, n. 37, 1 dez. 1999. Disponível em: https://jus.com.br/artigos/1828. Acesso em: 24 set. 2019.

OLIVEIRA, Alyne Farias, Letícia Andrade. **A vítima da pornografia de vingança no âmbito penal:** amparo judicial fronte a ausência de tipo penal incriminador. Disponível em: http://enpejud.tjal.jus.br/index.php/exmpteste01/article/view/32. Acesso em: 10 abr. 2019.

PAGANOTTI, Ivan. **Pressão virtual e regulamentação digital brasileira:** análise comparativa entre o Marco Civil da Internet e a Lei Azeredo. In: Media Policy and Regulation: Activating Voices, Illuminating Silences, University of Minho, dez. 2013.

PALAZZI, Pablo Andrés. **Delitos informáticos.** Buenos Aires: Ad Hoc, 2014.
PINHEIRO, Patricia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016.

_____ **Direito Digital**. 4. ed. São Paulo. Saraiva, 2010.

PISA, Pedro. **O que é IP**? Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html. Acesso em: 08 mai. 2020.

ROSSINI, Augusto. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica Editora, 2004.

SaferNet Brasil**. Combate crimes virtuais e a violação dos Direitos Humanos na internet**. Disponível em : https://new.safernet.org.br/denuncie#mobile . Acesso: 22 de maio de 2020.

SENADO FEDERAL. **CPI da espionagem**. Disponível em : www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1>. Acesso em: 08 de maio de 2020.

STJ. Conflito de competência: CC: 156284 PR 2018/0008775-5, Relator: Ministro RIBEIRO DANTAS, Data de Julgamento: 28/02/2018, S3 - Terceira seção. Disponível em : https://stj.jusbrasil.com.br/jurisprudencia/552870809/conflito-de-competencia-cc-156284-pr-2018-0008775-5 . Acesso em: 11 mai. 2020.

STJ. Conflito negativo de competência : CC 145576 MA 2016/0055604-1, Relator: Ministro JOEL ILAN PACIORNIK, Data de Julgamento: 13/04/2016, S3 - Terceira seção, Data de Publicação: DJe 20/04/2016. Disponível em : https://stj.jusbrasil.com.br/jurisprudencia/339952309/conflito-de-competencia-cc-145576-ma-2016-0055604-1/inteiro-teor-339952319. Acesso em: 22 mai. 2020.

TEIXEIRA, Tarcisio**. Curso de direito e processo eletrônico**: doutrina, jurisprudência e prática. São Paulo: Saraiva, 2014.

WENDT, Emerson.; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.