CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

CYBER CRIMES AND BRAZILIAN LEGISLATION

LAIS MOREIRA DE OLIVEIRA[1]
FERNANDO LOBO LEMES[2]

RESUMO

O presente artigo acadêmico tem o intuito de compreender os crimes cibernéticos e a legislação aplicada. Assunto este que se torna relevante no meio jurídico pela constante evolução tecnológica e consequentemente a necessidade de tipificação especifica em relação ao que é considerado um crime cibernético, a qualificação dos autores, o lugar considerado do crime, as competências para julgar e os meios de provas que podem ser utilizados para verificar o fato, compreendendo sua aplicação no âmbito brasileiro. Neste sentido, ao estudar a legislação vigente acerca do tema, analisando sua aplicabilidade e identificando os tipos penais será perceptível que há necessidade de uma legislação especifica e convincente que acompanhe os avanços tecnológicos, a fim de obter resultados positivos no combate e prevenção de crimes cibernéticos, como forma de garantir segurança aos usuários de redes de internet e punição expressiva aos infratores.

PALAVRAS-CHAVE: Crimes cibernéticos. Legislação brasileira. Redes de internet.

ABSTRACT

This academic article aims to understand cyber crimes and applied legislation. This issue becomes relevant in the legal environment due to the constant technological evolution and consequently the need for specific typification in relation to what is considered a cyber crime, the qualification of the authors, the place of the crime, the competency to judge and the means of evidence that can be used to verify the fact, understanding its application in the Brazilian scope. In this sense, when studying the current legislation on the subject, analyzing its applicability and identifying the criminal types it will be noticeable a need for specific and convincing legislation that accompanies technological advance, in order to obtain positive results in the fight and prevention of cyber crimes, as a way to ensure security for internet network users and significant punishment for offenders.

KEY-WORDS: Cybercrimes. Brazilian legislation. Internet networks.

---

[1] Graduanda do curso de Bacharelado em Direito na Faculdade Evangélica Raízes. Anápolis, Goiás, Brasil. E-mail: laismoreira5@hotmail.com.

[2] Pós-doutor em Ciências Humanas pela Pontifícia Universidade Católica de Goiás, (PUC GO), Doutor em História pela Université de la Sorbonne Nouvelle - Paris; Mestre em História pela Universidade Federal de Goiás (UFG), Graduado em História pela Pontifícia Universidade Católica de Goiás, (PUC GO) Professor pesquisador da Faculdade Evangélica Raízes Anápolis, Goiás, Brasil. E-mail: fernando.lemes@faculdaderaizes.edu.br

INTRODUÇÃO

Com o avanço tecnológico surgiram inúmeras facilidades, seja na realização de pagamentos, nos estudos, na forma de se comunicar, gerando rapidez e comodidade. Todavia, a rede de internet não é um meio totalmente seguro tendo brechas que facilitam a ação de criminosos.

A princípio será estudada a origem do computador e da internet, que surgiu tendo como propósito fins militares com objetivo de obter uma ferramenta que pudesse ser possível à comunicação de maneira rápida que trouxesse benefícios para eventuais pesquisas militares.

Com o avanço da tecnologia seja em computadores ou redes de internet surgiram como consequência, os Crimes cibernéticos ou também chamados *Cyber crimes*, que se tornaram recorrentes no mundo globalizado. Por vez não sendo noticiado diariamente no rádio, televisão ou mesmo no meio virtual, ocorrem diariamente delitos como estelionato, pornografia infantil e crimes contra a honra, que serão brevemente analisados no presente artigo.

Por conseguinte, há obstáculos quando se trata do lugar do crime, da jurisdição, competência, e os meios de provas utilizados para verificação do ato criminoso, onde há dificuldades técnicas para se chegar ao autor do crime.

O presente artigo, ao final irá abordar as legislações que tipificam os crimes cibernéticos, e apresentara a Convenção de Budapeste, que se trata de um tratado internacional a respeito de crimes praticados no espaço virtual. No entanto, como será demonstrada, a legislação existente não é suficiente e especifica para punir e prevenir restando tão somente a insegurança.

1 Origem da internet, História da legislação sobre crimes virtuais e Conceito

1.1 Origem dos computadores e internet

Como seres primitivos, o ser humano vem evoluindo ao longo da história, realizando novas descobertas e se aprimorando. Estudos históricos mostram que o primeiro sinal de evolução registrado foi à descoberta do fogo e a utilização de ferramentas para auxiliar nos afazeres diários (CARRES; MAGRO; PERREIRA, 2017). Da mesma forma aconteceu com a internet e os computadores, que foram

evoluindo ao longo dos anos; inventada a partir da necessidade de levar informações rapidamente para qualquer lugar do mundo.

Atualmente, a internet é o meio mais rápido e eficiente de levar informações de um lado do mundo para o outro. Essa descoberta marcou uma fase da evolução histórica da humanidade que jamais será esquecida, pois foi com a criação, primeiramente, dos computadores e, posteriormente, da internet que se iniciou uma nova fase da evolução da humanidade, tornando a globalização não só possível como também acessível para todas as classes sociais.

Carres, Magro e Pereira (2017, p. 2), explicam que a origem da internet está ligada as necessidades militares. Segundo os autores,

> Entretanto, a origem da internet está vinculada a evolução armamentista, pois os departamentos de pesquisa militares em busca de estarem à frente de seus inimigos, buscou formas de desenvolver sistemas que pudessem propiciar comunicações a longas distâncias bem como a interação de sistemas.

Além disso, Castells (*apud* CARRES; MAGRO; PEREIRA, 2017, p. 2) "ensina que a origem da internet remonta às primeiras redes de computadores criadas, dentre as quais se destaca a chamada Arpanet". A Arpanet (1969) foi criada para fins militares pelos Estados Unidos que queriam ter uma rede de recursos mais avançada do que a da União Soviética. Com o sucesso da Arpanet, os norte-americanos tiveram a possibilidade de tornar as redes de internet mais eficientes e, por essa razão, a Arpanet passou a interagir com outras redes de computadores. Através desse processo foi possível à interação entre várias redes de computadores, semelhante ao que conhecemos hoje como internet.

Jessica Fagundes Bortot (2017, p. 03) ensina que:

> Desde os primórdios da humanidade, o interesse em criar e desenvolver instrumentos que fossem capazes de auxiliar o trabalho do homem sempre existiu. Como decorrência disso, em 1830, o primeiro protótipo do computador que conhecemos foi construído, e nos anos 1970, a primeira versão comercial foi lançada.

Inicialmente, essas redes de computadores interligadas pela internet apenas para fins militares, passaram a chamar a atenção de espiões. "[...] assim ocorreram, antes mesmo de se tornar pública no final da década de 1980, as

primeiras condutas de cunho criminoso através da internet, atualmente chamadas de Crimes Cibernéticos” (BORTOT, 2017, p. 340).

Foi na década de 1980 que foram registrados os primeiros índices de crimes cibernéticos, devido ao aumento das organizações criminosas voltadas para crimes na internet. Essas organizações promoviam a pornografia infantil, criavam vírus cibernéticos *(malware)* e *software* piratas, bem como violações no sistema de telecomunicação (OLIVEIRA JUNIOR, 2013 *apud* ALMEIDA et al., 2015, p. 217).

Mas foi o ano de 1990 que marcou a sociedade mundial, quando a tecnologia das redes de computadores se tornou pública e disponível para venda, mas só adquiriu quem tinha condições econômicas de comprar um computador. Esse foi o início daquilo que viria a se tornar a maior dependência da humanidade, à internet e os aparelhos de telecomunicação (CASTELLS, 2003 *apud* CARRES; MAGRO; PEREIRA, 2017).

Para organizar as redes de informação foi criada a World Wide Webe (WWW), que são os ambientes dos navegadores que utilizamos. Esses navegadores foram criados pelos engenheiros da Centre Européen por La Recherche Nucléaire - CERN (ALMEIDA, 2005). Para Castells (1990), o sistema WWW “[...] organizava o teor dos sítios da internet por informação e não por localização, oferecendo aos usuários um sistema fácil de pesquisa para procurar as informações desejadas” (*apud* CARRES; MAGRO; PEREIRA, 2017, p. 2).

Sobre a importância e dependência da internet no meio jurídico Carres, Magro e Pereira (2017, p. 2) lecionam que:

> Assim também foi com a internet que nos propicia atualmente uma série de comodidades a ponto de muitas vezes sofrermos colapsos pela falta dela. Exemplos de utilidade estão estampados na utilização diária de eletrônicos, tais como celular, computadores, e também na importância que esta conquistou no mundo jurídico e profissional, como nos sistemas PROJUDI, PRC e PJE.

É cristalina verdade dizer que a internet criou um novo mundo, onde as pessoas podem ser quem elas realmente são sem precisar usar máscaras, que são defesas psicológicas usadas na convivência em sociedade. Contudo, essas mesmas pessoas já não mais compreendem que, como no mundo físico, também no mundo virtual as suas palavras têm o poder de provocar mudanças, afetando a vida de outras pessoas de forma positiva ou negativa. Neste aspecto, atualmente se

destaca o efeito negativo. Esse mesmo efeito tem o poder de mudar a visão que as pessoas têm sobre si mesmas, suas qualidades e defeitos, podendo desencadear atitudes diversas.

Enfim, a internet é uma ferramenta que marcou a sociedade moderna e se tornou indispensável, um verdadeiro vício, do qual somos todos dependentes. E, ao que tudo indica essa ferramenta só tende a crescer para atender a demanda que evolui incessantemente.

1.2 História da Legislação Brasileira sobre crimes virtuais

No Brasil, até o ano de 2012 não existia lei específica que dispunha sobre os crimes cometidos na internet. Desse modo, o legislador precisava fazer uso do Código Penal de 1940 para fundamentar suas decisões.

E notável que o legislador brasileiro pouco se preocupava com a tipificação e regularização dessa modalidade de crime, contudo, com o aumento desenfreado dos crimes cibernéticos no Brasil, o legislador foi obrigado a criar uma lei específica para o crime em comento. Por essa razão, em novembro de 2012 foi sancionada a Lei n° 12.735/2012 (BRASIL, 2012) que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similar, que sejam praticados contra sistemas informatizados.

E notório que houve pouca evolução dos conjuntos legislativos que tratam dos crimes digitais. Por outro lado, a rede de computadores, ambiente onde se desenvolve, por excelência, a prática dos crimes cibernéticos, tem muita notoriedade, porém escassa regularização. Senão vejamos:

> Devemos lembrar que o Direito deve acompanhar as transformações e mudanças da sociedade, adaptando-se dessa forma a sociedade da informação e ao mundo virtual, trabalhando em prol da segurança e garantindo a tutela jurídica dos direitos fundamentais da pessoa humana (GONÇALVES; PEREIRA; CARVALHO, referido em Sousa 2014).

Neste contexto, Lei n° 12.735/2012 (BRASIL, 2012) ficou popularmente conhecida no mundo jurídico como “Lei Carolina Dieckmann”, sancionada pela então Presidente Dilma Rousseff. Essa legislação trouxe algumas alterações no Código Penal, “tipificando os chamados delitos ou crimes informáticos”. Na prática, como

lembra Francesco (2014 *apud* ALMEIDA et al., 2015, p. 217), acresceu os artigos 154-A e 154-B e alterou os artigos 266 e 298 do Código Penal brasileiro.

Nesse sentido, explica Bortor (2017, p. 349):

> Até o ano 2012, não existia nenhuma lei para punir os crimes cibernéticos próprios, existindo somente legislação acerca dos crimes cibernéticos impróprios. Contudo, em decorrência de alguns episódios, como os DDoS - *Distributed Denial of Service* (ataques distribuídos de negação de serviço) a sites do governo e a divulgação de fotos íntimas da atriz Carolina Dieckmann, duas leis foram sancionadas com maior urgência, sanando algumas das várias deficiências existentes no ordenamento em relação a essa matéria, quais sejam, a Lei 12.735/201215, conhecida popularmente como “Lei Azeredo”, e a Lei 12.737/201216, conhecida como “Lei Carolina Dieckmann”.

Assim, a Lei nº 12.735/2012 (BRASIL, 2012) determina, em seu artigo 4°, que os órgãos da polícia judiciária deveram criar delegacias especializadas no combate a crimes digitais, tratando de tipificações para os crimes próprios, cita Marcelo Crespo (*apud* CAIADO; CAIADO, 2018) que:

> Crimes digitais próprios ou puros, condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas.

Além disso, frente à necessidade de maior regularização do uso da internet no Brasil, foi sancionada, em 23 de abril de 2014, a Lei nº 12.965/2014 (BRASIL, 2014), que estabelece princípios e garantias, direitos e deveres para o uso da rede mundial de computadores no Brasil. Sobre este dispositivo legal, Bortot (2017, p. 12) ensina que a referida lei ficou conhecida oficialmente como Marco Civil da Internet (MCI) que, por sua vez, estabelece princípios, garantias, direitos e deveres para os usuários e também para o próprio Estado. O artigo 1° da lei dispõe o seguinte: “Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria” (BRASIL, 2014).

Desta forma, o Marco Civil da Internet é uma lei criada com o intuito de proteger e garantir a liberdade de empresas e usuários e, ao mesmo tempo, fiscalizar atos supostamente ilícitos, oferecendo uma segurança legal para usuários e provedores de internet. Porém, em que pese sua importância, a simples outorga

de legislação deste tipo não é suficiente para suprir todas as lacunas existentes, pois existem, ainda, crimes graves sendo tratados por meio de leis brandas e, até mesmo, crimes não tipificados em nenhuma das leis citadas acima.

Além dos dispositivos supramencionados, a Lei nº 11.829/2008 (BRASIL, 2008) trouxe alterações na Lei nº 9.069/1990 (BRASIL, 1990), a fim de aprimorar o combate à produção de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionados à pedofilia na internet.

Ademais, devido ao aumento dos sites piratas para comercialização de propriedade intelectual, foi sancionada a Lei n° 9.606, de 19 de fevereiro de 1998 (BRASIL, 1998), que trata sobre a segurança da propriedade intelectual de programas de computador e de seu comércio no país.

Na verdade, os crimes cibernéticos são extremamente difíceis de serem combatidos, visto que é necessária qualificação profissional de funcionários para investigar e encontrar as pessoas responsáveis por tais delitos. Com o passar dos anos e a facilidade na comunicação, muitas pessoas deixaram de respeitar o que é bem público e o que é bem privado, e, em resposta, para salvaguardar a Administração Pública, foi, também, sancionada a Lei nº 9.983/2000 (BRASIL, 2000) que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da administração pública.

Além do mais, a Lei nº 9.296/1996 (BRASIL, 1996) disciplinou a interceptação de comunicação telemática ou informática. Por último foi sancionada a Lei n° 12.034/2009 (BRASIL, 2009) que delimita os direitos e deveres dentro da rede mundial de computadores durante as campanhas eleitorais.

Quanto aos aspectos históricos da legislação e órgãos de proteção, de acordo com Santos e Fraga (2010), para evitar crimes cibernéticos foram criadas as delegacias ou núcleos de investigação especializada, como a DIG-DEIC (4° Delegacia de Repreensão a Crimes de Informática de São Paulo/SP), DERCIFE (Delegacia Especializada de Repreensão a Crimes contra a Informática e Fraudes Eletrônicas em Belo Horizonte/MG) e a DRCI (Delegacia de Repreensão aos Crimes de Informática no Rio de Janeiro/RJ). Além desses órgãos e unidades, foi criada, em 1996, a Unidade de Perícia de Informática da Polícia Federal (SEPFIN).

Em 2005 foi criado, em Brasília, o Instituto Nacional de Criminalística da Polícia Federal (INC) que é reconhecido internacionalmente como uma organização

moderna e complexa. Além disso, como lembram Santos e Fraga (2010, p. 65), existe as organizações da iniciativa privada. Segundo os autores,

> Temos, ainda, outras medidas, algumas de iniciativa privada, tais como: a criação da SaferNet Brasil, organização não governamental, que através da Central Nacional de Denúncias de Crimes Cibernéticos, operada em parceria com o Ministério Público Federal, oferece à sociedade brasileira e à comunidade internacional um serviço anônimo de recebimento, processamento, encaminhamento e acompanhamento on-line de denúncias sobre qualquer crime ou violação aos Direitos Humanos praticado através da Internet. Ademais, temos a Cartilha de Segurança da Internet, que contém recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet, disponibilizado pelo centro de estudos, resposta e tratamento de incidentes de segurança no Brasil.

Finalmente foi criada, no ano de 2010, a Comissão do Direito na Sociedade da Informação da OAB/SP, destinada à elaboração:

> [...] de trabalhos escritos, inclusive pareceres, promoção de pesquisas, seminários e demais eventos que estimulem o estudo, a discussão e a defesa dos temas respectivos além da criação de grupos de trabalho e estudos sobre a temática, buscando o intercâmbio de informações com outras secionais da OAB, o Conselho Federal, órgãos públicos e universidades (OAB/SP, 2010).

.

Após realizada uma análise simplificada sobre o assunto, pode parecer que a legislação sobre os crimes na internet é extensa, contudo, uma análise pormenorizada indicará que, ainda que existentes, são incompletas e insuficientes, restando muito a ser feito quanto ao combate à criminalidade digital.

1.3 Conceitos e tipos de crimes virtuais no Brasil

O crime virtual vem sendo estudado mais a fundo há pouco tempo, pois com o passar dos séculos e o avanço tecnológico, esses crimes, que antes eram mais raros, estão, atualmente, em jornais impressos, televisivos ou nas redes sociais.

Os crimes contra a imagem ou produção intelectual são amplamente divulgados nos meios de comunicação, principalmente nas redes sociais, que se tornou um lugar sem normas, onde tudo é possível e as pessoas se sentem donas da vida particular do outro, divulgando imagens ou notícias de forma inconsequente. Esse tipo de publicações, sem autorização ou sem os direitos autorais, é tipificado

como crimes, mas de nada adianta estar positivado e não haver fiscalização adequada.

Com a popularização dos crimes virtuais, surgiram várias nomenclaturas, tais como crimes virtuais, crimes cibernéticos, crimes de alta tecnologia, digitais, informáticos, crimes por computadores, crimes na internet, fraude informática e crimes transnacionais (ALMEIDA et al., p. 08, 2015).

Para Bortot (2017, p. 341), “os crimes cibernéticos são, assim como os crimes comuns, condutas típicas, antijurídicas e culpáveis, porém praticadas contra ou com a utilização dos sistemas da informática”.

Rossini (p. 09, 2004) assim define:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

A respeito da classificação dos crimes digitais, existe divergência doutrinaria. Alguns doutrinadores classificam os crimes na internet como próprios ou impróprios, enquanto outros entendem tratar-se de crimes puros, mistos ou comuns.

Os crimes cibernéticos puros são aqueles que afetam diretamente o programa ou software, hardwares ou os dados armazenados na memória do aparelho. Os crimes classificados como mistos não atingem os programas da rede, pois “o computador é utilizado como mera ferramenta para se produzir a ofensa a outros bens jurídicos que não sejam do sistema de informática” (ALBUQUERQUE, p. 04, 2006).

Por último, segundo Pinheiro (2011, *apud* CARRES; MAGRO; PEREIRA, 2006, p. 04) os delitos considerados comuns são “aqueles onde a internet é usada como forma de difusão rápida de crimes que já estão tipificados nos códigos brasileiros, como a pornografia infantil”.

Com relação aos sujeitos, autores dos crimes virtuais, ficaram popularmente conhecidos como *hackers* ou *crackers*, todavia, existe uma diferença entre as duas nomenclaturas. Hackers, segundo Michaelis (2017 *apud* CARRES; MAGRO; PEREIRA, 2017, p. 5):

> [...] diz respeito a um indivíduo que se dedica a entender o funcionamento dos dispositivos, programas e redes de informática com a finalidade de, entre outras coisas, encontrar falhas em sua segurança ou conseguir um atalho inteligente que possa vir a resultar em um novo recurso ou ferramenta.

Os autores das grandes fraudes virtuais são os *crackers* ou piratas digitais, que segundo Barros (2017, p. 409), “são pessoas especialistas em sistemas informatizados, que invadem sistemas alheios sem autorização com o objetivo de adulterar programas e dados, furtar informações e valores e praticar atos de destruição deliberada”.

Essa definição incorreta dos *hackers* (ou chapéus brancos) foi difundida pelas manchetes de jornais, que imputavam uma autoria equivocada. Assim sendo, os sujeitos invasores de computadores e sistemas são os *crackers* (ou chapéus negros), que agem de forma premeditada, com o objetivo de obter vantagens ilícitas muitas vezes comparadas com terroristas.

No Brasil, para uma conduta ser considerada criminosa ela precisa ter três requisitos básicos, são eles: a conduta típica, antijurídica e culpável. A conduta será típica quando houver um dispositivo legal que a descreva como crime, seja dolosa ou culposa, comissiva ou omissiva. A antijuricidade é definida como a contrariedade entre o fato e o ordenamento jurídico. Por último, a culpabilidade diz respeito à culpa ou dolo na prática da conduta.

Esses requisitos básicos para classificar uma conduta como crime são muito difíceis de serem provados no âmbito dos crimes cibernéticos. Logo, Gatto (2011, *apud* CARRES; MAGRO; PEREIRA, 2017, p. 7) explica que em vários dos crimes cometidos diariamente “através da internet e não estão tipificados, resta prejudicada a sua punição em casos como este se busca aplicar a analogia jurídica para adequar os crimes a uma tipificação já existente em nosso ordenamento jurídico”. Ainda sobre o mesmo entendimento, explica o autor:

> Analogia na maioria dos casos não se efetiva, pois, se o juiz não pode aplicar pena a fato que não seja típico, este também não poderá julgar por analogia crime que seja atípico, até por que no Direito Penal, a analogia só pode ser usada em benefício do réu, o que prejudica substancialmente o fundamento jurídico da decisão do juiz, que sem este embasamento que é caráter essencial da sentença penal deverá proceder com a absolvição do acusado, sob pena de não o fazendo, considerar-se nulo o processo (GATTO, *apud* CARRES; MAGRO; PEREIRA, 2017, p. 7).

Por fim, a legislação brasileira sobre crimes virtuais, apesar de nova, ainda não prevê todos os tipos de crimes que são cometidos no ambiente virtual. Nesta seara, é unânime o entendimento de que, apesar da Lei n° 12.965/2014 (BRASIL, 2014) estar em vigência há poucos anos, a mesma já precisa ser atualizada, passando a tratar de crimes que ainda não foram tipificados.

2 Espécies de crimes cibernéticos

Os crimes cibernéticos se dividem em duas modalidades, os crimes exclusivamente cibernéticos e os crimes cibernéticos abertos. Wendt e Jorde (2013, p. 19) definem os crimes exclusivamente cibernéticos como aqueles que "somente podem ser praticados com a utilização de computadores ou de recursos tecnológicos que permitem o acesso à internet".

Exemplo de crime exclusivamente cibernético está previsto no artigo 241-D, da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente (BRASIL, 1990), que classifica como crime o ato de "aliciar assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso". Esse crime ocorre muito em salas de bate papo na internet com o fim de induzir crianças a se exibir de forma pornográfica (WENDT; JORGE, 2013).

Wendt e Jorde apresentam outros exemplos de crimes exclusivamente cibernéticos (2013, p. 20):

> Invasão de computadores mediante violação de mecanismos de segurança com o fim de obter, adulterar ou excluir dados e informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidade para obter vantagem ilícita; interceptação telemática ilegal; pornografia infantil por meio de sistema de informação; corrupção de menos em sala de bate papo; crimes contra a urna eletrônica.

Já os crimes cibernéticos abertos são aqueles que podem ser praticados de "forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele" (WENDT; JORGE, 2013. p. 19).

Trate-se de crimes mais conhecidos, são exemplos: os crimes contra a honra, ameaça, pornografia infantil, estelionato, furto mediante fraude, racismo, apologia ao crime, falsa identidade, concorrência desleal e tráfico de drogas (WENDT; JORGE, 2013, p. 20).

Desta forma, constata-se a enorme quantidade de crimes virtuais. Adiante, nos limitaremos a estudar alguns dos crimes cibernéticos abertos conhecidos socialmente.

2.1 Dos crimes contra a honra

A legislação brasileira classificou os crimes contra a honra, bem imaterial. Estão previstos dos artigos 138 ao 145 do Código Penal (BRASIL, 1940), sendo três espécies: calúnia, difamação e injuria.

O crime de calúnia está previsto no artigo 138 do Código Penal (BRASIL, 1940), *in verbis*: “caluniar alguém, imputando-lhe falsamente fato definido como crime”. Julio Fabbrini Mirabete (*apud* NETO, 2009, p. 30) explica o crime de calúnia dizendo que:

> Pratica o crime quem imputa, atribui a alguém, a prática de crime, ou seja, é afirmar, falsamente, que o sujeito passivo praticou determinado delito. É necessário, portanto, para a configuração da calúnia, que a imputação verse sobre fato determinado, concreto específico, embora não se exija que o sujeito ativo descreva suas circunstâncias, suas minúcias, seus pormenores. Trata-se de crume de ação livre que pode ser cometido por meio da palavra escrita ou oral, por gestos e até meios simbólicos. Pode ela ser explícita (inequívoca) ou implícita (equívoca) ou reflexa (atingindo também terceiro). A imputação da prática de uma contravenção não constitui calúnia, mas pode caracterizar o delito da difamação. Como a honra, objetica e subjetica, é um bem jurídico disponível, o consentimento anterior ou concomitante com o fato exclui o crime.

Nesse sentido, para configurar calúnia o fato descrito deve ser qualificado como crime e necessariamente sua imputação deve ser falsa.

O crime de difamação está previsto no artigo 139 do Código Penal (BRASIL, 1940) que conceitua como “difamar alguém, imputando-lhe fato ofensivo à sua reputação”. Diferente da calúnia, no crime de difamação à conduta imputada como ato ofensivo, não necessita estar descrita como crime (SOARES, 2016, p. 4).

Ney Moura Teles (*apud* NETO, 2009, p. 31) a partir de uma análise dos elementos objetivos do crime de difamação, explica que:

> A difamação é a imputação de um fato certo, determinado, capaz de macular a honra da pessoa. Não pode ser um fato típico de crime, pois aí haverá calúnia, mas imputada a prática de um outro ilícito, uma contravenção penal ou um ilícito civil, poderá constituir difamação desde

> que tal fato seja ofensivo. Não é necessário que o fato seja ilícito, todavia deve ser daqueles que martirizam a reputação da vítima.

Para o crime de difamação pouco importa se o fato imputado é verdade ou não, a simples acusação já configura o delito.

Por último, o crime de injúria previsto no artigo 140 do Código Penal (BRASIL, 1940), como “injuriar alguém, ofendendo-lhe a dignidade ou o decoro”. A conduta é ofender a honra subjetiva do sujeito passivo, atingindo a sua moral, e/ou atributos físicos, intelectuais, sociais (NETO, 2009, p. 31).

A internet vem ocupando lugar de destaque na sociedade, aproximando as pessoas, contudo vem sendo praticado nesses ambientes violações graves à honra, gerando principalmente consequências psicológicas aos usuários.

Esses crimes são agravados no mundo virtual, que podem ser cometidos de forma oral ou escrita, de difícil retirada, e são vistos por um número ilimitado de pessoas, além da dificuldade em identificar o criminoso. Portanto, estão se tornando cada vez mais comuns diante da facilidade na internet e a pouca fiscalização (NETO, 2009, p. 31).

Os tribunais brasileiros vêm decidindo que a internet é um fator agravado, por ter uma abrangência maior. Neste diapasão, o Superior Tribunal de Justiça (STJ) vem entendo, quanto “os crimes contra a honra praticados em ambiente virtual, que a competência é do local onde se encontra o responsável pela divulgação da notícia” (SOARES, 2016, p. 09).

Portanto, a internet contribui significativamente para o aumento do número de crimes contra a honra, uma vez que os dados que circulam pela internet são de difícil controle (NETO, 2009).

2.2 Da pornografia infantil

Como foi afirmado anteriormente, a pornografia infantil é crime cibernético aberto, previsto no artigo 241-A do Estatuto da Criança e do Adolescente (BRASIL, 1990), no qual é dito, o seguinte:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1 º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2 º As condutas tipificadas nos incisos I e II do § 1 º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo (BRASIL, 1990).

Destaca-se que a pornografia infantil virtual é diferente de pornografia real, no qual existem menores envolvidos. Na pornografia infantil virtual não existe a utilização física de uma criança, havendo duas possibilidades: a pornografia infantil "que visualmente represente uma criança envolvida num comportamento sexualmente explícito, tratando-se, contudo, de uma pessoa maior que aparenta ser uma criança", conhecido como pedopornografia aparente. A segunda possibilidade ocorre na "pornografia infantil que visualmente representa uma criança envolvida num comportamento sexualmente explícito, tratando de representações geradas, simuladas, criadas e manipuladas" por computadores, conhecido como pedopornografia virtual (SILVA, 2016, p. 22).

Esse tipo crime é de difícil fundamentação, pois existe o problema relativo à identificação do bem jurídico que se pretende proteger. Alguns doutrinadores entendem que o que se pretende salvaguardar é a liberdade de autodeterminação sexual, "uma vez que tanto no caso da pedopornografia aparente como no da pedopornografia virtual não existe qualquer ofensa concreta a um menor". Outra consideração possível é a tutela da moral e dos bons costumes, que entra em conflito com a liberdade de criação artística, e mesmo nos casos em que são consideradas inapropriadas, não constituem crime (SILVA, 2016, p. 22).

O maior problema da pornografia infantil virtual não reside apenas em conceitos morais, mas concretamente no "perigo de a divulgação e consumo desse material servir para estimular a facilitar a prática de crimes sexuais contra crianças". A pornografia infantil pode estimular instintos sexuais, despertar tendências de natureza pedófila e, consequentemente, a prática de crimes (SILVA, 2016, p. 26).

2.3 Do estelionato virtual

O crime de estelionato está previsto no artigo 171, *caput*, do Código Penal (BRASIL, 1940), *in verbis*: “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”. Consiste no ato ilícito praticado pelo meio virtual, com a finalidade de obter vantagem indevida para si ou para outrem.

Pinheiro (2006, p. 20) ensina que para configurar o crime de estelionato “e necessário induzir ou manter alguém em erro mediante ardil – ao menos uma determinada pessoa e não um sistema eletrônico”. Deve existir uma relação entre o autor e a vítima que está sendo iludida.

No tocante a aplicação do artigo 171 do Código Penal (BRASIL, 1940) para a modalidade de estelionato praticado através de sistemas informáticos, Torres (2016, p. 50) explica que caberá a “aplicação do art. 171, do Código Penal, vista a previsão de expressão de qualquer outro meio fraudulento”.

Julio Fabbrini Mirabete comenta o citado artigo (2003, p. 1350):

> A conduta do estelionato consiste no emprego de meio fraudulento para conseguir vantagem econômica ilícita. A fraude pode consistir em artifício, que é a utilização de um aparato que modifica, aparentemente, o aspecto material da coisa ou da situação... em ardil, que ardil, que é a conversa enganosa, em astúcia, ou mesmo em simples mentira, ou em qualquer outro meio para iludir a vítima [...].

Os exemplos mais comuns de estelionato virtual, com a finalidade de obter vantagem indevida, são as transferências fraudulentas de fundos nas contas bancárias, ou o arredondamento no valor em conta dos clientes ou empresa, tirando de pouco a pouco e acumulando lentamente na conta do autor. Outro exemplo é o acesso indevido a informações bancárias através de páginas falsas, fazendo com que a vítima forneça seus dados voluntariamente. Com esses dados o criminoso transfere o saldo em conta da vítima para sua titularidade (TORRES, 2016).

Resta evidente que é totalmente cabível a aplicação do artigo 171 do Código Penal (BRASIL, 1940), em decorrência da previsão da expressão “qualquer outro meio fraudulento” (TORRES, 2016, p. 50).

2.4 Dos crimes contra a propriedade intelectual

A proteção à propriedade intelectual é trazida ao ordenamento jurídico brasileiro pelo artigo 5º, XXVII, da Constituição Federal (BRASIL, 1988), *in verbis*:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> XXVII - aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar;
> [...]

Garante proteção aos autores de suas obras, podendo dispor delas de acordo com seus interesses e transmitindo esses direitos aos seus herdeiros (TORRES, 2016, p. 53).

Por sua vez, o Código Penal tutela o bem jurídico garantido pela Constituição Federal, tipificando como crime o furto de ideia de material corpóreo ou incorpóreo produzido intelectual, artístico ou cientificamente (TORRES, 2016). Vejamos o que diz o artigo 184 do Código Penal (BRASIL, 1940):

> Art. 184. Violar direitos de autor e os que lhe são conexos:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
> § 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
> § 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.

Há mais duas leis que tratam desse assunto: a Lei nº 9.609/98 (BRASIL, 1998) compõe sobre a segurança da propriedade intelectual de programa de computador, e sua comercialização no País, e a Lei nº 9.610/98 (BRASIL, 1998) que altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

É cristalino que, com o avanço da internet, muitos usuários têm a sensação de liberdade sem limites, não se importando com leis coercitivas e proibitivas, além do que tem se tornado cada vez mais difícil limitar a sensação de autonomia concedida aos que tem acesso a redes de computadores e internet (LIMA, 2010).

O meio ambiente virtual ampliou o acesso a informações e tornou mais fácil a divulgação de trabalhos intelectuais como a música, cinema, televisão, literatura, fotografia, que se adaptaram a internet. Porém, esse meio também tornou extremamente volátil, tendo em vista a facilidade de divulgar e reproduzir as obras intelectuais (TORRES, 2016).

A violação da propriedade intelectual na internet é associada ao termo pirataria virtual, como bem observa Henrique Galdemann (*apud* NETO, 2009, p. 41):

> Chama-se vulgarmente de pirataria à atividade de copiar ou reproduzir, bem como utilizar indevidamente – isto é, sem a expressa autorização dos respectivos titulares – livros ou outros impressos em geral, gravações de sons e/ ou imagens, *software* de computadores, ou, ainda, qualquer outro suporte físico que contenha obras intelectuais legalmente protegidas.

Para alguns doutrinadores o ato de “colocar arquivos sem que tenham sido respeitados os direitos autorais deve ser duramente punida”, por outro lado, alguns doutrinadores entendem que “só se configura o crime quando há a intenção lucrativa no compartilhamento dos arquivos”. Na realidade, em ambos os casos, mesmo que se confirme a pirataria virtual, é difícil provar quem é o sujeito do crime, devido a grande parcela de usuários na internet que fazem *downloads* ilegais (NETO, 2009, p. 41).

Enfim, o avanço tecnológico tornou mais fácil a globalização e o acesso a informações e, consequentemente, o surgimento dos crimes virtuais, que não possuem limitações dadas à característica global da internet. Vale ressaltar que todos os usuários são vítimas potenciais e que todo o cuidado é pouco (TORRES, 2016).

3 Legislação brasileira acerca dos crimes cibernéticos e a Convenção de Budapeste

3.1 Aspectos relevantes das normas

A internet é ferramenta indispensável no dia a dia de muitos trabalhadores, e não apenas para o trabalho, como também para o lazer. Com os índices sempre elevados de usuários, a internet se torna parte da realidade vivida pela quase totalidade de sujeitos de direitos no mundo todo.

Sua principal importância está nos negócios do chamado Comércio Eletrônico. Com a popularização do Marketing Digital, muitas empresas e/ou profissionais liberais utilizam a internet, principalmente das redes sociais, para divulgar e oferecer seus serviços e/ou produtos. Outrossim, possibilitou as transações realizadas em bolsas de valores, como a compra e venda de ações, que movimenta milhões de dólares anualmente, que não seria possível sem a internet e a rede de computadores (COELHO, 2008).

Nessa mesma linha, a internet revolucionou a educação, possibilitando o estudo à distância, tornando possível estudar com comodidade de casa. Por fim, o uso das cartas escritas a mão foi substituído pelo correio eletrônico e as redes sociais que tornaram a comunicação mais dinâmica e veloz (COELHO, 2008).

Impossível elencar as variadas formas de utilização da internet ou imaginar a ausência da tecnologia que enlouqueceria muitas pessoas, principalmente por se verem isoladas do restante do mundo. Porém essa ferramenta que conecta o mundo também é o local de vários crimes, os quais este trabalho vem estudando.

Jacinto (2014, p. 47) explica que “não se pode dissociar as formas de segurança do chamado mundo virtual e do mundo real, pois existem similaridades em ambas”. Com o passar dos anos, os usuários que antes eram amadores, tornaram-se extremamente atualizados e atentos aos métodos de segurança. Hoje, poucos são os casos de e-mail piratas que são abertos, mesmo os infratores sendo bastante criativos.

Na sociedade digital, a coleta de informações e dados se tornou uma prática bastante usual e necessária, tornando tais dados vulneráveis a ataques.

Senhas e outros tipos de dados não devem ser disponibilizados em qualquer tipo de *site*, e é preciso averiguar se a página virtual é de confiança, bem como todos os itens de segurança que os mesmo apresentam (JACINTO, 2014).

Podemos elencar algumas situações e atividades que os usuários não devem realizar:

> Divulgação de informações pessoais; compartilhamento ou mesmo envio de mensagens contendo spam é códigos maliciosos; compartilhamento de *password* (senhas); distribuição e cópia não autoriza de material protegido por direitos autorias; invasão a outros computadores (JACINTO, 2014, p. 50).

Outra ferramenta utilizada para se evitar ataques é a criptografia, que poderia ser definida como “um conjunto de regras que visa codificar a informação de maneira que só o emissor e o receptor consiga decifrá-lá”. No que tange a proteção dos dados pessoais dos usuários no mundo virtual, é correto afirmar que são as ações dos próprios usuários, principalmente os que não têm conhecimento das ferramentas de proteção, determinantes na invasão de terceiros aos dados e imagens disponibilizados em redes sociais (JACINTO, 2014, p. 51).

Uma medida de segurança ainda pouco conhecida nos casos de invasão aos dados e imagens e realizar um ata notarial no cartório, explicando o ocorrido:

> Uma solução para dar suporte a crimes ocorridos no mundo virtual e que pode servir para futuras ações judiciais, é, no momento em que se verificar a ocorrência desses ilícitos, se dirigir a um cartório, e realizar uma ata notarial do ocorrido. A vítima terá assim, uma prova robusta para uma futura ação judicial cabível (JACENTO, 2014, p. 52).

Dessa maneira a vítima teria provas concretas capazes de fundamentar uma futura ação judicial. Há que se deixar claro que, quando o assunto é proteção à intimidade, a dados pessoais, essencialmente os usuários devem ficar atentos, evitando ao máximo a divulgação de dados e imagens (JACINTO, 2014).

Por conseguinte, o universo das informações cria uma confusão entre o “virtual” e o “real”, permitindo a variedade de identidade, os usuários não conseguem diferenciar o que real, ou o que é apenas fruto da imaginação de outras pessoas ou da sua própria imaginação (OLIVEIRA, 2015).

Normalmente conseguimos diferenciar o real do virtual, através dos gestos, olhares, expressões corporais, que ajudam a identificar se a pessoa está mentindo ou não. Vejamos entendimento doutrinário:

> A linguagem deve ser a primeira atitude, logo após do olhar, movimento do corpo e seus atos onde os outros indivíduos devem ajustar a sua conduta. Nas comunicações virtuais, não há a possibilidade de expressão no rosto do outro, identificando assim, seus sentimentos (OLIVEIRA, 2015, p. 16).

O mundo virtual trouxe a ideia de que tudo é permitido, não havendo limites para as falsas alegações, a prática de crimes contra a honra, a pornografia infantil, estelionato virtual, entre outros (OLIVEIRA, 2015).

O avanço tecnológico tem impulsionado as relações sociais e econômicas, facilitando a comunicação e as transações financeiras, daí nasce a obrigação do Estado em oferecer instrumentos hábeis ao direito, buscando o ideal de justiça (OLIVEIRA, 2015).

A internet é um facilitador, ferramenta indispensável para a vida social, econômica, jurídica e para muitas áreas de serviço, mas seu uso, principalmente nas redes sociais, requer cuidados e responsabilidade (OLIVEIRA, 2015).

3.2 Dos meios de prova

Como todo crime no processo penal, as partes envolvidas no litígio além de alegar os fatos, deve comprová-los, demonstrando a veracidade das alegações por meio de provas que comprovem a materialidade do crime (COELHO, 2008).

A prova processual tem aspecto objetivo, ou seja, demonstra a existência de um fato, mas também tem aspecto subjetivo, isso é, a produção de provas deve causar ao magistrado um estado psíquico, levando-o a entender serem verdadeiros os fatos alegados (COELHO, 2008).

A convicção do magistrado está condicionada aos “fatos nos quais se funda a reação jurídica controvertida; às provas desses fatos, colhidas no processo; às regras legais e máximas de experiências; e o julgamento deverá sempre ser motivado”. Logo, as provas devem ser demonstradas com clareza, uma vez que deverão dar segurança e veracidade ao que foi alegado em sede de inicial (COELHO, 2008, p. 26).

Sobre a ação desses agentes criminosos, vejamos:

> Os criminosos atuam das mais diversas formas. Eles utilizam sites para proliferarem ideais racistas, invadem contas bancárias, praticam pedofilia e

> interceptam comunicações eletrônicas, piratarias que ferem o direito autoral, por exemplo, sem que para isso precisem utilizar qualquer ferramenta palpável, como armas, mas apenas sofisticados programas tecnológicos que possibilitam que o agente esteja até mesmo em outro território, a quilômetros de distância da vítima alvo da sua empreitada criminosa (COELHO, 2008, p. 34).

O correio eletrônico também é amplamente utilizado pelos criminosos, que enviam mensagens às vítimas de maneira que pode lhes causar diversos prejuízos, como, por exemplo, vírus, descobrindo senhas bancárias, enviando programas piratas, entre outros (COELHO, 2008).

Os criminosos virtuais quase sempre usam uma identidade camuflada, desde então nascendo a dificuldade de comprovar pelos meios lícitos admitidos em direito, ~~de~~ quem foi o autor. Essa tarefa de descobrir os autores desse tipo de crime cabe aos peritos dos órgãos encarregados (RONCADA, 2017).

Os peritos devem informar ao juiz os detalhes e circunstâncias que envolvem o crime, ou seja, o equipamento usado, os programas, arquivos, enfim, tudo aquilo que for necessário para demonstrar a materialidade e autoria do crime. Ressalta-se que a busca e apreensão do computador utilizado como instrumento do crime depende de autorização judicial (COURI, 2009).

Esses peritos devem sempre estar atualizados, bem como os operadores do direito:

> Além da constante atualização dos peritos criminais, necessária também a atualização dos operadores do direito, para que possam atuar de forma mais segura. Implantar eventos relacionais ao tema em faculdades de Direito tornase fundamental na busca de profissionais competentes. Os meios acadêmicos, o próprio Poder Judiciário, e também as entidades de classe devem ser alvo desta capacitação técnica.
> Não se olvidando da capacitação jurídica, demasiadamente importante, os operadores do direito devem se adequar à nova realidade mundial, que busca diminuir fronteiras e a celeridade. O conhecimento acerca do ordenamento legal tem que ser associado ao conhecimento sobre as ferramentas virtuais, possibilitando o surgimento de profissionais capazes de solucionar conflitos atuais, que em sua maioria envolvem questões tecnológicas (COELHO, 2008, p. 35).

O uso da tecnologia associada à competência profissional gera a prestação de um serviço muito mais eficiente, além de diminuir a morosidade da prestação judicial. O maior estimulo desses criminosos é a crença de que o mundo digital é um ambiente sem lei, a margem do mundo real. Isso acontece porque a sociedade não acredita na punição desses infratores, além dos poucos casos conhecidos de condenação (COELHO, 2008).

3.3 Do lugar do crime

Com relação ao local do crime, o Código Penal adotou a teoria da ubiquidade, conforme previsto no artigo 6º do referido diploma legal: “Considera-se praticado o crime no lugar em que ocorre a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado” (BRASIL, 1940).

Além disso, o artigo 5º do Código Penal adotou como regra o princípio da territorialidade, em que “aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regrar de direito internacional, ao crime cometido no território nacional” (BRASIL, 1940).

Com relação à teoria da ubiquidade vejamos:

> Revele-se que, quanto ao lugar do crime, a soberania dos Estados impõe a aplicação da lei penal incidente ao caso, em todo o seu território, ocorrendo situações que ultrapassam a sua fronteira, o que usualmente ocorre nos crimes pela internet, enquanto crimes praticados pelo computador (COURI, 2009, p. 18).

Como no meio virtual não possui um espaço físico geograficamente determinado, considera-se que o seu acesso é muito dinâmico, assim a concepção de território, como espaço físico, ganha a conotação de “espaço virtual, posicionado em espaço global, no qual há uma transcendência dos limites territórios”. Ademais existe a problema quanto ao momento do crime, sobretudo se a ação tiver sido programada com meses de antecedência (COURI, 2009, p. 18).

3.4 Da competência

Trata-se de um dos maiores problemas enfrentados pelos doutrinadores, visto que a internet rompe fronteiras pelo seu caráter transnacional, logo o mesmo fato criminoso pode ocorrer em um local e se consumar em outro completamente diferente.

O artigo 70, *caput,* do Código de Processo Penal fixa a competência dos crimes a distância, no qual são adotados, como regra, a teoria do resultado: a competência será, de regra, determinada pelo lugar em que se consumar a infração,

ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução (BRASIL, 1941).

Ou seja, a competência para apurar a infração penal e do foro onde se deu a consumação do delito. Porém quando por tratar-se de crimes virtuais, a questão é mais complexa, pois “as distâncias territoriais transformaram-se na distância entre olhos e mãos de um teclado de computador” (OLIVEIRA, 2015, p. 57).

Assim, a fixação da competência dos crimes praticados fora do território nacional possivelmente pode ser solucionada pelo artigo 88 do Código de Processo Penal: no processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República (BRASIL, 1941).

Contudo a solução não é tão simples, pois há de ser analisado, em caráter preliminar, o fato do crime cometido através de um computador constituir delito material ou formal, questão relevante para uma correta fixação da competência, uma vez que, os crimes materiais apenas se tornam perfeitos com a realização do resultado (OLIVEIRA, 2015).

Portanto nos crimes materiais, o local da produção do evento é que fixa sua consumação e competência. Assim, existe uma dificuldade em fixar a competência nos crimes praticados fora do território nacional (OLIVEIRA, 2015).

Outra questão relevante, mas agora dentro do território nacional, é a escolha do juízo competente. Alguns doutrinadores entendem ser competência da Justiça Estadual e outros da Justiça Federal.

O doutrinador Túlio Lima Vianna (2000, *apud* OLIVEIRA, 2015, p, 87) entende que:

> Quando o crime for praticado pela Internet, julgamos que a competência deverá ser da Justiça Federal, já que o interesse da União em ter a Internet resguardada dentro dos limites brasileiros é evidente. Além do mais, este é um crime em que o resultado nem sempre se produz no lugar da ação, podendo até ocorrer em países diversos (crimes à distância), com repercussões internacionais que nos fazem crer ser prudente deixar a competência para a Justiça Federal.

Existem longas discussões sobre a fixação da competência e outros aspectos dos delitos informáticos, no qual as divergências existentes atrasam a contemplação da Justiça e beneficia o infrator.

3.5 Convenção de Budapeste

A Convenção sobre Cibercrimes do Conselho da Europa, também conhecida como Convenção de Budapeste é um tratado internacional sobre crimes cibernéticos, firmado no âmbito do Conselho da Europa[1], que procura harmonizar as legislações penal e processual penal, a fim de permitir a cooperação para obtenção de provas digitais (DOMINGOS; RODER, 2017, p. 66).

Foi criada em 2001, na Hungria, pelo Conselho da Europa, e está em vigor desde 2004, após a ratificação de cinco países. A Convenção engloba mais de 20 países e tipifica os principais crimes cometidos na Internet. Ressalta-se que o "Brasil não é signatário da Convenção, mas por ser o único tratado sobre crimes cibernéticos existentes, acaba sendo o modelo e parâmetro para as demais legislações" (DOMINGOS; RODER, 2017, p. 66).

O tratado internacional possui 48 artigos, divididos em 4 capítulos: Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais. A convenção prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço e reconhece a necessidade de cooperação entre os Estados e a indústria privada (SOUZA; PEREIRA, 2009).

O artigo 23º da Convenção trata dos princípios gerais reativos à cooperação internacional, o qual aponta que:

> As partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes N sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou reciprocas, e do seu direito nacional, na medida mais ampla possível, para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para recolher provas sob a forma electrónica de uma infracção penal (BUDAPESTE, 2001).

[1] O Conselho da Europa é uma organização internacional fundada em 05 de maio de 1949, sendo a mais antiga instituição europeia em funcionamento. Os seus propósitos são a defesa dos Direitos Humanos, o desenvolvimento democrático e a estabilidade político sócia na Europa (CONSELHO DA UNIÃO EUROPEIRA, 2018)

O tratado também dispõe sobre extradição, no artigo 24º, a qual “ficará sujeita às condições previstas pelo direito interno na Parte requerida ou pelos tratados de extradição aplicáveis” (BUDAPESTE, 2001).

Enfim, com o fenômeno da globalização e da popularização da internet, as distâncias ficaram menores, como também facilitou a proliferação de crimes que antes apenas era possível no mundo real, como, por exemplo, a pornografia infantil. A Convenção parte da premissa de que o combate ao cibercrime deve ser realizado através de um regime internacional, possibilitando uma justiça mais célere.

Conclusão

O presente artigo teve o objetivo de explanar sobre a legislação acerca de crimes cibernéticos e estudar sobre os principais crimes virtuais praticados no âmbito brasileiro, delitos que surgiram em decorrência da revolução tecnológica, e como consequência, possibilitou o acesso a informações e meios eletrônicos viabilizando a ação de criminosos.

Nesse sentido, ao tempo que a tecnologia traz conforto e comodidade, surge com ela insegurança virtual onde o usuário não obtém respaldo ao ser vitima de algum crime cibernético. Restando evidenciado que o ordenamento jurídico brasileiro carece de legislação especifica que puna com rigor delitos praticados através de um computador, mesmo com a similaridade com os crimes dispostos no Código Penal, tais violações não possuem tipificações próprias.

Isso posto, entende-se que os Crimes cibernéticos estão se tornando habituais, evidenciando a importância de leis atuais que sejam efetivas na punição de criminosos virtuais, a fim de se obter resultados positivos no combate e prevenção de tais crimes.

REFERÊNCIAS

ALMEIDA, Jéssica de Jesus; MENDONÇA, Allana Barbosa; CARMO, Gilmar Passos do SANTOS, Kendisson Souza; SILVA, Luana Munique Meneses; AZEVEDO, Roberta Rayanne Dória de. **CRIMES CIBERNÉTICOS.** Caderno de Graduação Ciências Humanas e Sociais, Aracaju, v. 2, n. 3, p. 215-236, março 2015. Disponível em: https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217. Acesso em: 26 nov. 2019;

ALMEIDA, José Maria Fernandes de. **Breve História da Internet. 2005.** Dissertação (Artigo) Universidade do Minha, Departamento de Sistemas de Informação – DSI, Muceu Virtua de Informática, 2005. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/3396/1/INTERNET.pdf. Acesso em: 26 nov. 2019.

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática.** São Paulo: Editora Juarez de Oliveira, 2006.

BARROS, Marco Antonio de et al. Crimes Informáticos e a proposição legislativa: considerações para uma reflexão preliminar. **Revista dos tribunais**, v. 865, p. 401-417, 2007.

BORTOT, Jessica Fagundes. Crimes Cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **Revista VirtuaJus**. Belo Horizonte: v. 2, n. 2, p.338-362, 1º sem. 2017. ISSN - 1678-3425, 2017. Disponível em: http://periodicos.pucminas.br/index.php/virtuajus/article/view/15745. Acesso em: 26 nov. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 10 abr. 2020.

BRASIL. **Decreto-lei nº 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 mar. 2020.

BRASI. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 20 mai. 2020.

BRASIL**. Lei nº 8.069, de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Aceso em: 20 mar. 2020.

BRASIL. **Lei n° 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: 10 nov. 2019.

BRASIL. **Lei n° 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: 26 nov. 2019.

BRASIL. **Lei n° 12.965, de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 26 nov. 2019.

BRASIL. **Lei n° 11.829, de 25 de novembro de 2008.** Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm. Acesso em: 26 nov. 2019.

BRASIL. **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/L9609.htm>. Acesso em: 10 abr. 2020.

BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998.** Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9610.htm>. Acesso em: 10 abr. 2020.

BRASIL. **Lei n° 9.983, de 14 de julho de 2000.** Altera o Decreto-lei n.º 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm. Acesso em: 26 nov. 2019.

BRASIL. **Lei n° 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 26 nov. 2019.

BRASIL. **Lei n° 12.034, de 29 de setembro de 2009.** Altera as Leis nos 9.096, de 19 de setembro de 1995 - Lei dos Partidos Políticos, 9.504, de 30 de setembro de 1997, que estabelece normas para as eleições, e 4.737, de 15 de julho de 1965 - Código Eleitoral. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12034.htm. Acesso em: 26 nov. 2019.

BUDAPESTE. **Convenção sobre o Cibercrime.** Budapeste, 23 de setembro de 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: 22 mai. 2020.

CAIADO, Felipe B.; CAIADO, Marcelo. **CRIMES CIBERNÉTICOS. COLETÂNEA DE ARTIGOS.** Ministério Público Federal, 2ª Câmara de Coordenação e Revisão. Volume 3, CDDir 341.532, 2018, disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-deartigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 26 nov. 2019.

CARRES, Amanda Francisca do Nascimento; MADRO, Edinei Carlos Dal; PEREIRA, Jhonatan. Crimes Virtuais e a Problematização do Direito. **Revista Unoeste.** Paraná: Xii Encontro Científico de Ciências Sociais Aplicadas de Marehal Candido Rondon,

Fronteira: Aspectos Sociais, Jurídicos E Econômicos, Universidade Estadual do Oeste do Paraná – UNIOESTE – 28 a 30 de novembro de 2017.

COELHO, Ana Carolina Assis. **Crimes Virtuais:** Análise da prova. Dissertação (Monografia). Faculdades Integradas "Antônio Eufrásio de Toledo", Faculdade de Direito de Presidente Prudente, Presidente Prudente/SP, 2008. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/Direito/article/view/827>. Acesso em: 18 mai. 2020.

COURI, Gustavo Fuscaldo. **Crimes pela Internet.** Dissertação (Pós Graduação) Escola da Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, 2009. Disponível em: <https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2009/trabalhos_22009/GustavoFuscaldoCouri.pdf>. Acesso em: 20 mai. 2020.

CONSELHO DA UNIÃO EUROPEIA. **O Conselho Europeu.** União Europeia: Edifício Europa, ISBN 9789282463802, 2018.

DOMINGOS, Fernanda Teixeira Souza; RODER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição da Internet. In: MARCONDES, Cecília Maria Piedra et al. (orgs). **Investigação e prova nos crimes cibernéticos.** São Paulo: Cadernos de Estudos, Escola de Magistratura da Justiça Federal da 3ª Região – EMAG, TRF3, 1ª ed., 2017. Disponível em: <https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf>. Acesso em: 20 mai. 2020.

FERREIRA, Ivette Senise. **Direito e Internet:** aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2005.

GONÇALVES, Andrea Sodré; PEREIRA, Raíssa Reis; CARVALHO Maria do Socorro Almeida de. Aspectos sobre os crimes cibernéticos: a necessidade de leis específicas. **Revista Judicare.** Alta Floresta/MG: Revista Eletrônica da Facudade de Direito de Alta Floresta. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/da_ausencia_de_legislacao_especifica_para_os_crimes_virtuais.pdf>. Acesso em: 25 nov. 2019.

GOMES, Helton Simões. Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE. **Revista G1.** São Paulo: Globo Notícias, Brasileiros online somam 64,7% de toda a população; dados são de pesquisa de 2016 do IBGE, Publicado em 21/02/2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml. Acesso em: 25 nov. 2019.

HARVARD LAW REVIEW. **Child Pornography, The Internet, and The Challenge of Updating Statutory Terms**. Disponível em: https://harvardlawreview.org/wp-content/uploads/pdfs/vol_122_child_%20pornograph_%20the_Internet.%20pdf. Acesso em: 25 nov. 2019.

LIMA, Larissa da Rocha Barros. **A proteção aos direitos autorais e o acesso à informação:** cultura, downloads e cópia privada na internet. Dissertação (Mestrado) Universidade Federa de Alagoas – UFAL, Faculdade de Direito de Alagoas – FDA, Programa de Pós-Graduação em Direito – PPGD, Mestrado em Direito Púbico, Maceió/AL, 2010. Disponível em: <http://www.repositorio.ufal.br/bitstream/riufal/3889/1/A%20prote%C3%A7%C3%A3o%20dos%20direitos%20autorais%20e%20o%20acesso%20%C3%A0%20informa%C3%A7%C3%A3o%20cultura%2C%20downloads%20e%20c%C3%B3pia%20privada%20na%20internet.pdf>. Acesso em: 10 abr. 2020.

JACINTO, Clébio Wilian. **Dos crimes virtuais.** Dissertação (Monografia). Faculdades Integradas, Curso de Pós-Graduação "Lato-Sensu" Direito Penal e Processo Penal, Presidente Prudente/SP, 2014.

MIRABETE, Julio Fabbrini. **Código Penal Interpretado.** São Paulo: Editora Atlas, 2003.

MOLINA, Antônio Garcia-Pablos de; GOMES, Luiz Flávio. **Criminologia.** São Paulo: Revista dos Tribunais, 2011.

NETO, Pedro Américo de Souza. **Crimes de informática.** Monografia. Universidade do Vale do Itajaí – UNIVAI, Centro de Ciências Sociais e Jurídicas – CEJURPS, Curso de Direito, Itajaí, 2009. Disponível em: <http://siaibib01.univali.br/pdf/Pedro%20Americo%20de%20Souza%20Neto.pdf>. Acesso em: 20 mar. 2020.

OAB - SÃO PAULO. **Gestões Anteriores. 2010.** Sede em São Paulo: Disponível em: <http://www.oabsp.org.br/comissoes2010/gestoes-anteriores/direito-eletronico-crimes-alta-tecnologia>. Acesso em: 25 nov. 2019.

OLIVEIRA, Alisson Cortez. **Crimes Cibernéticos:** ordenamento jurídico brasileiro. Dissertação (Monografia), Faculdade São Lucas, Porto Velho, 2015.

PINHEIRO, Emeline Piva. **Crimes virtuais:** uma análise da criminalidade informática e da resposta estatal. Dissertação (Monografia). Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, 2006. Disponível em: https://pt.slideshare.net/mrojr/artigo-crime-virtual. Acesso em: 25 nov. 2019.

RONCADA, Rodiner. A prova da materialidade delitiva nos crimes cibernéticos. In: MARCONDES, Cecília Maria Piedra et al (orgs). **Investigação e prova nos crimes cibernéticos.** São Paulo: Cadernos de Estudos, Escola de Magistratura da Justiça Federal da 3ª Região – EMAG, TRF3, 1ª ed., 2017. Disponível em: <https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf>. Acesso em: 20 mai. 2020.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, Ministério Público do Estado de São Paulo, 2004.

SANTOS, Coriolano Aurélio de Almeida Camargo; FRAGA, Ewelyn Schots. As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico. São Paulo: Comissão dos Crimes de Alta Tecnologia. Editora OABSP “A cultura é um Direito”, 2ª Edição, 2010.

SILVA, João Miguel Almeida da. **Cibercrime:** O crime de pornografia infantil na internet. Dissertação (Mestrado). Universidade de Coimbra. Especialidade em Ciências Jurídico-Forense, Faculdade de Direito, 2016. Disponível em: <https://estudogeral.sib.uc.pt/handle/10316/34801?mode=full>. Acesso em: 10 abr. 2020.

SOUZA, Henry Leones de. Da ausência de legislação específica para os crimes virtuais. **Revista Judicare.** Alta Floresta: Revista Eletrônica da Faculdade de Direito de Alta Floresta. 2011. Disponível em: <https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais>.Acesso em: 25 nov. 2019.

SOUZA, Gills Lopes Macêdo; PEREIRA, Daliana Vilar. **A Convenção de Budapeste e as leis brasileiras.** Dissertação (Monografia). 1º Seminário Cibercrime e Cooperação Penal Intenacional, organizado pela CCJ da UFPB e pela *Association Internacionale de Lutte Contra La Cybercriminalite* (França), João Pessoa/PB, maio de 2009. Disponível em: <http://www.charlieoscartango.com.br/Images/A%20convencao%20de%20Budapeste%20e%20as%20leis%20brasileiras.pdf>. Acesso em: 20 mai. 2020.

SOARES, Samuel Silva Basilio. Os crimes contra honra na perspectiva do ambiente virtual. **Revista Âmbito Jurídico.** São Paulo: O seu portal jurídico da internet, 2016. Disponível em: <https://semanaacademica.org.br/system/files/artigos/artigo_-_dos_crimes_virtuais_-_ambito_0.pdf>. Acesso em: 20 mar. 2020.

TORRES, Rhuan Thyego Pinheiro. **Crimes virtuais.** Dissertação (Monografia). Centro Universitário Toledo, Araçatuva, 2016. Disponível em: <https://servicos.unitoledo.br/repositorio/bitstream/7574/525/1/CRIMES%20VIRTUAIS%20-%20RHUAN%20THYEGO%20PINHEIRO%20TORRES.pdf>. Acesso em: 30 mar. 2020.

WENDT, Emerson; JORGE, **Higor Vinicius Nogueira. Crimes Cibernéticos: ameaças e procedimentos de investigação.** Rio de Janeiro: Editora Brasport, 2013. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=iGY-AgAAQBAJ&oi=fnd&pg=PA1&dq=WENDT,+Emerson%3B+JORGE,+Higor+Vinicius+Nogueira.+Crimes+Cibern%C3%A9ticos:+&ots=OrIZJF88Wt&sig=D_ZrUv7rOAPPuTz5lF7DW5lJC7k#v=onepage&q&f=false>. Acesso em: 20 mar. 2020.