CENTRO UNIVERSITÁRIO DR. LEÃO SAMPAIO – UNILEÃO
CURSO DE GRADUAÇÃO EM DIREITO

ARTHUR MANOEL DA SILVA SANTOS

O PROCESSO INVESTIGATÓRIO NOS CRIMES VIRTUAIS À LUZ DA LEGISLAÇÃO BRASILEIRA E DA CONVENÇÃO DE BUDAPESTE

Juazeiro do Norte
2020

ARTHUR MANOEL DA SILVA SANTOS

O PROCESSO INVESTIGATÓRIO NOS CRIMES VIRTUAIS À LUZ DA LEGISLAÇÃO BRASILEIRA E DA CONVENÇÃO DE BUDAPESTE

Artigo apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Dr. Leão Sampaio, como requisito para a obtenção do grau de bacharelado em Direito.

Juazeiro do Norte
2020

ARTHUR MANOEL DA SILVA SANTOS

O PROCESSO INVESTIGATÓRIO NOS CRIMES VIRTUAIS À LUZ DA LEGISLAÇÃO BRASILEIRA E DA CONVENÇÃO DE BUDAPESTE

Trabalho de Conclusão de Curso apresentado à coordenação do curso de Direito do Centro Universitário Dr. Leão Sampaio, como requisito para obtenção de grau de Bacharelado em Direito.

Aprovado em: _____/_____/_____

BANCA EXAMINADORA

_____

IAMARA FEITOSA FURTADO LUCENA
Orientador(a)

_____

FRANCISCO ERCÍLIO MOURA
Avaliador(a)

_____

RAIMUNDO CARLOS ALVES PEREIRA
Avaliador(a)

O PROCESSO INVESTIGATÓRIO NOS CRIMES VIRTUAIS À LUZ DA LEGISLAÇÃO BRASILEIRA E DA CONVENÇÃO DE BUDAPESTE

Arthur Manoel da Silva Santos[1]
Iamara Feitosa Furtado Lucena[2]

RESUMO

O presente trabalho tem por objetivo investigar as dificuldades enfrentadas pelas autoridades brasileiras quanto ao processo de investigação dos crimes cibernéticos, verificando conceitos e o histórico dos crimes virtuais, bem como fazer uma análise dos cibercrimes no ordenamento jurídico brasileiro e no direito internacional. A pesquisa relevante para o Direito, principalmente no que diz respeito à atuação das autoridades policiais, exibindo as dificuldades enfrentadas, quando se trata de crimes virtuais. Com o avanço tecnológico, facilitou bem mais a comunicação entre as pessoas em vários fatores, tais como profissional, social, pessoal, etc., todavia além de suas vantagens, essas novidades na tecnologia trazem consigo suas desvantagens, dentre elas, os crimes praticados no ciberespaço. Embora o avanço tecnológico ajude bastante em alguns aspectos, as autoridades brasileiras enfrentam grandes obstáculos para que os crimes virtuais sejam investigados e possivelmente solucionados, tanto pela dificuldade de aplicar uma punição para aqueles que praticam ilícitos no ciberespaço, como pela ausência de delegacias e peritos especializados para solucionar os crimes praticados pela internet. Desta forma, a investigação acaba sendo tardia e complicada, em que acaba na maioria dos casos ocorrendo à prescrição daqueles crimes quando se identifica o verdadeiro infrator, facilitando e explicando como vai se inovando os golpes, que são praticados através da internet. O projeto irá tentar contribuir para que possa preencher essas lacunas, analisando tais dificuldades através da legislação brasileira, no que diz respeito à quebra do sigilo independente de que se tenha ordem judicial, dando um passo para motivar o processo penal, no que diz respeito, ao procedimento investigatório nos crimes virtuais, tentando ajudar para que a forma de investigar seja mais rápida e competente, para que assim chegue ao determinado infrator, podendo também tranquilizar os usuários que se utilizam dos meios virtuais com sua finalidade principal, qual seja a comunicação em seus aspectos sociais, profissionais e pessoais, em que com isso tanto terá vantagens para o procedimento investigatório como para a sociedade. Contudo diante da pesquisa espera-se sensibilizar a classe jurídica, no que tange a essa polêmica na legislação brasileira, em relação a grande importância que se tem a investigação criminal, assim como os valores das provas obtidas para que possam ser combatidos os ilícitos praticados através da internet. Para isso, será utilizada a pesquisa bibliográfica de método qualitativo e natureza básica.

Palavras-chave: Crimes Cibernéticos. Ciberespaço. Processo Investigatório. Convenção de Budapeste. Crimes Virtuais.

ABSTRACT

This paper aims to investigate the difficulties faced by the Brazilian authorities regarding the cybercrime investigation process, verifying concepts and the history of cybercrimes, as well

1Discente do curso de direito da UNILEÃO. Email: arthursantos_06@hotmail.com
2Docente do curso de direito da UNILEÃO. Email: iamara@leaosampaio.edu.br

as analyzing cybercrimes in the Brazilian legal system and international law. The relevant research for the Law, mainly with regard to the performance of the police authorities, showing the difficulties faced, when it comes to virtual crimes. With technological advances, it has made communication between people much easier on various factors, such as professional, social, personal, etc. However, in addition to its advantages, these innovations in technology bring with them their disadvantages, among them, the crimes practiced in the cyberspace. Although technological advances help a lot in some aspects, the Brazilian authorities face great obstacles for virtual crimes to be investigated and possibly solved, both due to the difficulty of applying punishment to those who practice illegal activities in cyberspace, as well as the absence of police stations and specialized experts. to solve crimes committed by the internet. In this way, the investigation ends up being late and complicated, in which in most cases it ends up in the prescription of those crimes when the real infringer is identified, facilitating and explaining how the scams that are practiced through the internet are innovating. The project will try to contribute so that it can fill these gaps, analyzing such difficulties through Brazilian legislation, with regard to the breach of confidentiality regardless of whether there is a court order, taking a step to motivate the criminal process, with regard to the investigative procedure in virtual crimes, trying to help so that the way of investigating is faster and more competent, so that it reaches the specific offender, and can also reassure users who use virtual media with their main purpose, which is the communication in its social, professional and personal aspects, in which it will have both advantages for the investigative procedure and for society. However, in view of the research, it is expected to sensitize the legal class, regarding this controversy in Brazilian legislation, in relation to the great importance of criminal investigation, as well as the values of the evidence obtained so that the illicit acts practiced through from Internet. For that, the bibliographic search of qualitative method and basic nature will be used.

Keywords: Cyber crimes. Cyberspace. Investigative process. Budapest Convention. Virtual Crimes.

1 INTRODUÇÃO

O presente trabalho irá abordar sobre o processo investigatório dos crimes virtuais à luz da legislação brasileira e da Convenção de Budapeste, uma vez que as autoridades brasileiras enfrentam dificuldades para penalizar criminosos que praticam crimes virtuais, partindo da hipótese de que essas dificuldades não são ligados totalmente à falta de legislação específica no ordenamento jurídico brasileiro, mas talvez pela ausência de instrumentos tecnológicos, delegacias e peritos especializados, para combater os determinados crimes.

O artigo irá tentar contribuir para que se possa preencher essas lacunas, analisando as dificuldades através da legislação brasileira, dando um passo para motivar o processo penal, no que diz respeito ao procedimento investigatório nos crimes virtuais, sugerindo alternativas para que a forma de investigar seja mais rápida e competente, podendo tranquilizar os usuários dos meios virtuais.

O objetivo principal será investigar as dificuldades que as autoridades brasileiras enfrentam no que diz respeito, ao processo de investigação dos crimes no ciberespaço. São diversas essas dificuldades, que podem levar à impunidade daqueles que praticam os ilícitos no meio virtual, passando então para a sociedade uma visão de que no Brasil não há legislação específica tratando-se desses crimes. Todavia ao longo do trabalho demonstra-se algumas leis recepcionada pelo ordenamento jurídico brasileiro tratando de ilícitos virtuais, como por exemplo, a Lei nº 12.737/12 (Lei Carolina Dieckmann), bem como a Lei nº12.965/14 (Lei do Marco Civil da Internet).

Dentre os objetivos gerais, serão abordados conceitos dos crimes virtuais, traçando seu contexto histórico. Além de identificar as dificuldades enfrentadas pelas autoridades brasileiras no processo investigatório dos crimes, no ciberespaço, fazer uma análise da legislação brasileira e da Convenção de Budapeste sobre os crimes cibernéticos.

A primeira seção do trabalho tem por finalidade, verificar o que são os crimes virtuais, sendo possível antecipar desde já que dizem respeito a qualquer ação ilícita executada através de computadores ou *smartphones*, podendo ser classificado em próprios ou puros quando praticados contra sistemas informáticos, e em impróprios ou mistos quando ferir direito à vida, liberdade, patrimônio ou honra.

A segunda seção tratará da legislação brasileira no que diz respeito aos crimes virtuais, em que a Constituição da República Federativa do Brasil traz consigo a proteção de dados, tendo em vista que somente no ano de 2012 o Brasil recepcionou lei para tratar de delitos através do meio virtual, isso pelo fato de que uma atriz brasileira teve seu computador invadido tendo fotos intimas divulgadas, e através desse fato surgiu a Lei nº 12.737/12, sendo denominada como Lei Carolina Dieckmann.

Quanto ao direito internacional, com a grande repercussão de crimes no ciberespaço originou-se a Convenção de Budapeste no ano de 2001 com a finalidade de ajustar normas penais tanto no direito material, como no processual em se tratando de crimes virtuais. O Tratado Internacional teve vigor em 01 (um) de julho de 2004, contando com 55 adesões ratificadas, e hoje conta com 5 (cinco) signatários, todavia apesar de ser relevante para o ordenamento jurídico brasileiro, o país não é um dos signatários da referida convenção.

No que diz respeito a competência para processar e julgar crimes cibernéticos, devem ser observados alguns requisitos, em que determinará se será da Justiça Federal ou da Justiça estadual. Ressalta-se que nos ilícitos em que não tiverem repercussão internacional, serão de competência Estadual, todavia, não basta ter repercussão internacional para competência ser

deslocada para Justiça Federal, deve ser analisada dentro do caso concreto as hipóteses previstas na Constituição Federal, em seu artigo 109.

O trabalho tem como característica metodológica a pesquisa bibliográfica e documental, de método qualitativo e natureza básica, sendo realizado através da análise de doutrinas, leis, tratado internacional, bem como artigos científicos disponíveis na internet. A pesquisa foi desenvolvida a partir do ano de 2019 entre os meses de fevereiro a junho, bem como no ano de 2020 do mês de janeiro ao mês de junho em que para realização da busca, foram utilizados os seguintes descritores: Crimes Cibernéticos; Crimes no Ciberespaço; Processo Investigatório dos crimes virtuais; Convenção de Budapeste; Crimes Virtuais.

2 BREVES CONSIDERAÇÕES SOBRE CRIMES VIRTUAIS

Para se chegar a uma definição de crime virtual, é essencial destacar que para se caracterizar o determinado crime, é indispensável o uso de um objeto eletrônico, como por exemplo, computador, smartphone, entre outros. Todavia, para atingir o que se almeja, que é cometer o crime virtual, é essencial que o objeto eletrônico tenha acesso a internet, ou seja, é como se o objeto eletrônico e a internet fossem dependentes entre si para a efetiva consumação do crime.

Castro (2003) dispõe que os crimes virtuais são aqueles executados por meio de computadores, contra os mesmos, ou por intermédio dele, ou seja, grande maioria dos crimes praticados ocorre por meio da internet, pelo qual é comum que o meio utilizado seja o computador. O uso do computador como instrumento essencial para a prática do crime cibernético se dá através de sua finalidade, entre diversas possibilidades. Conforme o minidicionário da língua portuguesa, de Antônio Augusto Soares Amora, o computador pode ser conceituado como: “Qualquer máquina com capacidade de receber informações, efetuar operações programadas e produzir uma saída em formato de números, textos, figuras, gráficos, sons, vídeos, etc.” (AMORA, 2013, p.160).

É notório, de acordo com o exposto acima, que um computador tem diversas atribuições, em que pode auxiliar as pessoas em várias funções de forma mais célere, todavia tornou-se um instrumento adequado tanto para vida profissional, como para vida pessoal, e com isso há aqueles maus intencionados, que fazem com que o uso de computadores se torne maléfico para sociedade. Pimentel (2018) relata que em meados dos anos 80 foi dado início aos primeiros estudos no âmbito dos crimes praticados por meio do computador, uma vez que já era uma ferramenta pessoal e de fácil acesso.

Pimentel (2018) dispõe ainda, que o patrimônio, a intimidade e a fé pública são bens jurídicos materiais que tem sua proteção prevista em lei, eram os principais a serem violados por meio do computador, mas além desses, outros valores imateriais que ainda não eram protegidos pelo Direito também sofriam violação. Todavia, nota-se que as ferramentas informáticas compostas por sistemas e dados eletrônicos se apresentam vulneráveis e valiosos. Lima (2011 apud PIMENTEL, 2018) define o disposto acima como: "um 'bem jurídico' informático que reclama, em consequência, uma proteção legislativa própria. São exemplos dos novos bens jurídicos que advém da informática os dados eletrônicos, o sigilo e a segurança da informação" (PIMENTEL, 2018, p. 24).

É ampla a denominação das condutas ilícitas exercidas por meio de computadores ou que se direcionem a sistemas e banco de dados informáticos, quais sejam: "crimes virtuais", "crimes cibernéticos", "crimes digitais", "crimes de informática", "delitos computacionais", "crimes eletrônicos", "cibercrimes", entre outras. Crespo (2015) dá preferência às denominações: "virtual" e "cibernético", para esses ilícitos cometidos no meio digital. Dispõe que virtual é algo que não se encontra na realidade e cibernético é um termo que não é mais utilizado e está ligado a uma comparação do desempenho do cérebro com os computadores.

À vista disso, a doutrina pátria traz consigo a denominação "crimes digitais" para mencionar tais práticas ilícitas através da internet, bem como classificações para esses ilícitos em que classificam como próprios ou puros, sendo aqueles praticados contra os sistemas informáticos e os dados que podem ser denominados também de delitos de risco informático; bem como são classificados impróprios ou mistos, são, por exemplo, aquelas condutas exercidas ilicitamente pelo meio digital contra os direitos à vida, à liberdade, ao patrimônio e à honra (CRESPO, 2015).

"Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação." (JESUS; MILAGRE, 2016). "Assim, temos que a informática não modificou, conforme salientado acima, o quanto preconizado pela teoria do crime, mas trouxe à baila um poderoso meio de consecução de condutas, delitivas ou não — o meio digital." (COSTA, 2011, p. 52).

Portanto, define-se como crimes virtuais qualquer ação no âmbito virtual em que deva se utilizar de instrumento tecnológico e internet, para prática de qualquer atividade, em que se espalham conteúdos ilegais, em ataque a um sistema, a honra, a privacidade, e o patrimônio do indivíduo. Vianna (2001) aborda dois tipos de classificação para os indivíduos que praticam os crimes cibernéticos, sendo assim classificados de forma objetiva: crackers de sistemas, aqueles que invadem computadores ligados em rede; crackers de programas, para

que possam utiliza-los quebram proteções de software, para parecerem cópias legítimas; pheakers são os profissionais em telefonia móvel ou fixa; desenvolvedores de vírus, worms e trojans, criam pequenos softwares que podem causar dano ao usuário; piratas de programas, clonam programas para fraudar direitos autorais; distribuidores de warez, publicam em suas páginas, softwares sem que seja autorizado pelos detentores dos direitos autorais.

Seguindo o entendimento de Vianna (2001) as classificações subjetivas são divididas pela sua forma de motivação, sendo então: curiosos, eles não causam danos à vítima, agem com curiosidade, para aprenderem novas técnicas; pichadores digitais, o objetivo deles é serem reconhecidos no mundo digital, têm uma pequena semelhança com pichadores de muros, sempre deixam seus pseudônimos; revanchistas, têm finalidade de vingança contra ex-patrão de empresa em que geralmente tenham trabalhado no setor informático; vândalos, agem com dolo, com a intenção de causar dano à vítima, podendo destruir todos os dados armazenados no seu computador ou fazer com que o computador não conecte a internet; espiões agem para obterem informações sigilosas da vítima, podendo ser de caráter profissional, político ou militar; cibertorroristas, aqueles terroristas virtuais, cuja finalidade direcionada a políticas, visando o furto de dados sigilosos; ladrões, aqueles que têm como objetivo o ataque a bancos para o desvio de dinheiro; e por fim os estelionatários têm o mesmo objetivo financeiro dos ladrões, porém visam obter números de cartões de créditos salvos em sites comerciais.

Aras (2001), por sua vez traz como exemplo as condutas em que se visam ferir um bem jurídico protegido pelo Direito Penal, utilizando-se do sistema, para ferir bem jurídico diverso do computador, como, quais sejam: crime de fraudes, em que atinge o patrimônio ou crimes de injúria, calúnia, difamação atingindo a imagem, honra e intimidade da vítima são os considerados crimes virtuais. Outros exemplos de crimes virtuais mais concretos são aqueles praticados por crackers em que se invadem o sistema, atacando por meio de vírus, como cavalos de troia, impossibilitando internautas de terem acesso aos sites, vindo a causar grandes prejuízos aos provedores.

Conforme expõe Rodrigos (2016), pouco importa que não exista lei específica em se tratando dos crimes virtuais, uma vez que a prática fraudulenta seja por meio de objetos tecnológicos, será caracterizado como crime virtual, ou seja, a lei penal será adaptada e os ofensores serão penalizados igualmente.

3 LEGISLAÇÃO BRASILEIRA QUANTO AOS CRIMES VIRTUAIS

Conforme ressalta Souza (2018), o Brasil é carente de legislação a respeito dos crimes virtuais, uma vez que não há norma específica que regulamente estes crimes. Todavia apesar dessa escassez de norma, pode ser possível punir aqueles que praticam os crimes virtuais com base em leis vigentes em relação ao tema, em conjunto com analogia, jurisprudência e doutrinas que podem contribuir para que sejam julgados esses delitos.

De acordo com Cruz e Rodrigues (2018) a Constituição Federal de 1988 recepcionou em seu primeiro capítulo a proteção dos dados, pelo qual a internet sucedeu-se no Brasil neste mesmo ano, uma vez que já existia antes mesmo da constituição de 1988, uma lei que tratava da Política Nacional de Informática e outras providências, como uma forma de prevenção. Até o ano de 2012 não foi criada nenhuma outra lei em se tratando da internet, todavia os crimes, que eram praticados por meio dela, eram julgados de acordo com a ação daqueles que praticavam os cibercrimes.

3.1 LEI Nº 12.737/12: "LEI CAROLINA DIECKMANN"

Crespo (2015) expõe que a lei de nº 12.737/12 foi publicada em dezembro do ano de 2012, em que passou pelo período de 120 dias em *vacatio legis,* sendo denominada de "Lei Carolina Dieckmann". A denominação da lei leva em conta o fato ocorrido no início de 2012 com a atriz Carlina Dieckmann, em que teve seu computador pessoal invadido por hackers, e através disso teve fotos íntimas divulgadas.

Seis meses após o ocorrido foram recepcionadas duas leis a "Lei Azeredo" nº 12.735/12 e a "Lei Carolina Dickmann" nº 12.737/12 no ordenamento jurídico brasileiro em que alterou o Código Penal, Código Penal Militar e a Lei de Preconceitos dispondo sobre a caracterização de crimes cibernéticos, alterações estas previstas nos artigos 1º, 4º e 5º da referida lei.

A Lei Carolina Dieckmann em seu artigo 2º acrescentou no Código Penal o que diz respeito à invasão de dispositivos informáticos que está exposto nos artigos 154-A e seus parágrafos em que tipifica a conduta do agente que invadir dispositivo informático de outrem sem seu consentimento, podendo está conectado ou não à internet, cuja finalidade seja obter, adulterar, destruir, produzir, oferecer, distribuir, vender os dados ou informações contidas nos dispositivos. E no artigo 154-B, que dispõe que a ação será pública condicionada à representação, com exceção quando o crime for praticado frente à administração pública direta ou indireta (União, Estado, Município ou Distrito Federal) ou contra empresas concessionárias de serviços públicos, em que a ação será Pública Incondicionada.

Em análise aos artigos cabe uma crítica quanto à postura do legislador, em que se nota então que o mesmo não se preocupava com os crimes virtuais propriamente ditos, mas sim com o momento em que a imagem íntima de uma pessoa famosa estava sendo exposta em público, e com objetivo de proteger a si mesmo dispõe no parágrafo 5º do art. 154-A do Código Penal uma pena maior quando praticado contra representantes do legislativo, executivo e judiciário.

Porém trouxe vantagens, no que toca a definição da invasão à privacidade no ambiente virtual, visando preencher a lacuna no ordenamento jurídico brasileiro, em que alterou o Código Penal como mencionado acima protegendo as fotos, vídeos, documentos de intimidade própria que se encontram nos aparelhos tecnológicos de cada indivíduo.

3.2 LEI Nº 12.965/14: "LEI DO MARCO CIVIL DA INTERNET (MCI)"

Pimentel (2018) ressalta que a Lei nº 12.965/14 resulta de projeto originado no ano de 2009. O MCI tem por objetivo solucionar lides sobre atribuições de provedores de conexão e uso a internet, até mesmo quando confronta os direitos dos internautas. Expões ainda que tais conflitos eram resolvidos com base no Código Civil e Código de Defesa do Consumidor, porém, não satisfazia os interesses em conflitos.

Assim nas palavras de Frischeisen (2016, p. 148/149), "Não é à toa que o MCI, disciplinado na Lei 12.965, de 23 de abril de 2014, chama-se Constituição da Internet". A lei tem como foco à liberdade e à privacidade em que elenca princípios tratando-se de direitos e deveres não somente dos usuários da internet, mas também dos portais e sites, das prestadoras de serviços e do Estado.

A Lei em seu artigo 2º traz fundamento no que diz respeito a liberdade de expressão, expondo em seus incisos: o reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; e a finalidade social da rede. (LEI Nº 12.965, 2014).

A lei ainda em seu artigo 5º, inciso I traz a definição de internet, sendo, portanto o sistema constituído do conjunto de protocolos lógicos, estruturando em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes; (LEI Nº 12.965, 2014).

Conforme artigo 4º e seus incisos, da Lei nº 12.965/14 todos tem o direito ao acesso à internet, à informação, ao conhecimento e à participação na vida cultural e na condução dos

assuntos públicos, à inovação e fomento à ampla difusão de novas tecnologias e modelos de uso e acesso, bem como a adesão a padrões tecnológicos abertos que permitam a comunicação, à acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Contudo, Souza (2018) aborda que é dever do Estado normatizar atos frente à internet que é resguardada por princípios constitucionais, fiscalizar as irregularidades que decorem através do uso da internet, vindo a caracterizar o crime virtual.

3.3 *REVENGE PORN* (PORNOGRAFIA DA VINGANÇA)

Não há lei específica em se tratando da pornografia da vingança, porém o Código Penal recepcionou em seu artigo 218-C §1º uma pena para aqueles que praticarem o determinado ilícito.

Como já dito, os crime cibernéticos se caracterizam através do uso de objetos como computadores, smartphones, por exemplo, em que pode ser ofendida a honra e a integridade da vítima. Crespo (2015) expõe a pornografia da vingança como uma violência moral, em que o agente divulga conteúdos íntimos da vítima nas redes sociais, sem o consentimento desta, e por sua vez na maioria dos casos, mesmo que por um período curto, tiveram uma relação de afeto.

Todavia, o termo pornografia da vingança diante do entendimento de Burgério, (2015) consiste na divulgação em redes sociais de fotos, vídeos de conteúdos íntimos, sexo a dois ou grupal ou qualquer conteúdo semelhante, vindo a ser circulada e desse fato cause enorme constrangimento na vítima, tendo o agente o objetivo de se vingar com a determinada conduta.

O Código Penal Brasileiro (1940) em seu art. 218-C dispõe sobre a importunação sexual em que assegura a restrição da liberdade do agente podendo cumprir pena de 1 a 5 anos quando do fato não constituir crime mais grave, em seguida no seu §1º traz uma pena mais branda, uma vez que o crime for praticado por agente que mantém ou até já manteve uma relação de afeto com a vítima, dispondo então sobre a pornografia da vingança, pelo qual enseja no oferecimento, na trocar, na disponibilização, transmissão, na venda ou distribuição, na publicação ou divulgação, por qualquer meio de 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.

O determinado ato ilícito é praticado com frequência, em que na maioria dos casos as vítimas são mulheres, sendo assim, o legislador visando proteger à privacidade, liberdade,

dignidade e moralidade estabeleceu penalidade mais branda para os infratores. Todavia, percebe-se que as condutas frequentes, que se passam pelo mundo virtual são apenas um reflexo do que acontece no mundo real, em que o bom caráter, e a ética deveriam prevalecer, tanto no meio digital como no dia-dia das pessoas.

4 CRIMES CIBERNÉTICOS À LUZ DO DIREITO INTERNACIONAL

Com a grande repercussão dos ilícitos praticados através da internet, alguns países, como por exemplo, Argentina, Canadá, Estados Unidos, Japão, Suécia, entre outros da União Europeia não hesitaram, e como forma de precaução, adaptaram suas leis internas para evitar litígios provenientes do ciberespaço (CIDRÃO; MUNIZ; ALVES, 2018).

O desenvolvimento de redes pelo crime organizado e seus aliados, com distribuídas práticas em todo o mundo, vem afetando amplamente a economia na esfera nacional e internacional, no campo político, da segurança, bem como da sociedade como um todo, tendo em vista que o fato das atividades criminosas serem internacionais, não causam conflitos entre organizações criminosas, mas criam-se alianças no crime organizado, sendo ainda mais prejudicial (CASTELLS, 2007).

Vale ressaltar que é grande a dificuldade em se tratando da definição do tempo e do lugar de determinado ilícito virtual, todavia ressaltam Cidrão, Muniz e Alves (2018), que esta dificuldade encontra-se associada com o lugar em que se executam, englobando, portanto, jurisdição de diversos países, causando dúvidas em relação a competência para processar e julgar os infratores.

Para que essa controvérsia seja esclarecida surge a figura dos Tratados e Convenções Internacionais, uma vez que o mundo virtual atravessa fronteiras de qualquer país, é evidente que apenas leis nacionais consigam trazer a definição da competência, tempo, lugar e qual seria a lei mais específica por determinado ato ilícito. (CIDRÃO; MUNIZ; ALVES, 2018).

Boiteux (2004) esclarece que no desenvolver de leis internacionais, bem como em debates sobre os ilícitos praticados na internet, conclui-se que no âmbito nacional não há método para soluciona-los, devendo, portanto essa questão ser discutida na esfera internacional, pelo fato da influência direta da globalização, em que rapidamente a prática destes ilícitos atravessa os limites dos países.

Ainda seguindo o entendimento de Boiteux (2004), a maior finalidade das convenções e tratados internacionais, é “internacionalizar” (entre os países membros) normas, em que facilite que os países signatários resolvam questões envolvendo o cibercrime. A presença de

inúmeras leis nacionais voltada ao combate do cibercrime pode ser um obstáculo, ou seja, a criação com o intuito de resolver o problema, pode vir a ser uma divergente da outra em determinados aspectos, em que acaba muita das vezes atrapalhando, não sendo determinada lide resolvida. Sendo assim, nota-se que facilitando a cooperação internacional, será a maior vantagem para conter ilícitos através do mundo virtual.

4.1 *STATUS* QUE OS TRATADOS ASSUMEM NO ORDENAMENTO JURÍDICO BRASILEIRO

De antemão vale ressaltar sobre o *status* que os tratados assumem no ordenamento brasileiro, uma vez que GONÇALVES (2012) relata que os tratados de direitos humanos compreendem natureza e características distintas de outros tratados, decorrendo essa distinção através do contexto histórico dos tratados sobre direitos humanos, uma vez que a adesão desses tratados ocorre através da vontade do Estado, comprometendo-se formalmente a proteger e promover os direitos humanos, cuja finalidade é proteger as vítimas.

Encontram-se duas teorias pelo qual explicam o vínculo entre o direito interno e o direito internacional: teoria monista, defende a presença de ordem única das normas internas e internacionais; teoria dualista resguarda a presença de duas ordens diferentes, com propósitos diferentes. A prevalência dos direitos humanos finaliza essa controvérsia, devendo tanto o direito interno, como o direito internacional estar direcionados a efetivação dos direitos da pessoa humana, devendo em caso de conflito de norma (interna ou externa) aplicar a que satisfazer os direitos humanos, tendo em vista que a Constituição Federal prevalece sobre os tratados. (GONÇALVES, 2011)

Há quem defenda que os tratados sobre direitos humanos detêm *status* de lei ordinária sendo, portanto a minoria, como também ainda tem quem defenda que aqueles tratados aprovados anteriores a EC45/2004 possuem a mesma hierarquia de lei federal, bem como há sustentação que tais tratados em todo o tempo possuíram *status* de norma constitucional. Sendo assim, faria sentido modificar o §3º da CF/88, permitindo que a Constituição Federal fosse alterada mediante tratado. (GONÇALVES, 2011 *apud* MANZZUOLI).

4.2 CONVENÇÃO DE BUDAPESTE

Criada em 21 de setembro de 2001, em que conta com mais de quarenta países signatários, pelo qual África do Sul, Canadá, Estados Unidos da América e Japão prezam pela

necessidade da criação de normas adaptadas a evolução da tecnologia, propondo elaborar política criminal com o intuito de proteger a sociedade contra infrações no ciberespaço (MUNIZ; CRIDRÃO; ALVES, 2018).

Conforme a *Council Of Europe* (2017), o Tratado Internacional cuja finalidade seja ajustar as normas penais tanto no direito material quanto no processual, passou a vigorar no dia 01 de julho do ano de 2004, pelo qual contou com 55 adesões ratificadas, e hoje conta com 5 (cinco) países signatários. É a ferramenta jurídica mais abrangente que procura por meio da cooperação internacional combater os ilícitos no mundo virtual, bem como aborda acerca da desobediência aos direitos autorais, pornografia infantil, fraude por meio de computadores, tratando também da segurança de rede de computadores.

Boiteux (2004) ressalta que os escritores da Convenção de Budapeste deram destaque aos aspectos de competência, bem como do direito material e processual, tendo em vista que o objetivo da convenção não é tão somente criar novos tipos penais, mas também adequar normas processuais penais ao direito penal internacional.

No que diz respeito ao direito material, a Convenção de Budapeste tipificando os crimes cibernéticos supracitados acima, deixou de fora as contravenções como o terrorismo cibernético e o jogo ilegal através da internet, assim, cabe ao Estado à decisão de torná-las ilícitas as determinadas práticas. No que diz respeito às condutas ilícitas estipuladas na Convenção, todas deve haver a figura do dolo, não se admitindo a conduta culposa, ou seja, a conduta pelo meio virtual deve ter a total intenção de praticar o ilícito. Cabe ainda ressaltar que no tocante a responsabilidade de pessoa jurídica a Convenção limita-se a expor que poderá ser nas três esferas, qual seja, administrativa, civil ou criminalmente. (BOITEUX, 2004).

Quanto à alteração da norma local, a Convenção de Budapeste somente exige o comprometimento e a adoção pelos países signatários em seus sistemas jurídicos, não havendo exigência de uma mera cópia, permitindo que possa se utilizar de conteúdos semelhantes ao disposto na Convenção (MUNIZ; CRIDRÃO; ALVES, 2018).

Seguindo o entendimento de Muniz; Cidrão; Alves (2018) na atualidade somente há a Convenção de Budapeste como mecanismo jurídico internacional que possa combater os crimes cibernéticos, todavia o Brasil não é signatário da referida Convenção. A adesão a Convenção seria relevante para a ordem jurídica do Brasil, pois se tratando de ilícito virtual há uma divergência quanto à competência e atuação territorial das autoridades nacionais, visto que há um limite a determinada jurisdição para que seja aplicada a lei nacional. Pelo caráter internacional da Convenção os países signatários terão como vantagem a adequação das

normas jurídicas quanto aos crimes praticados pela internet, ajudando de forma efetiva no combate de tais crimes.

4.3 POSSÍVEL ADESÃO PELO BRASIL

Conforme disposto no artigo 37 da Convenção de Budapeste, pelo fato do Brasil não ser um dos signatários da Convenção de Budapeste, só será possível um ingresso a esta, mediante convite do Comitê de Ministros do Conselho Europeu, em que será decido pelo voto unanime dos representantes dos Estados membros, ainda assim, é bastante provável o consentimento para a entrada do Brasil, uma vez que ainda há certo vínculo entre os principais países europeus e o Brasil.

Todavia mesmo o Brasil não sendo integrante, não afasta a possibilidade da criação de normas que possam tipificar e combater os crimes virtuais.

5 O PROCESSO INVESTIGATÓRIO

Expõem Lessa e Vieira (2017) que o primeiro ponto para o estudo da investigação do cibercrime é a existência da denúncia do crime virtual, sendo preciso à identificação da ferramenta utilizada para execução do ilícito (*facebook, whatsapp, e-mail, website,* etc), uma vez que para cada uma há uma forma diferente de investigação. Como forma de precaução a obtenção e até mesmo a destruição de dados através de ataque digital, é de suma importância à proteção do computador em que será utilizado na investigação para obtenção dos dados.

5.1 EVIDÊNCIAS NO ESPAÇO CIBERNÉTICO

Conforme Wendt e Jorge (2013) as evidências são conceituadas pelas provas de uma incidência delituosa, em que se relacionam com o local pelo qual teria ocorrido determinado crime. No que diz respeito às evidências no meio virtual, são exemplos desta as amostras de registros de sessões, registros de navegação da internet e registros de login.

As provas colhidas em averiguação dos ilícitos virtuais possuem extrema fragilidade, uma vez que a qualquer tempo é grande o risco da perda destas, desse modo, como forma de prevenção da perda ou modificação se faz necessário à preservação das provas obtidas desses delitos. Todavia há mecanismos específicos para análise, conservação, apresentação e

obtenção, que são necessários para dar juridicidade a essas evidências virtuais (LESSA; VIEIRA, 2017).

Cassanti (2014) entente que é extremamente importante salvar arquivos, como por exemplos imagens através do PrintScreen, bem como páginas da internet no qual se relacionem a determinado delito, uma vez que são frágeis essas evidências, de modo que poderão ser deletadas facilmente, inclusive ser modificadas com o intuito de ocultar o crime. O próximo passo é o registro dessas provas em ata notarial no cartório, para que possa dar a fé pública, tornando-a apta para expor em juízo.

5.2 PROCESSO DE INVESTIGAÇÃO EM SITES NACIONAIS

Quando a autoridade policial tem conhecimento de determinado delito que se deu através da denúncia da vítima ou até mesmo por alguém interessado, é que se instaura o processo de investigação. Caso a denúncia seja pela publicação em website, Lessa e Vieira (2017) lecionam que o método de execução deverá ser dividido em três fases, sendo, portanto: obtenção de dados quanto ao endereço IP do servidor tanto que hospeda, como também o referente ao domínio do website, e por fim, a coleta do conteúdo do website. Faz-se necessária a análise completa do conteúdo de um website, uma vez que através das informações pode ser possível a obtenção de e-mails que facilite a identificação do infrator.

Conforme Cassanti (2014), uma vez que o sujeito causador do delito possua cadastro no site, para que seja fornecidas informações da origem do ilícito, é relevante acionar o provedor de serviços, sendo somente possível mediante ordem judicial, fazendo-se necessária para que possa requerer ao provedor, informações do sujeito que se conectou ao site. Salienta-se que a depender da situação, fará necessário o requerimento de ordem judicial exigindo quebra de sigilo dos dados pessoais do sujeito infrator para que seja possível localiza-lo (WENDT; JORGE, 2013).

Nos casos em que o acesso à internet está ligado a telefone móvel através das linhas 3G ou 4G, para que seja possível fornecer dados pela empresa responsável, também se faz necessária ordem judicial (LESSA; VIEIRA, 2017)

5.3 PROCESSO DE INVESTIGAÇÃO EM SITES ESTRANGEIROS

Não é muito diferente do método adotado em sites nacionais, porém tem a opção que é possível perquirir no site do órgão responsável pelo registro de sites do país específico, e, uma

vez que o site possua domínio genérico, é possível perquirir no respectivo site responsável pelo registro (LESSA; VIEIRA, 2017).

Na hipótese em que o provedor localiza-se em outro país, e não possuindo agência, filial ou sucursal no Brasil, se faz necessário o requerimento de cooperação internacional ao Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça. O DRCI é responsável por prestar informações de como será feito o pedido de cooperação. (WENDT; JORGE, 2013).

Todavia, quando no Brasil há repartição do provedor, conforme expresso no artigo 21, parágrafo único do Código de Processo Civil (CPC/2015), não se faz necessária o requerimento de cooperação. Neste caso torna mais ágil o processo de investigação, uma vez que pode demorar na resposta do país requerido de cooperação internacional, sendo, portanto prejudicial ao andamento da investigação (LESSA; VIEIRA, 2017).

Lessa e Vieira (2017) expõem que é possível também cooperação policial internacional, hipótese prevista no tratado *Network for Computer Crime Matters*, em que, no Brasil o setor de crimes virtuais da Polícia Federal é o responsável por tal rede.

Essa rede tem como finalidade tornar menos burocrática a pesquisa sobre legislação internacional, sendo relevante também no encaminhamento de pedidos de resguardo de evidências virtuais e na remoção de conteúdos que tenham relação a crimes cibernéticos (WENDT; JORGE, 2013).

6 COMPETÊNCIA DOS CRIMES CIBERNÉTICOS

A competência determina qual o local em que será iniciado o processo, como também em qual esfera judicial será apreciado o ilícito virtual, em que se destaca a *ratione materiae* (competência material) e *ratione loci (*competência territorial). A Justiça Federal é que possui a competência material, tendo em vista que esta será tratada nos casos de divulgações ou publicações de fotos, gravação ou outro registro de pornografia infantil através da internet, tendo em vista que o Brasil é signatário da Convenção sobre os Direitos da Criança (Decreto nº 99.710/90), bem como levando em consideração o disposto no artigo 109, inciso V da Constituição Federal de 1988 (CF/1988), pelo qual será de competência da Justiça Federal delitos que tenha a execução iniciada no Brasil, e tenha o resultado se dado ou não no estrangeiro (ou vice-versa), devendo também tal delito está previsto em tratado ou convenção internacional.

Tem-se como exemplo da regra citada o CC 112.616, pelo qual o STJ passou a entender que crime de difamação através de redes sociais, e tendo como vítimas crianças ou adolescentes, a competência para processar e julgar será da Justiça Federal pelo fato que fere direitos dispostos na Convenção sobre os Direitos da Criança, e ainda conforme o artigo 109, inciso V da CF/1988 poderá ter acesso ao site em que venha a ocorrer o ilícito, ainda que no exterior.

Nos ilícitos em que não tiverem repercussão internacional, a competência será da Justiça Estadual sendo, portanto residual conforme o art. 109 da CF/88, tendo como exemplo a troca de e-mails, vídeos ou fotos entre pessoas que residem em âmbito nacional. Lopes Jr. (2014) destaca que o fato de determinado ilícito ter caráter internacional não desloca a competência para Justiça Federal bem como não basta à mera presunção, sendo relevante que as hipóteses do artigo 109 da CF sejam comprovadas dentro do caso concreto.

Costa (2011) explana que até o momento atual não se tem norma possibilitando que o intérprete se posicione quanto à legislação aplicável ao delito cibernético, tendo em vista que, se faz necessária à determinação de qual lei seria aplicada, como também qual seria a jurisdição competente para apreciar assuntos distintos ali ocorridos. Para alguns países, determinadas ações na internet pode ser lícita, mas para outros não. Observa-se que não tem como regular esse espaço, porém a lei pode punir a conduta ofensiva através dele.

Apesar da lei não ser internacionalmente uniforme a respeito do que pode ser considerado crime ou não, é imprescindível a reunião de normas quanto àquela que será cabível, que até mesmo é um dos objetivos da Convenção de Budapeste. Tendo em vista o caráter criminoso dos crimes cibernéticos se aplica a mesma legislação dos crimes em geral, uma vez que o ordenamento jurídico brasileiro conhece as regras aplicáveis a lei penal. (COSTA, 2011).

Valin (2000) aborda que para os crimes cibernéticos teria que ser aplicada a teoria da atividade, destacando-se o local em que foi exercida a conduta, evitando-se a extradição do agente e tornando a averiguação mais célere e objetiva. Meira Junior (2007) se resguarda do mesmo pensamento e entende que jurisdição seria tanto o local das investigações, como onde se daria o processo e julgamento. Nesse contexto, seria mais aplicável a legislação do país onde ocorreu o crime, devendo respeito ao direito de defesa do acusado, a proteção na apuração de provas e agilidade em deter o criminoso.

Conforme Costa (2011) *apud* Chacon a melhor solução quanto ao julgamento de um delito virtual e em respeito ao princípio da ubiquidade, seria admitir a competência dos países abrangidos, mesmo podendo gerar conflitos de jurisdição.

O Código de Processo Penal (CPP) é quem prevê a competência territorial, estando disposta no artigo 69 do referido código, tendo como primeiro critério de competência o lugar em que ocorrer o ilícito. Por sua vez o Código Penal (CP) em seu artigo 6º determina o lugar do crime sendo competente o lugar em que ocorreu a ação ou omissão, bem como onde se produziu ou deveria produzir-se o resultado, em que esta regra trata-se da teoria da ubiquidade ou teoria mista.

O segundo critério de competência territorial, é o local de domicílio ou residência do réu, que será adotado nos casos em que se verifica que há mais de um juízo competente, causando o conflito de competências. Todavia nem sempre é possível localizar o réu no momento em que ocorreu a conduta ilícita, uma vez que há a possibilidade do ilícito ser praticado através de dispositivo eletrônico em *lan house* cuja localização seja em cidade distinta do domicílio do infrator (LESSA; VIEIRA, 2017).

Costa (2011) expõe que dada inexistência de fronteira na rede, torna-se digna de atenção mais específica à exposição do *locus delicti* nos crimes cibernéticos, tendo como exemplo os cassinos virtuais, em alguns países são considerados ilícitos, porém o servidor é inserido em país que permite que seja realizado o jogo, todavia o usuário conecta-se em um país em que o jogo é proibido, surgindo a questão a respeito da presença ou não de ilicitude.

Assim, a Convenção de Budapeste determinou em seu artigo 22,§5º que quando tiver relação a ilícito reconhecido pela convenção e reivindicação de competência por mais de uma parte, deverão as partes quando conveniente consultar-se para que determinem qual jurisdição mais adequada no processamento.

É necessário instituir adequação de normas de diversos países, bem como a regra quanto à aplicação da lei. Ademais, no Brasil é adotada a teoria da ubiquidade referente ao lugar do ilícito, em que o Brasil se considera competente quando ocorre determinado delito em seu território nacional. (COSTA, 2011 *apud* Gilberto Martins de Almeida).

Todavia, Costa (2011) aborda que caso o resultado e a conduta ocorram em países distintos, deve prevalecer o lugar da conduta. Desse modo deverá ser aplicada aos crimes virtuais a teoria da atividade no que diz respeito ao *locus delicti*, tendo em vista que pela teoria da atividade, a conduta não sendo ilícita no país em que se deu o resultado, será aplicada a legislação do país em que ocorreu a conduta.

Contudo dispõe o artigo 70, §3º do CPP, sendo também entendimento do STJ (HC 106074 PR) que em casos de incerteza quanto ao limite territorial ou quanto a jurisdição, a competência será fixada pela prevenção (RAMIRES, 2016).

7 CONSIDERAÇÕES FINAIS

O avanço tecnológico tornou bem mais fácil a comunicação entre as pessoas em vários fatores, tais como profissional, social ou pessoal. Todavia, além de suas vantagens, essas novidades na tecnologia trazem consigo suas desvantagens, dentre elas os crimes praticados no ciberespaço. Embora o avanço tecnológico ser de grande relevância, as autoridades brasileiras enfrentam grandes obstáculos para que os crimes virtuais sejam investigados e possivelmente solucionados, pela dificuldade de aplicar uma punição para aqueles que praticam ilícitos no ciberespaço.

Sendo assim, a investigação acaba sendo tardia e complicada, em que na grande maioria dos casos ocorre à prescrição daqueles crimes, quando se identifica o verdadeiro infrator, facilitando e explicando como vai se inovando os golpes, que são praticados através da internet.

Feita a análise dos principais pontos jurídicos do mundo virtual, nota-se a divisão da conduta criminosa no que diz respeito a classificação dos crimes virtuais, sendo portanto: próprios ou puros, aqueles praticados contra os sistemas informáticos e sobre dados, que podem ser denominados também de delitos de risco informático; bem como são classificados impróprios ou mistos, são, por exemplo, aquelas condutas exercidas ilicitamente pelo meio digital contra os direitos à vida, à liberdade, ao patrimônio e à honra.

Nota-se, portanto o envolvimento de dois binômios, tendo de um lado, a censura e a liberdade de informação, em que está disposta no art. 5º, IV — que inclusive é um direito fundamental — e no artigo 220 da Constituição Federal, pelo qual devem ser observadas as circunstâncias de informação ativa (informar) e passiva (ser informado), devendo manter equilíbrio nesses aspectos. Por outro lado, a privacidade e monitoramento, devendo haver defesa do monitoramento para que seja efetiva a identificação dos infratores virtuais, porém a monitoração fere a liberdade individual. Dessa forma o meio adequado para resolução aos crimes cibernéticos, é através da ponderação sob o prisma da razoabilidade nos âmbitos jurisdicional e legislativo.

Quanto ao direito internacional a solução para os crimes cibernéticos é a Convenção de Budapeste, sendo o instrumento jurídico de maior abrangência, em que se busca através da cooperação internacional, meios ao combate dos delitos virtuais. A referida convenção conta com 55 adesões ratificadas, e com 5 (cinco) países signatários, lembrando que o Brasil ainda hoje não é dos países que aderiram a Convenção de Budapeste, contando somente com a Lei

Carolina Dieckmann e o Marco Civil da Internet, sendo na prática insuficiente ao combate dos cibercrimes.

Em Análise ao Marco Civil da Internet, nota-se um problema quanto ao direito à privacidade, como também ao sigilo, em que se faz necessária ordem judicial para obtenção de informações essenciais para a investigação, objetivando identificar o verdadeiro infrator. Outro problema encontrado é quando se verifica no delito envolvimento de outros países, pelo fato que o Brasil não é signatário da Convenção de Budapeste, dificultando na cooperação internacional. Ainda nesse contexto, se faz necessária que a Administração Pública invista nos órgãos da segurança pública, através do preparo de peritos na área criminal, bem como em delegacias especializadas no aspecto dos crimes cibernéticos.

REFERÊNCIAS

_____. Código de Processo Penal. **decreto lei nº 3.689**, de 03 de outubro de 1941. Disponível em: http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm. Acesso em: 22 jan 2020

AMORA, Antônio Augusto Soares. **Minidicionário da língua portuguesa**. Editora Saraiva, 2013.

ARAS, Vladimir. Crimes de informática. **Uma nova criminalidade**. 2001. Disponível em: <https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em: 12 de maio de 2019.

BARROS, Thiago. **Internet completa 44 anos; relembre a história da web**. 2013. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-hiatoria-da-web.html>. Acesso em: 28 de abril de 2019.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais.** São Paulo: Revista dos Tribunais, 2004.

BRASIL. "Lei Carolina Dieckmann". Lei 12737/2012. Brasília, Novembro 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14/04/2017.

BRASIL. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25/06/2020.

BRASIL. Lei Azeredo. **LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012**, Brasilia, 2012.

BURÉGIO, Fátima. **Pornografia da vingança. Você sabe o que é isto?** Disponível em: <https://ftimaburegio.jusbrasil.com.br/artigos/178802845/pornografia-da-vinganca-voce-sabe-o-que-e-isto>. Acesso em: 21 de maio de 2019.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: BRASPORT, 2014.

CASTELLS, Manuel. **Fim do Milênio: A Era da informação: economia, sociedade e cultura**; v. 3, 4ª ed. Trad.: Klauss Brandini Gerhardt e Ronei de Venancio Majer. São Paulo: Paz e Terra, 2007.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** 2. Ed. Rio de Janeiro: Lumen Juris, 2003.

CIDRÃO, Taís Vasconcelos ; MUNIZ, Antonio Walber; ALVES, Ana Abigail. A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da Convenção de Budapeste à legislação brasileira. **Brazilian Journal of International Relations**. Disponível em: http://www2.marilia.unesp.br/revistas/index.php/bjir/article/view/7069. Acesso em: 5 fev. 2020.

CÓDIGO Penal de 1941. Disponível em: https://presrepublica.jusbrasil.com.br/legislacao/ 91622/codigo-processo-penal-decreto-lei-3689-41. Acesso em: 24/10/2019.

CONGRESSO NACIONAL. Lei 12.965/14. **Marco Civil da Internet**, Brasília, 2014.

COSTA, Fernando José da. ***Locus delicti* nos crimes informáticos**. 2011. Tese (doutorado) - Direito, Universidade de São Paulo - USP, 2011.

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 185**. 16 jun. 2017. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=44BgUu5q. Acesso em: 10 fev. 2020.

CRESPO, Marcelo. **Crimes digitais: do que estamos falando. 2015**. Disponível em: <https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/amp/?crimes-digitais-do-que-estamos-falando/>. Acesso em: 03 de maio de 2019.

DODGE, Raquel Ferreira. Ministério Público Federal. **Roteiro de Atuação Sobre Crimes Cibernéticos**. Brasília: 2ª Câmera de Coordenação e Revisão Matéria Criminal e Controle Externo da Atividade Policial, MPF, Brasília – DF, 2013.

FRISCHEISEN, Luiza Cristina Fonseca. 2ª Câmara de Coordenação e Revisão Criminal. **Roteiro de atuação: crimes cibernéticos**. MPF Brasília-DF, 2016.

GOMES, Helton Simões. **Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE; Brasileiros online somam 64,7% de toda a população; dados são de pesquisa de 2016 do IBGE**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>. Acesso em: 28 de abril de 2019.

GONÇALVES, Francysco Pablo Feitosa. **Ainda o *status* dos tratados sobre direitos humanos no direito brasileiro**. Disponível em: https://www.dropbox.com/s/rcsouq91xvn75h9/Fco%20Pablo%20Feitosa%20Goncalves%20Jose%20Antonio%20Albuquerque%20Filho%20-

%20Ainda%20o%20status%20dos%20tratados%20sobre%20direitos%20humanos%20no%20direito%20brasileiro%20variacoes%20sobre%20um%20mesmo%20tema.pdf?dl=0. Acesso em: 22 jun. 2020.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. [E-Book]

JORGE, Higor Vinicius Nogueira; WENDT, Emerson. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2. Ed. Rio de Janeiro: Brasport, 2013.

LESSA, Isabella Maria Baldissera; VIEIRA, Tiago Vidal. **Crimes virtuais: análise do processo investigatório e desafios enfrentados**. 5º simpósio de sustentabilidade e contemporaneidade nas ciências sociais. 2017. Disponível em: <http://www.fag.edu.br/contemporaneidade/sumario-2017>. Acesso em: 28 de abril de 2019.

MEIRA JUNIOR, Jóse de Castro. A tutela penal dos cybercrimes e o projeto de lei contra os crimes de informática. **Revista da Fundação Escola Superior do Ministério Público do Distrito Federal e Territórios**, Brasília, v. 15, p. 117-159, dez. 2007.

MELO, Adriana Zawada. Ministério Público Federal. **Crimes cibernéticos: Manual prático de investigação**. São Paulo: Procuradoria da República no Estado de SP, 2006.

PIMENTEL, José Eduardo de Souza. Introdução ao direito digital; An introduction to digital law. **Revista jurídica ESMP-SP**, v.13, 2018: 16-39.

RAMIRES, Bruno. **Conflitos de competência em matéria processual penal: competência territorial dos crimes cibernéticos**. 2016. Disponível em: https://jus.com.br/artigos/47505/conflitos-de-competencia-em-materia-processual-penal-competencia-territorial-dos-crimes-ciberneticos. Acesso em: 16 de março de 2020.

RODRIGOS. ABPERITOS, Instituto Brasileiro de Perícias Forenses. **O que são crimes virtuais?** 2016. Disponível em: <https://www.abperitos.com.br/web/2016/10/2019/o-que-sao-crimes-virtuais/>. Acesso em: 18 de maio de 2019.

SOUZA, Juliane Silva de. **Crimes Virtuais**. Porto Velho – RO, 2018. Disponível em: <http://repositorio.saoluca.edu.br:8080/xmlui/handle/123456789/2836>. Acesso em: 28 de abril de 2019.

VALIN, Celso. **A questão da jurisdição e da territorialidade nos crimes praticados pela internet**. In: VOVER, Aires José (Org.). *Direito, sociedade e informática*: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.

VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de Direito Penal Informático**. Disponível em: <http://www.bibliotecadigital.ufmg.br/dspace/handle/1843/BUOS-96MPWG>. Acesso em: 06 de maio de 2019.