CRIMES CIBERNÉTICOS E A EFICÁCIA DA LEGISLAÇÃO BRASILEIRA

Samuel Souza Pires[1]

Prof. Esp. Abizair Antônio Paniago[2]

RESUMO

A pesquisa investiga os crimes cibernéticos, ou seja, aqueles praticados no ambiente virtual, por meios telemáticos e sua conformidade com os preceitos instituídos na legislação atual, assim como, a eficácia dessas normativas em relação a proteção aos usuários da rede mundial de computadores. O objetivo geral é analisar os crimes cibernéticos no Brasil e a eficácia das normativas na proteção aos usuários na internet. Neste sentido, os objetivos específicos, pressupõem, abordar o conceito de crime cibernéticos, as vítimas e identificar o criminoso virtual, demostrar a importância das leis eficientes para punição desses crimes e apresentar a jurisprudência sobre o tema. Para realizar o estudo, foi necessário levantamento bibliográfico com uso de doutrina do Direito, jurisprudências, legislações que englobam os crimes cibernéticos. Portanto, chegou-se à conclusão que as normas editadas até o presente momento, não satisfazem a finalidade total para qual foram criadas, ou seja, reprimir a prática de crimes virtuais.

Palavras-chave: Ambiente Virtual; Crimes Cibernéticos; Eficácia; Legislação; Rede Mundial de Computadores.

1 INTRODUÇÃO

A pesquisa foi desenvolvida com o intuito de apresentar os crimes cibernéticos em outros termos, aqueles praticados no ambiente virtual, assim como, a importância de discussão do tema em conformidade com os preceitos instituídos na legislação atual e a eficácia dessas normativas na proteção aos usuários. O propósito da prática de crimes cibernéticos, é ganhar dinheiro com base nas informações coletadas de cada usuário ou por motivos pessoais, a invasão de um aparelho que esteja conectado à internet, se tornou um problema mundial que faz milhões de vítimas todos os anos.

Dentre as legislações brasileiras de proteção ao usuário na rede mundial de computadores, mais relevantes, cita-se a Lei Carolina Dieckmann (Lei 12.737/2012), o Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados (Lei 13.709/2018).

[1] Acadêmico do Curso de Direito do CEULP/ULBRA. E-mail: samuelsouzapires95@gmail.com

[2] Professor do Curso de Direito da Ulbra/Palmas. E-mail: Abizair.paniago@ulbra.br

Todas essas legislações têm como ponto em comum, oferecer tutela aos indivíduos que usam a rede mundial de computadores. E na seara internacional, o Tratado do Conselho Europeu sobre crimes cibernéticos.

Diante desse arcabouço normativo, o direito de privacidade dos usuários da internet, imposto pela Constituição de 1988, no artigo 5º, inciso X, poderá ser violando pela falta de eficácia das normas brasileiras de proteção à privacidade no ambiente virtual.

É ponto crucial, investigar se as leis regulamentadoras do ambiente virtual são condizentes com os desafios cotidianos encontrados no mundo virtual como o uso de dados pessoais, fraudes, comprometimento financeiro das vítimas, as consequências podem repercutirem além da esfera patrimonial, atrelando-se ao contexto moral de violação ao princípio da dignidade da pessoa humana.

Como objetivo principal do estudo, tem-se a abordagem dos crimes cibernéticos no Brasil e a eficácia das normativas na proteção aos usuários na internet. Este trabalho foi dividido em duas seções. Na primeira seção tratou-se sobre o conceito e origem dos crimes virtuais, além das fraudes financeiras e computacionais. Na última seção abordou-se sobre a complexidade dos crimes cibernéticos em comparação a eficácia das normas brasileiras de punição aos crimes cibernéticos.

Tendo por base que a internet, é constantemente utilizada para cometimento de crimes, se tem como propósito acadêmico e social, demonstrar a exigência de mais rigor das leis para punir e prevenir os eventuais crimes. Esse estudo pode esclarecer e demonstrar que a internet não é um lugar seguro, ao contrário disso, é um espaço perigoso, portanto, faz-se necessária a explanação, para que os crimes virtuais possam ser reduzidos e com isso, menos pessoas se tornem vítimas da sua própria exposição virtual.

Ademais, a metodologia utilizada envolve pesquisas na legislação, nas doutrinas, em artigos e decisões jurisprudenciais. Para realizar o estudo, foi necessário levantamento bibliográfico com uso de doutrina do Direito, jurisprudências, legislações que englobam os crimes cibernéticos.

2 DEFINIÇÃO E TIPOS DE CRIMES CIBERNÉTICOS

Antes de tratar da temática proposto na presente pesquisa, faz-se por necessário apresentar a conceituação do que venha a ser ambiente digital, visto ser esse o meio pelo qual as práticas delituosas são cometidas com a utilização da rede mundial de computadores, e, a partir desse escopo, verificar-se a legislação existente e aplicável aos crimes cibernéticos.

Outra questão relevante a ser abordada é a quanto à evolução dos crimes cibernéticos, devido ao crescimento da internet e do ambiente virtual, resultando na exposição de quantidade incalculável de pessoas que são diretas ou indiretamente afetadas, tendo suas vidas e informações expostas, facilitando práticas ilícitas por parte daqueles que utilizam o ambiente virtual para cometer vários crimes.

Por consequência, faz-se mister apreciar se as leis que existem são suficientemente eficazes para possibilitar a realização de investigações que condução à apuração dos crimes cometidos e a individualizar as respectivas autorias, residindo aqui o ponto mais difícil de se atingir.

2.1 ATAQUES A SISTEMAS COMPUTACIONAIS E FRAUDES ELETRÔNICAS E FINANCEIRAS

Sabe-se atualmente que o avanço tecnológico social, embora traga enormes benefícios a todos os campos da existência humana, também traz consigo ameaças de várias ordens, devido a abrangência da rede mundial de computadores, na medida em que a internet possibilitou uma alta disseminação de informações e conhecimentos, o que, notadamente, também propicia a atuação de criminosos por meio de ataques a dispositivos e subtração de informações (dados públicos e/ou privados), desse modo, os quais se acham armazenados e disponibilizados em sites, que via de regra estão alocados em computadores interligados a internet que são chamados de servidores.

Dentre os diversos incidentes de segurança ocorridos na internet, grande parte está relacionada ao uso de *malwares* (programas maliciosos) inseridos em sistemas computacionais, com o objetivo de comprometer a confidencialmente, integridade ou a disponibilidade dos dados pessoais da vítima, dos seus aplicativos ou próprio sistema operacional, assim, ocasionalmente acarretando prejuízos financeiros a centenas de pessoas (DIORO E OUTROS, 2018).

Nesse cenário, os *malwares* podem infectar ou comprometer o computador e sistemas computacionais, passando o criminoso a ter acesso a dados de usuários ou empresas, ali armazenados. Desse modo, resta claro que os *malwares* representam uma ameaça aos sistemas computacionais na sociedade atual.

A par da inquestionável importância e até essencialidade da rede mundial de computadores e da internet na atualidade, é certo também afirmar que ela permitiu uma mudança drástica na disseminação de dados, possibilitando que milhares de computadores

possam ser atacados em poucas horas de modo a causar mau funcionamento do dispositivo ou perda de arquivos, e. infelizmente, até o “roubo” de dados.

Na sequência, há inúmeras formas de programas danosos que são utilizados em ataques em contato direito com a vítima, por meio de telefonemas, ou até mesmo pessoalmente o que exige um planejamento antecipado e detalhado, além de articulação, os ataques indiretos normalmente a vítima é influenciada por sentimentos de curiosidade, ambição e medo, e aproveitando-se disso, o criminoso monta armadilha (BOMFATI; 2020).

Para ganhar a confiança das vítimas, o criminoso se aproveita da ingenuidade delas, usando simbolismos de marcas ou instituições conhecidas e confiáveis como bancos, órgãos públicos, visando obter informações pessoas ou invadir computadores. Assim, as mudanças ocorridas em relação às novas tecnologias, permitiram o desenvolvimento dos meios de comunicação e informação em uma velocidade extrema. Porém, os mesmos meios digitais são usados como massa de manobra por criminosos.

Não são incomuns as oportunidades que, através de recursos eletrônicos, os agentes delituosos transferem de forma fraudulenta valores de contas bancárias fazendo uso da ferramenta de internet *banking*. Segundo dados do instituto Synovate, realizada em 2017, o Brasil é o terceiro país em número de fraudes via internet banking, possuindo em média uma fraude a cada 16 segundos conforme o Serasa (SANTOS, 2021).

A jurisprudência do Superior Tribunal de Justiça, no julgamento do Conflito de Competência nº 115.690/Distrito Federal, de relatoria do Ministro OG Fernandes, sintetizou o entendimento que a transferência fraudulenta de recursos de contas bancárias por meio da internet configura o crime de furto qualificado e não o delito de estelionato (BRASIL, 2011).

Após as alterações introduzidas pela Lei nº 14.155/2021 no Código Penal (Decreto-lei 2.848/1940), foi inserido ao artigo 171, que dispõe sobre o estelionato, o § 2º-A, tipificando-se a fraude eletrônica:

> Fraude eletrônica
>
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
>
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
>
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

É notório que a grande maioria dos usuários da rede mundial de computadores, não tem conhecimento que ao utilizar um computador ou outro dispositivo eletrônico para acessar a rede gerará registros em suas ações, ao contrário do que pensam não estão seguras ao navegar na rede. Assim, o deslumbre pela internet torna boa parte dos usuários suscetíveis a ataques e fraudes eletrônicos, até mesmo golpes financeiros. Esses crimes podem estar presentes em inúmeros ambientes cibernéticos tipificados no ordenamento jurídico-penal brasileiro como é o caso do estelionato.

2.2 EVOLUÇÃO TECNOLÓGICA E SURGIMENTO DE NOVOS DELITOS

Conforme se observa do panorama atual, é inquestionável que a internet tornou a vida das pessoas melhor, mas também não se pode negar que trouxe consigo efeitos colaterais, como a prática de delitos cibernéticos, valendo-se da revolução tecnológica, iniciada no Brasil nos anos 1990, e da redefinição global que possibilitou o uso da tecnologia de informação e conhecimento, surgindo o ambiente virtual, onde são supridas as fronteiras, podendo-se atingir milhões de pessoa em qualquer lugar do mundo e ao mesmo tempo (BARRETO; BRASIL, 2016).

Em decorrência da revolução tecnológica, a internet despontou mundialmente como uma ferramenta necessária para o cotidiano social, ao otimizar a distribuição de informações e conhecimentos. No mesmo passo que a evolução dos recursos tecnológicos, as ameaças praticadas via computador se aprimoraram com o passar dos anos.

A informação sobre programas de computador que se autorreplicam remontam ao final da década de 1950. Porém, não existe uma posição pacífica sobre quando surgiu o primeiro vírus de computador, havendo registros de que em 1986 surgiram os primeiros, sendo denominados de cavalos de Troia, devido à forma furtiva que adentravam nos sistemas operacionais. Com a popularização de dispositivos utilizados para o acesso à rede mundial de computadores, também surgiram nos meios para difusão de ameaças. No ano de 2004 surgiu o primeiro vírus de celular, oriundo das Filipina Denominado Cabir, criado para infectar esses aparelhos móveis (WENDT, 2021).

Atualmente, não se tem como imaginar um mundo sem internet e sem os aplicativos de mídias sociais que permeiam sobre as relações sociais ou mesmo sem celulares e outros dispositivos móveis. Os avanços tecnológicos se traduzem em uma verdadeira revolução cibernética, na qual as fronteiras são frágeis e as comunicações são instantâneas. Os crimes se multiplicaram em espécie e quantidade no meio virtual, ao ponto que fora criada uma estrutura

jurídica para penalização das condutas criminosas praticadas na rede mundial de computadores (BARRETO; BRASIL, 2016).

A evolução das práticas maliciosas nos meios eletrônicos, realizadas por condutas indevidas em computadores ou dispositivos móveis implicam em ações prejudiciais, intituladas como crimes cibernéticos. A definição de crime está na Lei de Introdução ao Código Penal (Lei 3.914/1941), ante a disposição do artigo 1º, entende-se por crime a conduta (ação ou omissão) cuja punição afeta a liberdade do indivíduo (BRASIL, 1941).

Os crimes cibernéticos são crimes plurilocais, pois normalmente a vítima e o criminoso estão em locais diversos ou ainda, pelo fato da execução do delito se iniciar em um lugar e a consumação ocorrer em outro, mas no mesmo país. (BARRETO FILHO, 2016)

No contexto geral, o crime é uma conduta não permitida legalmente, cuja punição é a mais severa de todas, pois afeta diretamente a liberdade do indivíduo. Por seu turno, a espionagem, invasão de privacidade, crimes sexuais, tudo isso sempre existiu, com leis a punir os infratores, consolidadas no ordenamento jurídico. Entretanto, com a internet, surgiram novas maneiras de praticar alguns crimes. Assim, o crime cibernético, é uma conduta, na qual ocorre a utilização de algum recurso de tecnologia da informação como meio para realizar a ilicitude (BOMFATI, 2020).

Muitos crimes cibernéticos são de autoria conhecida, nesses casos a vítima pode indicar a autoridade policial o autor e apresentar provas da materialidade delitiva. Não sendo possível identificar a autoria, além de averiguar a materialidade delitiva, cabe à investigação, identificar também os autores para garantir a punição. (MARTINS, 2020)

Diante de um cenário de avanço tecnológico e, consequentemente, o surgimento de crimes cibernéticos, necessitou-se de um acompanhamento das novas relações sociais desenvolvidas via internet, acelerando o dinamismo das normas jurídicas de modo a criminalizar condutas que ocorrem no meio digital com vistas a aprimorar a segurança jurídica e social. Nesse sentido, tem-se que a criminalidade no Brasil, é potencializada pelos crimes praticados nos meios eletrônicos, o que justificou uma atenção especial para tipificação dos crimes cibernéticos, conforme se verá a seguir.

2.3 LEGISLAÇÃO INTERNACIONAL E BRASILEIRA SOBRE CRIMES CIBERNÉTICOS

Após entender sobre o contexto histórico dos crimes cibernéticos no Brasil, é interessante abordar as previsões legais sobre os crimes cibernéticos previstas no país, e os

aspectos legais sobre a matéria no plano internacional. A revolução tecnológica emergida pelo fenômeno da globalização, resultou em novos anseios da sociedade contemporânea exigindo legislações para regulamentar a questão dos crimes virtuais. Assim, foram editadas normas internacionais e nacionais para disciplinar sobre a matéria, buscando a adequação legal da evolução da sociedade, para suprir suas necessidades regulando seu bem-estar.

Em que pese o Direito Penal brasileiro não respondesse as transformações sociais com adequação da legislação de forma imediata. A tipificação dos crimes cibernéticos no Brasil, aconteceu tardiamente em comparação com o contexto mundial e a criminalização de condutas virtuais.

O ordenamento brasileiro passou por um longo período de ausência de previsões legislativas adequadas a coibir as práticas danosas na rede mundial de computadores, que desde o início deviam ter sido classificadas pela Lei Penal como imorais e danosas, ou seja, tratadas como crime (SANTOS, 2020).

A primeira legislação específica a dispor sobre crimes cibernéticos foi a Lei nº 12.737, de 30 de novembro de 2012, apelidada de Lei Carolina Dieckmann, que dispõe sobre a tipificação dos crimes de informática, acrescentando ao Código Penal os artigos 154-A e 154-B, e alterando os artigos 266 e 298, também daquele Diploma Repressivo.

Na invasão de dispositivos informáticos ligados ou não a rede mundial de computadores, o bem jurídico tutelado é o constitucionalmente previsto direito à intimidade e à privacidade, que mesmo sem haver extração de conteúdo encontra-se violado a partir do momento em que um terceiro tem acesso a informações privadas que constam do computador pessoal de um determinado sujeito (SANTOS, 2020).

Além disso foram tipificadas criminalmente pela Lei 12.737/2012, as condutas de interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, ou de informação de utilização pública, incluindo também a falsificação de cartão de crédito (Arts. 266 e 298) (BRASIL, 2012).

A segunda legislação especifica a respeito dos crimes cibernéticos é a Lei 12.735/2012 (Lei Azeredo), visando caracterizar os crimes cibernéticos como ataques praticados por hackers e crackers, como as alterações indevidas de senha mediante uso de sistema informático (BRASIL, 2012). Cabe destacar que, anteriormente a Lei Carolina Dieckmann e a Lei Azeredo Outras leis esparsas foram incluídas no Código Penal brasileiro, cita-se:

> Inserção de dados falsos em sistema de informações (Incluído pela Lei nº 9.983, de 2000)
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
>
> Modificação ou alteração não autorizada de sistema de informações (Incluído pela Lei nº 9.983, de 2000)
>
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)

Essas disposições legais foram incluídas no Código Penal brasileiro pela Lei 9.983/2000, de modo a criminalizar condutas realizadas por meios informáticos que colocassem em risco os serviços da Administração Pública (BRASIL, 2000).

Outra legislação que já dispunha sobre crimes informáticos, era o Estatuto da Criança e Adolescente (Lei 8.069/1990), no artigo 241, visando abordar novos crimes cometidos contra crianças e adolescentes, ou seja, indivíduos vulneráveis dentro dos instrumentos informáticos (BRASIL, 1990).

Uma legislação de destaque, é o Marco Civil da Internet (Lei 12.965/2014). Contudo, essa legislação será abordada especificamente no próximo tópico. Dando seguimento, a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), alterou o Marco Civil da Internet, é a mais recente novidade legislativa voltada aos crimes cibernéticos sancionada em 14 de agosto de 2018 pelo Presidente da República à época, Michel Temer, torna-se de suma importância, ao consagrar os princípios fundamentais e controle de dados pelo titular (BARRETO FILHO, 2019).

Em 26 de dezembro de 2018, foi instituído também pelo Governo Federal, a Política Nacional de Segurança da Informação, por meio do Decreto 9.637/2018, cuja finalidade é assegurar a disponibilidade, integridade, confidencialidade, e a autenticidade da informação a nível nacional (BRASIL, 2018). Em função da inserção destes dispositivos, o ordenamento jurídico passa a ser capaz de praticar condutas que visem coibir ações prejudicais aos usuários, como roubo de senhas, divulgação de informações privadas, entre outras (MATTOS, 2020).

A primeira norma internacional com o escopo de combater os crimes cibernéticos eletrônicos resultou na chamada Convenção de Budapeste, que foi criada pelo Conselho da Europa, tendo entrado em vigor em 2004, e que, atualmente tem participação de mais de 20 países. O seu preambulo esclarece que tem como projeto principal uma política criminal

comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, através da adoção da legislação adequada e da melhoria da cooperação internacional. (SANTOS, 2020).

Segundo Bertholdi (2020, p. 33-34) são tipos previstos pela Convenção de Budapeste:

> Seção 1 - Direito penal material
> Título 1 - Infrações contra a confidencialidade, integridade e disponibilidade de sistema informáticos e dados informáticos
> Artigo 2º - Acesso ilegítimo.
> Artigo 3º - Interceptação ilegítima.
> Artigo 4º - Interferência em dados.
> Artigo 5º - Interferência em sistemas.
> Artigo 6º - Uso abusivo de dispositivos.
> Artigo 7º - Falsidade informática.
> Artigo 8º - Burla informática.
> Título 3 - Infrações relacionadas com pornografia infantil
> Artigo 9º - Infrações relacionadas com pornografia infantil.
> Artigo 10 - Infrações relacionadas com a violação do direito de autor e dos direitos conexos.

Durante muito tempo o Brasil não era signatário dessa Convenção, não obstante, em que pese o país não ter a ela aderido de fato, alguns trechos foram replicados ou inspirados na criação da Lei 12.737/2012, especialmente as infrações relacionadas com a confidencialidade, integridade e disponibilidade dos sistemas e dados informáticos (Capítulo II - Medidas a tomar a nível nacional).

Pode-se verificar que o Brasil não acompanhou por um grande lapso temporal a legislação penal informática, estando, por isso mesmo, atrasado, tendo positivado apenas uma parte das condutas internacionalmente entendidas como ofensivas a bens jurídicos. (BERTHOLDI, 2020). Somente em 2023, com o Decreto nº 11.491 de 12 de abril de 2023, que promulgou a Convenção sobre o Crime Cibernético, firmada em Budapeste, que o Brasil passou a aderir tal instrumento internacional, ampliando os laços de cooperação com parceiros estratégicos no enfrentamento aso crimes cibernéticos (BRASIL, 2023).

Evidentemente, a tipificação do crime cibernético exige a colaboração e preservação da comunidade internacional e territorial. Mas, ainda que o Brasil não seja signatário da Convenção de Budapeste, realiza a cooperação internacional ativa e passiva.

2.4 MARCO CIVIL DA INTERNET: RESPONSABILIDADE E PRIVACIDADE ONLINE

Por oportuno, explica-se os contornos da Lei 12.695, de 23 de abril de 2014, legislação que instituiu o Marco Civil da Internet no Brasil, com o objetivo de disciplinar questões

principiológicas acerca da utilização da internet e os direitos e garantias dos usuários. Com isso, trazendo consigo conceitos e procedimentos para disciplinar o ciberespaço.

O Marco Civil da Internet, é a Lei 12.965/2014, que contém trinta e dois artigos, estabelecendo garantias, direitos, deveres e responsabilidades de provedores, internautas, empresas e poderes Executivo, Legislativo e Judiciário. Essa legislação estabelece muitas situações de modo amplo, como conceitos, princípios e objetivos para regulamentação de outras legislações (BRASIL, 2014).

Destaque-se o inciso I, do artigo 4º do Marco Civil da Internet, prevê o direito de acesso à internet a todos os cidadãos:

> Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
> I - do direito de acesso à internet a todos;
> II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
> III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
> IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

O Marco Civil prevê ainda, no artigo 7º, que o acesso à internet é essencial ao exercício da cidadania, levando a considerar é essencial ao exercício, a inviolabilidade da privacidade e sigilo do fluxo das comunicações de dados dos usuários, protegendo a intimidade, a vida provada, a honra e a imagem das pessoas, em conformidade com o que prega o texto constitucional expresso no artigo 5º, inciso X. Esse artigo se associa ao artigo 3º do mesmo diploma que enumera, dentre outros princípios, o princípio da proteção da privacidade e dos dados pessoais (BRASIL, 2014).

Posto isto, quando se fala em tecnologia da informação e comunicação, diz respeito a não invadir a privacidade de alguém. O Marco Civil da Internet abordou esses aspectos, assegurando aos usuários da rede, a inviolabilidade e sigilo do fluxo das comunicações dos dados dos usuários, conforme exprime o artigo 7º. Essa questão da proteção de dados tem extrema importância na sociedade atual, onde as pessoas vivem hiperconectadas, lançando informações em inúmeros aplicativos e banco de dados diversos (públicos e privados), e toda essa informação pessoal deve ser protegida (BOMFATI, 2020).

A Lei foi editada, para garantir direitos aos usuários da internet e, para isso, também abordou as formas de identificação, investigação e responsabilização daquele que comete crimes cibernéticos (MARTINS, 2020).

O Marco Civil da Internet trata-se de uma legislação cuja finalidade é regular sobre as relações sociais entre os usuários da internet, na busca pela preservação da privacidade, da intimidade e da liberdade tecnológica. Outro aspecto, que é válido pontuar, tem a ver com a responsabilidade do provedor que vai possibilitar ao usuário o acesso à rede, que está esculpida no texto do artigo 12, do Marco Civil da Internet, que prevê:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Os artigos 10 e 11 da referida legislação, também preveem as penalidades para as condutas praticadas no artigo 12, que contemplam advertência, proibição de exercício das atividades, suspensão e multa. As mesmas regras são aplicáveis aos provedores estrangeiros, desde o momento que passam a prestar serviços no país (BRASIL, 2014).

Segundo a jurisprudência do Tribunal de Justiça do Distrito Federal e Territórios, a responsabilidade civil do provedor de internet por danos provocados por terceiros é subsidiária:

> APELAÇÃO. CONSTITUCIONAL E CIVIL. LIBERDADE DE IMPRENSA. RESPONSABILIDADE CIVIL. DANO MORAL. DIREITO DE IMAGEM. MATÉRIA JORNALÍSTICA. NOTÍCIA VEICULADA APÓS SUFICIENTE INVESTIGAÇÃO. FONTE FIDEDIGNA. VEROSSIMILHANÇA DO RELATO QUANTO AOS FATOS NOTICIADOS. DIREITO À INFORMAÇÃO. TEXTO MERAMENTE NARRATIVO. VERSÃO DO APELANTE. DEVIDA CONSIDERAÇÃO. INTERESSE PÚBLICO DE INFORMAR PRESERVADO. INEXISTÊNCIA DE ATO ILÍCITO. DANO MORAL NÃO RECONHECIDO. RESPONSABILIDADE SUBSIDIÁRIA DO PROVEDOR DE APLICAÇÕES DE INTERNET. PRESSUPOSTOS DE INCIDÊNCIA NÃO VERIFICADOS. AUSÊNCIA DE ORDEM JUDICIAL OU PEDIDO DA PARTE. OMISSÃO ILÍCITA. INOCORRÊNCIA. RESPONSABILIDADE NÃO CONFIGURADA. RECURSO CONHECIDO E DESPROVIDO. Recurso conhecido e desprovido. Honorários majorados. (BRASIL, 2021, sem página cadastrada)

Conforme a decisão a responsabilidade subsidiária do provedor de aplicações de internet por conteúdo gerado por terceiro (art. 18 do Marco Civil da Internet Lei 12.965/14) exige o descumprimento de prévia ordem judicial ou pedido do ofendido para a exclusão do conteúdo. Inexistente ordem judicial ou pedido do ofendido, ausente se mostra pressuposto

necessário à caracterização de omissão ilícita ensejadora de responsabilidade civil e impositiva do dever de indenizar (BRASIL, 2021).

Posto isso, o entendimento jurisprudencial pressupõe que a responsabilidade civil do provedor de internet por danos de terceiros, ocorrerá apenas nos casos em que estiver constatado o descumprimento de ordem judicial que determine a indisponibilização do conteúdo ilícito ou da permanência deste após a ciência sobre os fatos ocorridos.

Acertadamente, diante dos pontuado ao longo do capítulo, a Lei 12.965/2014, foi um enorme marco para o desenvolvimento da tipificação dos crimes cibernéticos no ordenamento brasileiro. Trata-se de uma alternativa do Governo a fim de promover a segurança dos usuários da rede mundial de computadores, assim como seus dados (no âmbito público e privado). Porém, algumas situações que envolvem os delitos virtuais continuam com lacunas.

3 DESAFIOS E COMPLEXIDADES DOS CRIMES CIBERNÉTICOS

Nos dias atuais, utiliza-se muito os meios tecnológicos, na maioria das vezes, para se comunicar e interagir, seja no trabalho ou lazer. Por outro lado, é preciso se atentar ao fato de que os criminosos virtuais carregam a arma do crime na mão, no bolso, bem perto do cidadão. Nesse cenário de aumento dos crimes cibernéticos a investigação desses crimes tem se tornado um desafio complexo, diante da variedade de crimes cibernéticos existentes.

3.1 FRONTEIRAS VIRTUAIS: DESAFIOS NA JURISDIÇÃO E COOPERAÇÃO INTERNACIONAL

Com o aumento de usuários no ambiente virtual, houve uma tutela jurisdicional envolvendo a proteção dos dados na rede mundial de computadores, tanto na esfera nacional como na internacional. A internet é um campo vasto em informações, sem barreiras físicas, o que dificulta a imposição de jurisdição para julgar essas demandas.

Esse aumento significativo da criminalidade cibernética no Brasil, está relacionado com o fato de que a web permite que os criminosos tenham franco acesso a um número incalculável de vítimas, especialmente em uma nação que não se preocupa com segurança no uso da internet, as técnicas utilizadas pelos crackers para ocultar as atividades dos criminosos, são extremamente complexas, raras vezes encontram resistências nas frágeis estruturas investigáveis e judiciais brasileiras (BERTHOLDI, 2020).

Apesar das legislações contra crimes eletrônicos representarem grande marco para o desenvolvimento da internet os problemas envolvem que envolvem a criminalização não podem ser ignorados, principalmente em razão das lacunas sem preenchimento, é o caso da competência para julgar os cibercrimes, que falta disposição específica, e traz insegurança jurídica (MATTOS, 2020).

Em um primeiro momento, o Marco Civil da Internet, no texto do artigo 11, dispõe sobre a jurisdição internacional de dados:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Assim, a transferência de dados virtuais no ordenamento jurídico brasileiro é regulada pelo artigo 11 do Marco Civil da Internet, estabelecendo-se também as transferências desses dados para órbita internacional. Os parágrafos § 1º, § 2º e § 3º do artigo 11 ordenam também sobre a imperatividade das leis brasileiras em detrimento de qualquer operação realizada no Brasil.

Outra legislação que trata sobre a transferência internacional de dados é a Lei Geral de Proteção de Dados Pessoais. No seu artigo 33 dispõe sobre a transferência de forma lícita para países e organismos internacionais que propiciem a proteção de dados nos mesmos termos descritos na legislação brasileira, no que se trata da proteção à privacidade dos dados pessoais em concordância com a Constituição Federal de 1988 (BRASIL, 2018).

O Direito brasileiro é contido, os estados dividem-se em fronteiras, jurisdições, limitando também a comunidade internacional, ou seja, a soberania de Estados e Organizações internacionais. A divisão dos territórios brasileiros impõe desafios, quando se trata de investigar e julgar uma conduta criminosa. Pois as provas de tais condutas podem se encontrar a milhares de quilômetros de onde os reflexos do crime foram sentidos (GUIDI; KEZEK, 2018).

Em decorrência da criação de várias normativas que vigoram em relação aos crimes virtuais. Proíbe-se a ideologia que a “internet é terra sem lei” e que o agente delituoso poderá ficar isento das responsabilidades cíveis e criminais. Nesse sentido, o artigo 21 da Convenção do Conselho da Europa sobre Crimes Cibernéticos ou Convenção de Budapeste (Decreto nº 11.491/2023) estabelece que “uma parte adotará as medidas legislativas e outras que sejam

necessários para estabelecer jurisdição sobre qualquer ofensa incluída na Convenção, quando a ofensa é cometida no seu território" (BRASIL, 2023).

Por outro lado, surge um problema decorrente dessa transferência internacional de dados. O direito brasileiro não especificou de forma clara e precisa, no Direito já positivado há dificuldade em se estabelecer a jurisdição responsável por um crime ocorrido no mundo virtual. Em algumas situações a legislação brasileira acaba não sendo suficiente para abranger as novas demandas advindas no mundo virtual. A jurisdição sobre demandas digitas, seja no Brasil ou em qualquer outro Estado, é um problema cotidiano que está longe de ser resolvido e ter um consenso mundial (BALDISSERA, 2019).

O Poder Judiciário tem atuado de forma tímida no que corresponde a jurisdição de fronteiras. Durante muito tempo, somente o Supremo Tribunal detinha competência para decidir sobre processos apresentados por órgãos estrangeiros. Após a Emenda Constitucional nº 45/2004 essa competência foi transferida para o Superior Tribunal de Justiça. No cenário da cooperação internacional, tem-se um protagonismo do Poder Executivo, especialmente o Ministério das Relações Exteriores (SCHULZE, 2015).

Nesse contexto, surge a cooperação judiciária internacional, a fim de possibilitar o cumprimento de pedidos realizados por um Estado no território de outro Estado, com regiões diversas, como ocorre no ordenamento brasileiro.

Para coleta de provas no exterior, os Estados usam de instrumentos como cartas rogatórias ou auxílio direto do Poder Judiciário, por força de tratados de cooperação judiciária. Porém, a inexistência de fronteiras no ambiente virtual repercute efeitos sobre a cooperação judiciário e obtenção de informações ou provas relacionadas aos crimes cibernéticos. Assim, as autoridades enfrentam o desafio de obter acesso, tempestivamente, aos dados armazenados em território estrangeiro, incluindo também a falta de delimitação do exercício da jurisdição executiva. Em outras palavras, é possível observar lacunas capazes de produzir ruídos entre Estados soberanos (OLIVEIRA, 2023).

Por essa razão, podem surgir casos de autoridades internacionais, que diante da urgência em conseguir informações sobre dados eletrônicos, passam a buscar meios alternativos para obtenção desses dados, especialmente em consequência da demora no fornecimento desses dados pela via diplomática.

Assim, a carta rogatória consiste em um instrumento de cooperação internacional. Uma segunda forma de cooperação é o auxílio diplomático. Por fim, cite-se que os tratados de mútua assistência judicial em matéria penal ou MLATs, criam também procedimentos de

cooperação capazes de conceder assistência internação no trâmite de um processo localizado em território estrangeiro (GUIDI; KEZEK, 2018).

Afinal, a cooperação entre organismos internacionais no fornecimento de dados virtuais, podem contribuir para inibição do aumento da criminalidade envolvendo crimes virtuais.

Recomenda-se um cuidado ao analisar um delito informático, na hora de se estabelecer a competência do processo e julgamento do delito, que poderá atender também as disposições do Código Penal brasileiro nos artigos 5º (territorialidade), 6º (lugar do crime) e 7º (extraterritorialidade) (BRASIL, 1940). Da mesma forma, o artigo 70 do Código de Processo Penal versa que o juízo competente será de acordo com o local da infração (BRASIL, 1941).

Dentre as dificuldades aduzidas, anota-se os diferentes sistemas jurídicos dos países, a variação entre as leis nacionais e internacionais, direcionados aos crimes cibernéticos, bem como a diferenciação na coleta de provas e no processo criminal de averiguação do crime cibernético. Diante dessas considerações, torna-se necessário a aproximação entre os Estados Cooperativos, a fim de aproximar-se as relações estatais. O Estado brasileiro precisa avançar em relação as questões de cooperação jurídica internacional.

3.2 EVIDÊNCIAS DIGITAIS E INVESTIGAÇÃO FORENSE

Os crimes digitais também envolvem os desafios da coleta e evidencias digitais por parte da autoridade policial que investigará delitos dessa natureza, pois a investigação de infrações penais praticadas por dispositivos eletrônicos exige a utilização de mecanismos adequados par coleta e extração das evidências.

A correta coleta dos dados digitais para forense digital envolve a colaboração entre profissionais da área do direito, da segurança policial e da informática. Caso o responsável pela investigação, não apreenda provas digitais de forma a serem usadas em um processo forense, essas informações (em sua maioria relevantes) podem ser perdidas, e o juízo a quo também poderá desconsiderar o uso dessa prova colhida de maneira inadequada (NASSIF, 2019).

A perícia forense computacional é “padronizada pela Norma ABNT NBR ISO/IEC 27037:2013 em relação ao tratamento das evidências digitais, processos de vital importância na investigação com a finalidade de preservar a integridade dessa informação com valor probatório” (OLIVEIRA; SANTIAGO; COSTA, 2023, p. 3.979).

Consoante a isso, a forma correta de coletar dados digitais apresenta desafios para extração de evidências. Além de tudo, a evidência digital somente será aceita em juízo desde

que a extração seja realizada por especialista em evidência digital, ou seja, um indivíduo que tenha conhecimento e aptidão para lidar com questões técnicas.

Desse modo, o direito a produção de provas é estabelecido na Constituição de 1988, no artigo 5º, inciso LVI que afirma "são inadmissíveis, no processo, as provas obtidas por meios ilícitos" (BRASIL, 1988, sem página). Essa disposição trata de uma garantia constitucional ao devido processo legal, sendo incumbência do Estado prestar a devida assistência jurisdicional. Por outro lado, o inciso LXIII, também do artigo 5º garante o direito do indivíduo em não produzir prova contra si mesmo, protegendo a produção de provas.

Para condenação pela prática de crime cibernético é necessária a comprovação de autoria, intenção, e a utilização dos meios informáticos por meios ilegítimos de acesso a dados, de forma a obter provas que confirmem a acusação, por isso, é preciso a realização de perícias em todos os dispositivos de armazenamento para obtenção de provas que fortifiquem, a condenação. Porém, deve-se atentar que as evidências digitais podem ser encontradas em dispositivos da vítima com alteração das configurações, arquivos, vírus, dentre outras ameaças operacionais e arquivos desconhecidos, o que pode prejudicar o uso dessa prova no bojo processual (OLIVEIRA; SANTIAGO; COSTA, 2023).

Ao se falar em evidências digitais é necessário lidar com um problema, a falta de veracidade nessa espécie de prova. Apesar do alto nível de confiabilidade da computação forense, a evidência ainda é considerada uma fragilidade, já que a coleta de forma errônea ou ilícita pode invalidar a prova e com isso corromper todo o processo investigatório e a perícia dos dados coletados. Deve-se observar um procedimento minucioso, que envolve várias fases, obtenção, preservação, validação, identificação, análise, interpretação e apresentação das evidências digitais. É função do perito digital encontrar dados e informações que ajudem a comprovar os fatos, como a identificação do local do crime, os suspeitos e a coleta de evidências que sejam consistentes para comprovação dos atos praticados ilicitamente (SILVA, 2017).

Ao executar esse trabalho de coleta de evidências, o perito precisa ter cautela, tomando os devidos cuidados para não invalidar as evidências e promover a segurança das informações coletadas, isso envolve uma execução complexa e minuciosa, além de amplo conhecimento técnico de como os sistemas computacionais funcionam. Por conseguinte, observa-se a importância do manuseio correto dos dados coletados pela perícia computacional durante a investigação forense, realizando a coleta das evidências conforme a cautela que o ordenamento brasileiro trouxe consigo no texto constitucional.

3.3 IDENTIFICAÇÃO E RASTREAMENTO DE ATORES MALICIOSOS

Destaca-se que a ausência de cooperação internacional entres os países, dificulta as investigações relacionados aos crimes cibernéticos, que exigem a harmonia entre leis tipificados por ambos os países em conflitos. Como visto, as solicitações de apoio internacional demandam muito tempo, produzindo resultados sobre a identificação e rastreamento dos agentes delituosos.

Não obstante, em pesquisa desenvolvida pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança gerenciada pelo Comitê Gestor de Internet no Brasil, no ano de 2017, foram relatados 833.775 incidentes dos quais, em sua maioria, foram na modalidade fraude na internet (MARTINS, 2020).

Assim, em linhas gerais, o aumento desses crimes representa crescimento acentuado, em relação aos crimes presenciais, seja pelo aumento do número de usuários, pelas vulnerabilidades existentes na rede ou a falta de atenção do usuário (MIRANDA, 2020).

Ante ao panorama social em que números de casos de crimes virtuais já superaram os crimes reais, ou seja, crimes presenciais, surge a necessidade da adoção de técnicas e ferramentas que possam identificar os praticantes desses crimes e com isso buscar diminuir sua ocorrência na internet. Apesar dos inúmeros benefícios, os recursos virtuais apresentam também riscos, como a prática de crimes cibernéticos que podem proporcionar transtornos e prejuízos a diversas vítimas.

O tipo penal parte da análise de um agente que procede com destreza e habilidade para praticar o crime. Pela internet, o criminoso sequer precisa manter contato com a vítima, se faz valer de uma ferramenta tecnológica para praticar o crime (BOMFATI, 2020).

Assim, é importante destacar que um facilitador dos delitos virtuais é a falta de conhecimento sobre o ambiente virtual, por parte da população, no manuseio da proteção de seus dados pessoais. A falta de conhecimento da sociedade eleva a capacidade de praticar delitos.

É certo que, ao contrário das vítimas, o criminoso utiliza de técnicas para aprimorar seus métodos fraudulentos, por meio de programas de camuflagem que deslocam os agentes para os paraísos cinéticos (mudança de localidade no âmbito da internet, dos conteúdos, de um servidor para outro, especialmente servidores que se encontram em território em que a conduta praticada não é tipificada na lei, além disso, inexistindo recursos para investigação (MATTOS, 2020).

A investigação dos crimes virtuais e o rastreio dos criminosos é tarefa árdua, uma vez que as fontes de prova e materialidade são os dados eletrônicos relacionados aos delitos. Entre as dificuldades encontradas, podem ser citadas três características: a primeira é o anonimato, que inclui a criptografia e a camuflagem dos dados de identificação. Em seguida, a transitoriedade, pois os dados eletrônicos em sua maioria, são transitórios e possuem prazo curto de armazenamento. Por fim, a fluidez, esse é o elemento mais complexo, por se constituir na ideia de que os dados eletrônicos são fluidos, podendo ser armazenados em qualquer lugar do mundo, transitar por várias jurisdições, sem possuir barreiras físicas (OLIVEIRA, 2023).

É importante destacar as características inerentes e específicas à criminalidade cibernética, quais sejam, as peculiaridades que distinguem esses delitos, dos demais, tais como a instantaneidade, a igualdade entre os usuários da rede mundial de computadores, a sensação de anonimato dos delitos e consequentemente a impunidade (MATTOS, 2020).

Os crimes cibernéticos representam grande desafio para legislação por apresentarem facilidades como anonimato, a desterritorialidade e a facilidade de valer-se dos meios empregados, um computador ou celular com acesso à internet instiga o criminoso a praticar o crime. Assim, há demanda para novidades legislativas que possam criar ferramentas de investigação. A totalidade das peças legislativas vigentes, não é eficaz na inibição da violação de dados ou aparelho informativos de cidadãos (SANTOS, 2020).

No ciberespaço a falta de conhecimento das vítimas gera proveito por parte dos criminosos. Outrossim, o anonimato representa garantia de sucesso a um ataque cibernético aliado a transitoriedade e fluidez dos dados armazenados.

Como percorrido, ao longo do estudo, a construção histórica nacional da tipificação dos crimes cibernéticos, é remanescente as edições internacionais relacionadas a esses crimes, fato este comprovado com a adoção tardia do Brasil como signatário da Convenção de Budapeste. Mesmo que a atual tipificação dos crimes cibernéticos represente um avanço significativos com a vigência das Leis Carolina Dieckmann, do Marco Civil da Internet e da Lei Geral de Proteção de dados. Entretanto, há muito ainda a ser percorrido, até que todos os delitos informáticos possam ser tipificados no ordenamento brasileiro.

4 CONCLUSÃO

Os crimes virtuais são cometidos através da rede mundial de computadores, ou seja, na internet, sendo que o agente delituoso se utiliza para prática dos delitos, computadores, telefones, tablets ou outros meios telemáticos.

Sabe-se que os impactos dos crimes cibernéticos na era tecnológica vão além do ambiente digital, trazem maiores prejuízos, como financeiros ou psicológicos, permitindo também a incidência de crimes como pornografia, ciber terrorismo, roubo e lavagem de dinheiro.

Tratar de crimes cibernéticos no ordenamento brasileiro, era um desafio, especialmente por um Código Penal tão omisso, somente a partir de 2012 que houve inserção de tipificação de crimes virtuais nas normas brasileiras, após a implementação da Lei Carolina Dieckmann (Lei 12.737/2012), seguida pelo Marco Civil da Internet (Lei 12.965/2014) e da Lei Geral de Proteção de Dados Pessoais. Isso pode ser resultado da chegada tardia da rede mundial de computadores no Brasil, somente em 1992 a primeira rede conectada à intermete foi implementada no país, nas principais universidades brasileiras.

Com o crescimento da internet e dos serviços digitais as pessoas tendem a se expor, colocar suas informações em sites sem certificação de segurança. Para, tanto, foi necessária a criação de leis para proteger esses usuários lesadas de alguma forma.

As condutas informáticas consideradas como crimes, comportam ofensas que vão além da esfera penal, enquanto bem jurídico agregado, ultrapassam os direitos de personalidade como a honra, a imagem das pessoas, conforme o que estabelece artigo 5º, inciso X, da Constituição de 1988. Ou seja, atingindo uma esfera extrapatrimonial que poderá prejudicar o indivíduo em seu íntimo, lesando sua dignidade como pessoa humana.

Diante dessas disposições legais, cada vez mais, verifica-se que o estado vem se preparando e aprimorando os seus agentes públicos para o enfrentamento desse problema. Todavia, a atualização trazida pelas novas regulamentações não é eficaz para preencher as lacunas, visto que ainda levará certo tempo para adaptação e conhecimento das normas pela sociedade.

O atraso nas políticas públicas pautadas na punição dos crimes virtuais, apresenta-se como empecilho para jurisdição, na coleta de provas envolvendo evidências digitais e na identificação e rastreio dos agentes delituosos que se aproveitam da falta de conhecimento informático das vítimas, para praticar os mais variados crimes cibernéticos.

Portanto, apesar de recentes, as leis de proteção à privacidade virtual estão preparadas para produzir efeitos jurídicos e sociais. Mas no caso prático são muito brandas para natureza dos crimes praticados na internet. As normas editadas até o presente momento, não satisfazem a finalidade total para qual foram criadas, ou seja, reprimir a prática de crimes virtuais. Sugere-se um maior rigor na imposição de normas direcionadas a punição dos crimes cibernéticos no ordenamento brasileiro.

REFERÊNCIAS BIBLIOGRÁFICAS

BALDISSERA, Wellington Antônio. Jurisdição e transferência de dados: desafios para a proteção do direito à privacidade. **Revista de Estudos e Comunicação da Universidade Católica de Santos,** ano 45, nº 126, 2019.

BARRETO; Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do Marco Civil da Internet.** Rio de Janeiro: Brasport, 2016.

BARRETO FILHO, Marcelo Vandré Ribeiro. **Os contornos jurídicos da lei geral de proteção de dados frente ao consumo no ambiente virtual.** Santa Rita, 2019. Disponível em: https://core.ac.uk/download/pdf/297213148.pdf. Acesso em: 02 set. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília/DF, 5 de outubro de 1988.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Código Penal.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal.

BRASIL. **Decreto-lei nº 3.914, de 9 de dezembro de 1941.** Lei de introdução do Código Penal (decreto-lei n. 2.848, de 7-12-940) e da Lei das Contravenções Penais (decreto-lei n. 3.688, de 3 outubro de 1941).

BRASIL. **Lei nº 9.983, de 14 de julho de 2000.** Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (e da Internet). Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, *caput*, inciso

IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023.** Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência nº 115.690/Distrito Federal,** Relator: Ministro OG Fernandes, Terceira Seção, julgado em 14/3/2011, DJe 28/3/2011.

BRASIL. Tribunal de Justiça do Distrito Federal. **Classe do Processo: 07165425920198070020 - (0716542-59.2019.8.07.0020 - Res. 65 CNJ),** Registro do Acórdão Número: 1369225, Data de Julgamento: 01/09/2021, Órgão Julgador: 1ª Turma Cível, Relator: Diva Lucy De Faria Pereira, Data da Intimação ou da Publicação: Publicado no DJE: 16/09/2021 . Pág.: Sem Página Cadastrada.

BERTHOLDI, Juliana. **Crimes informáticos.** Curitiba: InterSaberes, 2020.

BOMFATI, Claudio Adriano. **Crimes cibernéticos.** Curitiba: InterSaberes; 2020.

DIORO, Rafael Fernando; SERAFIM, Edivaldo; ALVES, Karlan Ricomini; MEIRA, Matheus Carvalho. Segurança da Informação e de Sistemas Computacionais: Um Estudo Prático sobre Ataques Utilizando Malwares. **Anais SULCOMP, v. 9 (2018).**

GUIDI, Guilherme Berti de Campos; KEZEK, Francisco. Crimes na internet e cooperação Internacional em matéria penal entre Brasil e Estados Unidos**. Revista Brasileira de Políticas Públicas,** volume 8, nº 1. Abr. 2018.

KOLBE JÚNIOR, Armando. **Investigação de crimes digitais.** Curitiba: Contentus, 2020.

MARTINS, Dheneb. **Investigação cibernética.** Curitiba: Contentus, 2020.

MATTOS, Marilia Soares de. **Núcleo de combate as cibercrimes.** Curitiba: Contentus, 2020.

MIRANDA, Sabrina Leles de Lima. O crescente uso da internet e o aumente de crimes cibernéticos. **Revista Renascer,** Futurando. ed. 53, 01, set. 2020.

NASSIF, Lilian Noronha. Os desafios de dados e em evidências digitais. **O Alferes,** Belo Horizonte, 74 (29): 89-107, jan./jun. 2019.

OLIVEIRA, Bianka Zloccowick Borner de. **Jurisdição e internet:** os desafios da cooperação internacional para a coleta de dados eletrônicos no combate aos crimes transnacionais Conteúdo Jurídico, Brasília-DF: 20 fev 2023, 04:27. Disponível em:

https://conteudojuridico.com.br/consulta/artigos/61081/jurisdio-e-internet-os-desafios-da-cooperao-internacional-para-a-coleta-de-dados-eletrnicos-no-combate-aos-crimes-transnacionais. Acesso em: 23 out 2023.

OLIVEIRA, Daiana Souza de; SANTIAGO, Vinicius Vale.; COSTA, Adriana Vieira da. Perícia forense computacional: a admissibilidade e a fragilidade das evidências coletadas via computação forense. **Revista Ibero-Americana de Humanidades, Ciências e Educação,** [S. l.], v. 9, n. 5, p. 3978–3997, 2023.

SANTOS, Flavio Augusto de Oliveira. **Planejamento e prevenção a crimes cibernéticos.** Curitiba: Contentus, 2020.

SANTOS, Flavio Augusto de Oliveira. **Gestão de risco e estratégias antifraudes.** Curitiba: Contentus, 2021.

SILVA, Tamara Bruna Ferreira. **Perícia digital:** estratégias para analisar e manter evidências íntegras em forense computacional. Repositório Universitário da Ânima, 2017. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/3713/1/Artigo_Pos_v5.pdf. Acesso em: 24 out. 2023.

SCHULZE, Clenio Jair. Jurisdição de fronteiras e o Estado Constitucional Cooperativo. **Revista de Doutrina da 4ª Região,** Porto Alegre, n. 64, fev. 2015.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação: 3. ed. Rio de Janeiro: Brasport, 2021.