FAI- FACULDADE DE IPORÁ

BACHARELADO EM DIREITO

ANDRESSA SANTOS OLIVEIRA
KAREN SILVA DE SOUZA

OS CRIMES CIBERNÉTICOS E OS DESAFIOS DO DIREITO PENAL EM SEU COMBATE

IPORÁ-GO
2022

FOLHA DE APROVAÇÃO

ANDRESSA SANTOS OLIVEIRA
KAREN SILVA DE SOUZA

OS CRIMES CIBERNÉTICOS E OS DESAFIOS DO DIREITO PENAL EM SEU COMBATE

Trabalho de Conclusão de Curso submetido ao Curso de Bacharelado em Direito da FAI – Faculdade de Iporá, como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Direito.

BANCA EXAMINADORA

Maria Alvinia Cunha Pereira da Silva

Prof. Me. Maria Alvinia Cunha Pereira da Silva _____

Presidente da Banca e Orientador

Tales Gabriel Barros e Bittencourt.

Professor Tales Gabriel Barros Bittencourt _____

Membro

Professora Delana _____

Membro

IPORÁ – GO

2022

RESUMO

O presente estudo objetiva analisar a evolução da legislação relativa aos crimes cibernéticos no Brasil e sua efetividade, com ênfase no princípio da extraterritorialidade, evidenciado no art. 7 do CP. Com o advento tecnológico, a internet se elevou como mecanismo de comunicação massificada e sem fronteiras, sendo observadas não apenas contribuições, mas também o cometimento de vários crimes neste âmbito, como, por exemplo, a pedofilia, o estelionato virtual, a pornografia de vingança, dentre outros. Assim, para a adequada coibição a tais delitos, a legislação brasileira se viu obrigada a acompanhar a evolução dos meios tecnológicos e promulgou diplomas relevantes, como é o caso da Lei nº 12.965/2014 (Marco Civil da Internet) e da Lei nº 13.709/2018 (LGPD), considerados grandes avanços no ordenamento jurídico pátrio. Como resultados, verificou-se que apesar da nítida progressão da legislação pátria, a identificação dos autores destes crimes ainda se demonstra complexa para a investigação criminal e, quando o indivíduo se encontra em território estrangeiro, verifica-se a possibilidade de aplicação do princípio da extraterritorialidade, com fulcro na legislação penal e no entendimento do Superior Tribunal de Justiça. A técnica de pesquisa utilizada no presente trabalho é a bibliográfica, sendo o método dedutivo empregado, a fim de adequar ideias ou descobrir intuições sobre a temática abordada.

Palavras-chave: Crimes. Cibernéticos. Legislação. Tecnologia. Extraterritorialidade.

ABSTRACT

This study aims to analyze the evolution of legislation on cybercrime in Brazil and its effectiveness, with emphasis on the principle of extraterritoriality, as evidenced in art. 7 of the CP. With the advent of technology, the internet has emerged as a mass communication mechanism without borders, with not only contributions being observed, but also the commission of various crimes in this area, such as, for example, pedophilia, virtual embezzlement, revenge pornography , among others. Thus, for the proper restraint of such crimes, Brazilian legislation was obliged to follow the evolution of technological means and enacted relevant diplomas, as is the case of Law No. 12.965/2014 (Marco Civil da Internet) and Law No. 13.709/ 2018 (LGPD), considered great advances in the Brazilian legal system. As a result, it was found that despite the clear progression of national legislation, the identification of the authors of these crimes is still complex for criminal investigation and, when the individual is in foreign territory, there is the possibility of applying the principle of extraterritoriality, with fulcrum in criminal legislation and in the understanding of the Superior Court of Justice. The research technique used in this work is bibliographical, with the deductive method used in order to adapt ideas or discover intuitions about the topic addressed.

Keywords: Crimes. Cybernetics. Legislation. Technology. Extraterritoriality.

SUMÁRIO

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me deu forças para concluir mais esse objetivo.

Aos meus pais e familiares, pelo incentivo e compreensão nas horas em que precisei estudar ao invés de participar das atividades familiares.

À professora orientadora Me. Maria Alvinia Cunha Pereira da Silva, por ter aceitado me orientar neste trabalho e ter compartilhado seus conhecimentos comigo, além de sempre estar disponível para me auxiliar.

1 INTRODUÇÃO

A evolução social denota a clara ligação entre a evolução do ser humano e da tecnologia, elevada com os estudos técnicos e de adequação de instrumentos necessários à sobrevivência e à melhoria de qualidade de vida das pessoas na modernidade. A tecnologia, desse modo, se revela como mecanismo essencial para o desenvolvimento econômico e social.

Nesse contexto, se originam entre as relações humanas os reflexos jurídicos oriundos de atividades digitais, sobretudo pela frequente utilização da internet. Com a visível indispensabilidade dos instrumentos virtuais, e tendências cada vez mais pela substituição do plano físico pelo virtual, é preciso que se examine as normas jurídicas nessa nova seara, que viabilizem segurança às relações virtuais de maneira específica.

Levando-se em consideração que a internet se demonstra uma ferramenta indispensável na vida dos indivíduos, assim como a vasta ocorrência de crimes cibernéticos neste plano, o estudo almeja analisar a evolução da legislação brasileira e sua efetividade em relação a tais delitos, com ênfase no princípio da extraterritorialidade, com fulcro no art. 7 do Código Penal. A importância da temática encontra fundamento na crescente insegurança observada na sociedade da informação, tendo em vista que ao passo que a tecnologia progride, na mesma medida se evoluem as práticas ilícitas no ambiente cibernético.

Para tanto, o presente trabalho se divide em três capítulos, onde o primeiro expõe noções introdutórias aos crimes cibernéticos, como seu conceito, evolução histórica, classificação, sujeitos e espécies. No segundo momento, analisa-se a evolução da legislação brasileira em relação a tais delitos, iniciando-se pela pioneira Lei nº 12.735/2012 (Lei Azeredo) até a Lei nº 13.709/2018 (LGPD), considerada esta última a legislação mais recente no que tange ao ambiente virtual.

No terceiro capítulo, o estudo aborda sobre os desafios da ciência criminal no combate aos delitos cibernéticos, explanando os aspectos concernentes à sua investigação, a dificuldade na identificação do cybercriminoso e, por último, apresente as possíveis soluções para a coibição dos supracitados crimes, a fim de elevar o debate sobre o tema no cerne acadêmico e jurídico, tendo em vista a escassez de estudos na área, em razão de sua atualidade.

De acordo com as características do trabalho, tem-se uma pesquisa bibliográfica, qualitativa e descritiva que foi utilizada para sustentar cientificamente os objetivos da pesquisa. Com uma didática de cunho exploratório, a pesquisa realiza o levantamento bibliográfico, buscando reunir as informações sobre o tema com o propósito de identificar os assuntos relevantes que deem sustentação aos argumentos elencados.

2 CRIMES CIBERNÉTICOS

2.1 CONCEITO DE CRIME

O ordenamento jurídico pátrio adota o denominado sistema bipartido para definir crime. Através do Código Criminal do Império, as expressões crime e delito foram consideradas sinônimos. Tais terminologias se distinguem da outra espécie de infração penal observada no sistema nacional – as contravenções – tendo em vista que estas últimas são consagradas infrações com menor grau de gravidade (JUSTINO, 2016).

Para tanto, em consonância a legislação vigente, a Lei de Introdução ao Código Penal apresenta o conceito legal do que seja crime ou delito, distinguindo-o da contravenção penal. Em seu dispositivo 1º, aduz:

> Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente (BRASIL, 1940).

Em suma, no que diz respeito à conceituação legal de crime, o Brasil historicamente preferiu pela adoção do denominado critério dicotômico. Contudo, uma análise mais intensa sobre o crime não deve se contentar somente com o que aduz a lei codificada. Munida de tal conhecimento, a Criminologia deve se atentar à edificação de um conceito científico do que seja crime.

O conceito de crime não é igualmente o mesmo para o Direito Penal e para a Criminologia. Para o âmbito penal o crime é a ação típica, ilícita e culpável. Pode-se verificar, nesse conceito, que a acepção que o Direito Penal possui do crime é uma acepção centralizada no comportamento de quem realiza o delito.

Dessa forma, mesmo que a definição englobe aspectos voltados para generalidades das leis – e como decorrência para a generalidade de indivíduos –, como é o caso da ilicitude, não se pode olvidar que tal definição assenta para o caminho natural e frequente realizado pelos operadores do direito no tocante aos fatos delitivos: um verdadeiro juízo de subsunção do fato à norma, sendo este meramente individual (VIANA, 2018).

Na seara do Direito Penal existem três conceitos de delito: material, formal e analítico. A definição material encontra-se vinculada ao ato que denota prejuízo social, ou que acarrete lesão a um bem jurídico; a definição formal encontra-se conexa ao fato de existir uma norma penal que disponha estabelecido ato como infração criminal; por seu turno, a definição analítica de delito explana os aspectos estruturais e essenciais do conceito de crime.

O conceito material considera crime todo fato humano que, de maneira proposital ou descuidada, afere lesão ou expõe a risco bens juridicamente considerados fundamentais para a existência do coletivo e para o alcance da paz social. Desse modo, sob a ótica do conceito puramente material, se o fato é lesivo aos bens juridicamente tutelados, tal fato é tido como crime, independente da existência de lei o dispondo como tal (CAPEZ, 2019).

Por sua vez, o conceito formal aduz que crime é tudo aquilo que o legislador pátrio descrever como tal, independentemente do seu conteúdo. Nesse sentido, pela definição puramente formal, não importa se um fato é ou não materialmente lesivo a um bem jurídico, bastando somente sua descrição na legislação. Por fim, o conceito analítico intenciona determinar, sob um viés jurídico, os elementos estruturais do crime, levando-se em consideração ambos os conceitos delineados acima, o material e o formal, mas não se limita a nenhum destes de maneira isolada (CAPEZ, 2019).

Desta feita, através desse conceito, o crime é, ao menos, um fato típico e ilícito (concepção bipartida), podendo ser demandado ainda o elemento de ser culpável (concepção tripartida) ou, em adição, também o elemento de ser punível (concepção quadripartida). Vale ressaltar que o Brasil utiliza o conceito analítico de crime.

Posto isso, segundo o entendimento de Sumariva (2010, p. 06) “o crime é um fenômeno social e comunitário, que se demonstra como um problema maior, carecendo, assim, dos estudiosos, uma visão ampla que permita aproximar dele e compreendê-lo em seus variados enfoques.” Corroborando ao estudo, as lições de Maíllo (2007, p. 45) apresentam a acepção de delito sob um viés legal e natural, segundo o autor:

> A concepção legal de delito refere-se à ideia de que o limite do objeto de estudo da criminologia é o Código Penal e as leis penais especiais. A concepção natural, por sua vez, propõe a definição de crime como todo ato de força física ou fraude que é realizado pelo indivíduo em busca de benefício próprio.

Ambas as concepções explanadas acima são alvos de críticas. O viés legal de delito é refutado pelo fundamento de que cada área deveria definir, por si só, seu objeto de estudo. Ademais, fundamenta-se que as normas penais são muito imprecisas e vagas, “além de serem constantemente modificadas, assim como podem ser puramente representativas dos interesses dos grupos sociais dominantes” (MAÍLLO, 2007, p. 46).

O viés natural de delito partiu da adequada posição de defender a necessidade de que a Criminologia defina por si só seu próprio objeto de estudo. Todavia, também sofreu muitas críticas, relativas ao fato de contar com definições demasiadamente imprecisas para o entendimento do crime. Contestou-se, ainda, o fato de que tal concepção “engloba mais condutas do que aquelas que realmente interessam a referida ciência, além do fato de que, em consonância a tal viés, um crime não poderia ser realizado em benefício alheio” (MAÍLLO, 2007, p. 46).

Sendo assim, é possível conceber que o crime na sociedade contemporânea não consiste apenas num fenômeno social, mas uma realidade. Ele está presente no cotidiano das pessoas e não pode ser definido unicamente como um conceito imutável, estacionário e único no espaço e tempo. O significado de crime evoluiu ao longo do tempo. Dessa forma, para identificar um crime de maneira analítica basta somente o seu fato típico e antijurídico, de acordo com a teoria bipartida.

Portanto, apesar de existirem argumentos que elevam a teoria tripartida, apontando a culpabilidade como um dos elementos que compõem o crime, o ordenamento jurídico nacional escolheu claramente por adotar a bipartida, uma vez que estabelece no artigo 23 do CP não existirá crime quando o agente realizar um ato típico em virtude da existência de uma razão que exclui a ilicitude de sua conduta.

2.2 CONCEITO E BREVE HISTÓRICO DOS CRIMES CIRBERNÉTICOS

Em relação à definição exata de crimes cibernéticos, é importante notar que não há um consenso doutrinário. Muitas expressões são usadas para se referir a este fenômeno, como crimes virtuais, informáticos ou *cybercrimes*. Independentemente da linguagem utilizada, todos esses termos têm características inerentes: os delitos são cometidos através de meios informáticos; há a utilização de redes de transmissão de dados para facilitar o delito; e o bem jurídico prejudicado tem que ser um ato típico, antijurídico e culpável (SILVA, 2015).

Sendo assim, apesar de não haver um consenso sobre o que são os crimes cometidos no mundo on-line, eles sempre são perpetrados do mesmo jeito: a pessoa usa métodos tecnológicos, como a internet, para cometer o crime. De igual modo, Jorge e Wendt, corroborando a compreensão anterior, apontam que, apesar do termo utilizado, de forma geral todos se referem à ação criminosa auxiliada por meio de dispositivos informáticos (JORGE; WENDT, 2013).

Desse modo, a definição que mais condiz com o crime cibernético é aquela em que há invasão de um equipamento tecnológico ou violação de uma rede com a finalidade obter, suprimir ou adulterar dados e informações sem consentimento da vítima. O delito aqui apontado consiste na instauração de *softwares* maliciosos que revelam vulnerabilidades no acesso às informações pessoais (JORGE; WENDT, 2013).

Nessa diretriz, o entendimento de Rossini (2004, p. 145) mostra que:

> O crime informático é uma ação ilícita que pode ser um crime ou contravenção penal, culposa ou dolosa, cometida por uma pessoa física ou jurídica usando meios informáticos. Isso viola direta ou indiretamente a segurança informacional, que inclui confidencialidade, integridade e disponibilidade.

Descrevendo o conceito de forma mais clara, para que seja possível compreendê-lo, percebe-se que os crimes cibernéticos, apesar de geralmente cometidos por pessoas físicas - sobretudo os *hackers* - também podem ser perpetrados por pessoas jurídicas. O ato ilícito cometido pelos sujeitos citados acima deve ser típico, ilícito e descrito como crime ou contravenção penal.

Assim, resta nítido que o ato pode ser intencional (doloso), onde há a vontade de causar dano, sendo o efeito planejado pelo responsável pelo fato; ou ainda pode ser involuntário (culposo), consequência da negligência, imprudência ou imperícia do autor da conduta, podendo esta ser comissiva ou omissiva.

Por fim, é possível notar que a atitude criminosa pode ser cometida com a ajuda de ferramentas tecnológicas, como celulares, laptops e computadores, usando ou não a *internet* global de forma ilícita com o objetivo de violar seguranças digitais. Contudo, conforme apontado pelo autor, os crimes cibernéticos podem acontecer sem essa rede mundial sendo o foco principal para esses delitos a utilização desses meios informáticos (ROSSINI, 2004).

No que tange à evolução histórica, é possível aferir que a discussão sobre os crimes cibernéticos se intensificou internacionalmente nos anos 60, por conta da questão da invasão de privacidade, mas nesse período as medidas tomadas eram

basicamente civis e regulatórias, sendo que o Direito Penal tinha uma tarefa acessória. Dez anos depois, com o aumento no número de fraudes e outros crimes ligados à economia através das redes informacionais, a importância de possíveis medidas penais também cresceu para a população e para o Estado. E assim, com chegada da era digital, surgiram também problemas referentes à propriedade intelectual (VIANNA, 2003, p. 11).

Em meados de 1990, outras evidências dos crimes cibernéticos surgiram, como é o caso de conteúdos ilícitos ou danosos, como a pornografia infantil e os discursos de ódio na *internet*, além da concretização de crimes tradicionais com ajuda de computadores, como estelionato, que passou a alcançar o âmbito virtual. No entanto, apesar das medidas paliativas, a comunidade internacional não proporcionou uma solução coesa e satisfatória para essa questão. Em particular, só se verificou a Convenção de Budapeste 2001 da União Europeia, mas também estendida a outros países (VIANNA, 2003).

A transição que se deu da década de 1960 até os dias atuais não indica tão somente um aumento nos crimes cometidos por meio da tecnologia, como também foi um momento com mudanças sociais mais fortes, que podem ser resumidas como a passagem da sociedade industrial para a sociedade informacional, marcada pelo surgimento da Terceira Revolução Industrial (BECK, 2010).

A referida transformação paradigmática trouxe uma elevação do trabalho e dos bens materiais. A mesma alteração afetou demasiadamente o Direito, que passou a precisar se adequar aos novos contextos da vida social. Dessa forma, a informação alcança um status de bem econômico, político e cultural, “ao passo que o avanço tecnológico se tornou indispensável, sendo inserido na perspectiva de um novo Direito Penal com completa atenção às particularidades dessa era” (VIANNA, 2003, p. 34). Essas inovações apesar de oferecerem diversas contribuições para a sociedade também evidenciam uma nova realidade de riscos no meio virtual.

A informação, ao contrário dos bens materiais, deve ser inicialmente considerada um bem público numa sociedade ampla. A liberdade de informação e sua promoção irrestrita são dois princípios centrais para um sistema econômico livre. Assim sendo, não é permitido apenas analisar os interesses financeiros do dono da informação, mas também é necessário observar os outros indivíduos interessados nesse conteúdo ou que possam de alguma forma ser afetados por ele.

No entanto, o Direito ainda não conseguiu se adequar totalmente a esse novo panorama e isso acontece em parte devido à própria natureza dessas mudanças. A facilidade e a agilidade com que as informações e os dados são propagados, bem como o anonimato alcançado através das novas tecnologias, tornam-se obstáculos para um efetivo tratamento normativo da questão. No centro da legislação penal, esses elementos levam a uma difícil identificação do suposto autor do delito, o que resulta em uma questionável discussão sobre a responsabilidade de intermediários, tais com servidores e provedores de *internet* (BECK, 2010).

Ainda antes da chegada da sociedade da informação, estudiosos já dialogavam sobre o uso da frase "sociedade de risco" para indicar os perigos que surgem com os novos meios tecnológicos nos mais variados âmbitos. Para estes, três fatores caracterizam o novo momento: os reflexos possíveis não se limitam a um tempo, espaço ou grupo afetado originalmente; o risco tem um impacto social e não pode ser aferido aos sujeitos individualmente responsáveis; e a dificuldade e velocidade do desenvolvimento social e tecnológico são gradativas (BECK, 2010, p. 117).

A mesma análise se pode estender à sociedade da informação, pois uma pequena alteração de dados pode ter consequências substanciais. A sabotagem no ambiente informacional pode até paralisar setores da economia internos, bastando somente que se ateste o grau de dependência dos sistemas bancários e das redes computacionais, tendo as modificações tecnológicas informacionais um ritmo acelerado e ininterrupto (CASTRO, 2003).

Diante do aumento dos perigos, um procedimento apropriado de prevenção de delitos cibernéticos torna-se crucial, assim como controles institucionais e legais mais criteriosos e funcionais. Nesse panorama, é possível observar que somente as medidas repressivas apresentam-se insuficientes, uma vez que os novos riscos não podem ser controlados apenas pelo Direito Penal.

No âmago dos riscos advindos das tecnologias, medidas que não são criminais também se tornam relevantes para pensar na prevenção de crimes. Em grande parte das situações, padrões técnicos de segurança e medidas civis e administrativas também se mostram como complementares à legislação penal, para distanciar a criminalidade *on-line*. Tal afirmativa não apaga o fato de que o Poder Público e a sociedade permanecem a notar, no âmbito penal, a principal maneira de lidar com este fenômeno. Apesar da efetividade ou não da resposta penal, a necessidade clara

desta proteção exige pelo menos tentar racionalizar os procedimentos presentes na base da legislação (CASSANTI, 2014).

Além disso, a sociedade da informação tem alcance global, visto que as barreiras entre os países têm sua relevância reduzida, o que subsequentemente aumenta a importância da harmonização com o direito internacional. A informação espalhada pelo mundo de maneira célere e assustadora quase não pode ser controlada, minimizando, assim, a eficácia dos controles estatais em favor de soluções locais ou supranacionais (DE LUCA; SIMÃO, 2000, p. 125).

Portanto, mesmo se existisse uma harmonia apenas na seara legal, ela não seria eficaz por completo, pois o fluir de informações é global e não há como vedar toda e qualquer lacuna, assim, a cooperação dos documentos internacionais também tem grande importância.

2.3 CLASSIFICAÇÃO E SUJEITOS

A tecnologia propiciou uma nova realidade no cometimento de crimes, com a facilidade de uso, a variedade das informações e os dados sendo disponibilizados e acessíveis em qualquer lugar do mundo. Além disso, o anonimato presumido dos usuários e os meios informáticos que estão sempre se alterando tornaram complexa a atividade de perseguição para um adequado controle e coibição. Hoje em dia, como se verifica, ainda não existe um consenso quanto ao conceito de crimes cibernéticos, devido à constante geração de novos tipos de delitos.

Assim sendo, em relação à classificação dos crimes cibernéticos, Jorge e Wendt (2013) escrevem que:

> Os crimes virtuais são todas as atividades típicas, antijurídicas e culpáveis que são cometidas usando computadores ou qualquer outro meio tecnológico, sendo os meios variados. A classificação mais aceita admite a diferenciação entre crimes próprios e impróprios, enquadrando o autor do crime como sujeito ativo, reconhecidamente cracker ou hacker, sendo este, qualquer pessoa física ou jurídica; ao passo que o sujeito passivo é elevado como a pessoa sobre a qual recaiu a ação.

Sendo assim, os crimes virtuais impróprios são concretizados por intermédio de um sistema digital de dados. Nessa subdivisão dos crimes virtuais, os recursos tecnológicos se tornam um mecanismo propício ao delito, logo, os crimes pertencentes a essa classificação decorrem da mesma forma que aqueles já dispostos na legislação.

A concretização desse tipo de delito não requer grandes compreensões técnicas sobre dispositivos informáticos e infiltração em sistemas de informações e dados. O bem jurídico protegido em tais circunstâncias não é a inviolabilidade de dados automatizados, mas sim outros bens jurídicos, já previamente tipificados para impor penalidades a atitudes cometidas habitualmente.

Quando a atuação do sujeito se amolda às espécies de crimes cibernéticos próprios, tal conduta lesiona, por meio da tecnologia, outros bens jurídicos que não os informáticos com a intenção de causar o efeito naturalístico pretendido. A maioria dos crimes virtuais são impróprios, concentrados na realização de atividades ilícitas com o auxílio de um dispositivo tecnológico para alcançar o meio jurídico já tipificado e fazer ações conhecidas por um método totalmente inovador.

Não obstante utilizarem a *web* como instrumento e até como local de concreção de tais crimes, os mesmos não permanecem estritamente no plano virtual, podendo estender sua continuidade para o mundo físico. Como exemplo, verifica-se o estupro, a pedofilia *on-line*, dentre outros. Nota-se que nessa classificação de crimes cibernéticos, computadores e *internet* são usados como mecanismo para o cometimento de atos ilícitos tipificados, a exemplo ainda dos crimes contra a honra, com fulcro no Código Penal.

Como afirma Damásio de Jesus (2001, p. 4):

> Os crimes impuros ou impróprios são aqueles em que o sujeito usa o computador como meio para criar um resultado naturalístico, violando o mundo físico ou espaço real, ameaçando ou prejudicando bens não-informáticos.

Dado que a violação dos bens jurídicos mencionados já é considerada crimes no sistema jurídico, com os atos atentatórios específicos tipificados, não se exclui a necessidade que os crimes comuns, quando cometidos por meio de ferramentas informáticas no plano virtual, alcancem uma tipificação própria e relevante às suas peculiaridades, visando garantir um completo exercício da jurisdição. Isso evitaria a necessidade de se recorrer à analogia para enquadrar essas condutas.

Por outro lado, os chamados crimes cibernéticos próprios, que são diferentes dos impróprios - cuja existência é anterior à era tecnológica - são aqueles que surgiram com o uso da informática para armazenar dados, criando atitudes específicas para este campo. Dada a sua singularidade, essa classificação de crime requer, ao contrário da primeira, conhecimentos técnicos e especializados em computação para serem concretizados.

Neste sentido, o mencionado ato criminoso cometido pela ação ilegal atenta contra o sistema de dados em si, afetando-o no que diz respeito à privacidade e inviolabilidade de informações e dados, além da disponibilidade e veracidade dos mesmos, prejudicando gravemente a segurança informática. Desse modo, é possível dizer que os crimes cibernéticos próprios são menos comuns, uma vez que requerem necessariamente a utilização do sistema informático não apenas como mecanismo para a realização do delito, mas sim como objeto material desejado com o ataque criminoso.

Nos casos de referidas condutas, haverá violações diretas ao *software* do computador da vítima, o que levará ao acesso de informações e dados não permitidos, incluindo senhas e documentos. Isso possibilitará a modificação, inserção ou eliminação desses arquivos. Neste contexto, os estudos de Damásio de Jesus e Aras (2001, p. 6) também salientam que:

> Os crimes cibernéticos próprios são aqueles que são cometidos através do computador e ocorrem também em um ambiente eletrônico. Nesses casos, a informática (segurança dos sistemas, integridade das máquinas, dados e periféricos) é o objeto juridicamente tutelado.

Assim, os crimes virtuais próprios caracterizam um novo tipo de delito, que aumenta à medida em que a *internet* se populariza e evolui. Na face da inovação do tema e das mudanças constantes nos meios informáticos, a legislação não consegue se adequar com a esperada rapidez às novas condutas ilícitas que surgem no ambiente virtual.

Nesse panorama, devido à falta de uma legislação específica e completa que disponha sobre esse assunto e punir essas condutas prejudiciais, ocorrem atos que, embora causem danos irreparáveis às vítimas, ainda são considerados atípicos e não podem ser punidos pelo princípio da legalidade que dirige de maneira inevitável o ordenamento jurídico brasileiro - principalmente quando se trata de temas penais.

A doutrina nacional classifica os crimes cibernéticos de acordo com seu propósito. Para isso, os crimes cibernéticos impróprios são cometidos através do banco de dados do sistema informático, enquanto que os próprios são cometidos contra o banco de dados do sistema informático. Desta feita, os crimes cibernéticos próprios podem ser classificados pela doutrina como formais, visto que sua concretização se eleva no momento da realização da conduta delitiva, independentemente da realização do resultado no mundo naturalístico (SANTOS; RIBEIRO, 2018, p. 228).

Logo, chega-se à conclusão que a maioria dos criminosos virtuais é encorajada pela sensação de impunidade que o ambiente virtual oferece. Contudo, quer sejam os delitos cibernéticos próprios ou impróprios, a utilização de meios informáticos deixa, na maioria das situações, vestígios, que muitas vezes são mais perceptíveis do que os crimes cometidos no mundo físico.

Portanto, os vestígios deixados pelos criminosos cibernéticos são dados que são registrados no acesso à rede de computadores, sendo inseridos nesse contexto as informações de IP, que é o número de identificação atribuído a um aparelho ou roteador de internet quando estabelece uma conexão com a rede, bem como fatores como localidade e os dados de cadastro do sujeito.

3 EVOLUÇÃO LEGISLATIVA DOS CRIMES CIBERNÉTICOS

3.1 LEI Nº 12.735/2012

A Lei nº 12.735/2012, reconhecida como Lei Azeredo, alcançou sua vigência através do Projeto de Lei nº 84/1999, o qual denotou questões polêmicas no tocante ao teor de suas disposições sobre os delitos, sanções e procedimentos investigativos relativos ao plano virtual. Assim, em sua redação definitiva, a supracitada Lei propiciou sucintas modificações na legislação penal, penal militar e na Lei nº 7.716/1989, que tratava sobre os delitos advindos de preconceito. No entanto, evidencia-se que não fora verificada a adição de qualquer tipo penal no sistema jurídico brasileiro.

Dentre as alterações ocasionadas, o dispositivo 4º dispunha a edificação de setores especializados, na conjuntura das polícias judiciárias, hábeis a operar contra a "ação criminosa na rede de computadores, dispositivos de comunicação ou sistema informatizado." (BRASIL, 2012) Tal determinação foi de suma relevância na intensificação das pesquisas sobre a temática. A imposição da particularização elevou a propagação de centros policiais em partes do Brasil, direcionados à investigação peculiar dos crimes virtuais, edificando novas medidas e tecnologias no tratamento de tais ilícitos.

Segundo Wendt e Jorge, como exemplo, verifica-se a instauração, no estado do Paraná, do Núcleo de Combate aos Cibercrimes (NUCIBER), o qual é incumbido pelo direcionamento das investigações, em todo o estado, no tocante aos crimes cibernéticos. Mesmo dispondo de uma equipe pequena, o NUCIBER se evidencia como uma forte referência entre tais órgãos norteados ao âmbito virtual. Seu posicionamento central viabiliza um amplo exame das complexidades, bem como prepondera a aderência de medidas padronizadas a serem trilhadas em todo estado. (WENDT; JORGE, 2013, p. 253)

Contudo, vale aferir que mesmo demonstrado o advento no NUCIBER, no Paraná, a maioria dos estados brasileiros ainda não comportam estruturas similares, seja pela ausência de profissionais especializados ou em virtude da escassez de recursos direcionados ao âmbito. Posto isso, "nota-se que o combate no plano prático aos delitos virtuais ainda está muito longe do contexto ideal." (WENDT; JORGE, 2013, p. 254)

Desta feita, verifica-se ainda o ponto crucial da ausência de integração entre os órgãos de investigação criminal. Pois, de acordo com os autores, a ausência de uma cultura de compartilhamento aliada à nítida precariedade de estrutura é capaz de tecer danos à troca de informações entre cidades e estados, inviabilizando a constituição de uma rede à nível nacional defronte à criminalidade virtual.

Conforme destacado, a Lei nº 12.735/2012 também teceu alterações na Lei nº 7.716/1989, especificamente em seu dispositivo 20, §3º, II, na intenção de dispor a hipótese de "cessação das respectivas transmissões radiofônicas, eletrônicas, televisivas ou ainda da publicação por qualquer via", cujas expressões detenham conteúdo discriminatório ou preconceituoso. (BRASIL, 2012)

Isto é, mesmo sendo breve, tal determinação viabilizou a extensão da seara de atuação contra tais expressões preconceituosas, classificando os novos meios tecnológicos em um rol até o momento edificado somente pelos meios midiáticos tradicionais, como o rádio e a televisão.

Portanto, conforme vislumbrado, apesar de ter propiciado colaborações no trato dos crimes virtuais, com ênfase para a obrigação de instituir centros especializados para a adequada investigação e estudo destes ilícitos, vislumbra-se que a Lei Azeredo foi muito branda no trato da questão, especialmente quando equiparada a outros Diplomas que vieram posteriormente, como é o caso da Lei nº 12.737/2012, que será explanada no tópico seguinte.

3.2 LEI Nº 12.737/2012

Em conformidade aos estudos de Brito, a vigência da Lei nº 12.735/2012 denotou um marco na legislação relativa aos crimes cibernéticos, em virtude do demasiado avanço que diz respeito à criminalidade neste âmbito. A supracitada Lei alcançou seu sancionamento no governo de Dilma Roussef, com a árdua tarefa de diminuir as lacunas observadas sobre o tema, assim como coibir a imunidade no cerne dos crimes digitais. (BRASIL, 2012)

Após grande repercussão midiática, em maio de 2012, a atriz Carolina Dieckmann procurou ajuda policial para início das investigações relativas ao vazamento de mais de trinta fotos pessoais de Carolina propagada na internet, sobretudo imagens ao lado de seu filho, com quatro anos na época. A atriz recebia

constantemente ameaças dos delinquentes em busca de dinheiro para a não divulgação do material obtido ilicitamente.

No período do delito, o Brasil ainda não detinha uma legislação específica para os crimes cibernéticos, tendo em vista que a citada anteriormente pouco modificou os Diplomas existentes. Posto isso, a justiça brasileira se valeu da legislação penal para a solução do caso da atriz, onde os criminosos foram indiciados por extorsão qualificada, furto e difamação.

Após o período investigativo, a polícia obteve o IP com a identificação do equipamento suspeito, onde fora realizada a interceptação de conversas entre os acusados, onde os mesmos confessaram o delito e, dias após, os policiais chegaram até eles. Neste caso, a polícia acredita que os criminosos não imaginavam que poderiam ser pegos, uma vez que se investiam do suposto anonimato da internet.

Nesse sentido, as lições de Lira (2014, p. 55) explanam qual foi a tipificação usada para enquadrar os criminosos da ação penal movida por Carolina, uma vez a ausência legislativa específica para a invasão de equipamento informático. Ainda, aferiu que “quem fizer a mesma ação, a partir de então, terá enquadramento distinto, tendo em vista que a ocorrência de tal fato foi significativo para a elaboração de norma específica sobre crimes virtuais.”

Sendo assim, o tratamento dispensado ao caso da atriz, antes da promulgação da referida Lei, apenas abria possibilidade que tais crimes fossem tipificados na legislação penal, com penas mais brandas do que o adequado, assim, a Lei nº 12.735/2012 alcançou grande visibilidade pois, antes mesmo de sancionada, já havia sido apelidada com o nome da atriz, tendo em vista a grande repercussão do caso. (BRASIL, 2012)

A modificação elevada pelo novo Diploma fora inserida oficialmente no sistema jurídico pátrio em abril de 2013, quando a legislação penal recebeu a adição dos arts. 154-A e 154-B no Capítulo IV que dispõe dos crimes contra a liberdade individual, sobretudo na seção dos delitos contra a inviolabilidade de segredos. Segundo as lições de Delmanto (2016, p. 225) é possível verificar duas condutas incriminadoras no caput do art. 154-A, sendo a primeira relativa à invasão de dispositivo informático de outrem, ligado ou não à rede, por intermédio de violação inadequada de instrumento de segurança, como, por exemplo, a ruptura de senhas, aliado ao elemento normativo do tipo sem permissão expressa ou tácita do dono do dispositivo.

Ainda, a lei aponta que a instalação de vírus, controle à distância ou programas de espionagem em equipamento alheio também é vedado. Em muitos casos, para que a invasão de um sistema informático se concretize, será essencial, a priori, instalar programas e, se na situação concreta, o indivíduo invade e instala ou instala e invade, responderá este por apenas um crime.

Também em consonância ao dispositivo analisado, Prado aponta que este protege a liberdade individual, especialmente a privacidade no tocante aos dados e informações, de natureza pessoal ou profissional, elencados em dispositivo informático, cuja segurança deve ser de algum modo rompida sem o consentimento do titular. (PRADO, 2013, p. 406)

Por sua vez, Capez e Garcia sinalizam acerca do efeito do referido artigo, que o âmago basilar da conduta típica é consubstanciado no termo “invadir”, ou seja, ingressar digitalmente, sem o consentimento expresso ou tácito do titular do equipamento. A conduta de invasão eleva a falta de permissão do dono ou usuário do dispositivo, tendo em vista que não se pode aferir que houve invasão quando o acesso ocorre mediante sua aceitação. Ainda assim, “o tipo penal do art. 154-A caput do CP, de maneira superficial, repete ao final a exigência do elemento normativo do tipo sem autorização expressa ou tácita do titular do dispositivo.” (CAPEZ; GARCIA, 2013, p. 345)

Além do mencionado, a Lei nº 12.735/2012 também inseriu o art. 154-B no CP[1], o qual faz menção à ação penal. Nessa toada, Delmanto aduz que a ação penal será pública incondicionada quando o crime for cometido contra a Administração Pública de qualquer Poder, Estados, DF ou Municípios o contra organizações empresariais concessionárias de serviços públicos. Eleva-se também que a ação penal, em regra, por qualquer dos ilícitos dispostos no art. 154-A será condicionada à representação do indivíduo ofendido, na data limite de seis meses a contar da ciência indubitável do fato e de sua autoria, sob pena de decadência. (DELMANTO, 2016, p. 227)

Todavia, vale ressaltar que não foram apenas essas modificações com a vigência da Lei nº 12.735/2012, como também o dispositivo 266 do CP, que alcançou novo texto em seu parágrafo 1º e 2º, referindo-se acerca da interrupção ou

[1] Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

perturbação de serviço informático, telegráfico, telefônico, telemático ou de informação de utilidade relevante para a sociedade; ainda, o dispositivo 298 em seu parágrafo único fora alterado quando direcionado para a falsificação de documento particular. (BRASIL, 2012)

Assim, em análise ao art. 266, as lições de Nucci sustentam que responde pelo delito tanto o indivíduo que interrompe o serviço como aquele que coíbe ou obsta o seu reestabelecimento. Na situação de ser o mesmo autor para todas as ações, responde por só um delito, pois se refere ao tipo misto alternativo. E prosseguindo com o art. 298, o doutrinador expõe que o cartão de débito ou crédito, propriamente dito, não se perfaz em um documento (elemento material disposto a revelar informe ou outra informação), mas dessa forma será considerado para propósitos de falsificação. (BRASIL, 2012)

No entendimento de Amâncio, essa vulnerabilidade das normas foi o principal ponto para a edificação da criminalidade cibernética, motivo pelo qual demonstrou-se indispensável a elaboração de legislação específica que disponha sanções a estes delitos. De acordo com o autor, “merece a evidência a Lei nº 12.735/2012, que pode ainda se demonstrar restrita ou branda, no entanto se revelou um importante passo na tutela das vítimas de crimes virtuais.” (AMÂNCIO, 2013, p. 29)

De acordo com Reis, a modificação perpetrada na legislação pátria para a tipificação dos delitos realizados virtualmente, por meio da Lei nº 12.735/2012, veio ao encontro dos anseios vislumbrados na sociedade contemporânea, tendo em vista que se inclina a vedar práticas delitivas no plano informático, que de algum modo afere benefício indevido a outrem em detrimento das vítimas. Assim, sustenta-se que “a Lei nº 12.735/2012 representa um avanço na legislação brasileira, uma vez que a tutela cibernética edificou um novo bem jurídico.” (REIS, 2013, p. 174)

Portanto, conclui-se que a discussão acerca de uma legislação específica para o âmbito virtual já se propagava em velocidade lenta há mais de uma década no Brasil, no entanto, somente alcançou notoriedade após a invasão do dispositivo da atriz Carolina Dieckmann, representando, assim, um caso necessário para que houvesse maior preocupação e atenção com os crimes perpetuados no plano virtual.

3.3 LEI Nº 12.965/2014 “MARCO CIVIL DA INTERNET”

Como já demonstrado, na sociedade contemporânea, a internet representa um mecanismo essencial para a propagação de informações, o que influencia tanto o crescimento econômico quando o direcionamento dos discursos políticos, de modo que o seu controle vem sendo ponto de diversas disputas entre Estados soberanos.

Evidencia-se também a importância do ambiente virtual para o avanço no processo de democratização do acesso à informação, tendo em vista que viabiliza que indivíduos em localidades distintas e com graus diferentes de educação possam ter acesso ao mesmo material, e para o aumento da participação popular na própria elaboração das informações e conteúdos propagados.

Em análise à conjuntura do que se denomina sociedade da informação, os estudos de Ascensão (2012, p. 36) elevam que esta teria como ferramenta nuclear a internet que, segundo o autor, “foi motivo de intensas modificações, pois de rede militar passou-se à rede científica desinteressada, depois a meio de comunicação de massas, para se tornar, finalmente, um relevante veículo comercial.”

No tocante à informação, Ascenção (2012, p. 36) assevera que:

> Nesta evolução, a informação que seria o seu conteúdo vai mudando de natureza. Não só passa a abranger qualquer conteúdo de comunicação — de maneira que melhor se falaria em sociedade da comunicação que em sociedade da informação — como a própria informação se degrada. O saber transforma-se em mercadoria. De conhecimento livre transforma-se em bem apropriável. É cada vez mais objeto de direitos de exclusivo, que são os direitos intelectuais. Estes, por sua vez, são cada vez mais dissociados dos aspectos pessoais, para serem considerados meros atributos patrimoniais, posições de vantagem na vida económica.

A natureza global da internet e a falta de um domínio pleno sobre seus nuances carecem uma maior atenção sobre os possíveis impactos e reflexos do ambiente virtual na vida do ser humano. Dessa forma, parece errônea a afirmação de que na internet a transmissão de informações deveria ser totalmente livre e ilimitada, assim como que naquele âmago as ferramentas legais de proteção à pessoa humana não seriam totalmente aplicáveis.

Mesmo que a internet seja um local investido de liberdade, isso não significa dizer que seria um espaço sem leis e adverso à responsabilidade pelos abusos ocorridos. No mundo físico, assim como no virtual, a relevância da dignidade da pessoa humana é apenas um só, de modo que nem o ambiente em que os agressores transpassam e nem os instrumentos tecnológicos que utilizam poderão afastar ou enfraquecer a natureza intransferível e única do supracitado princípio.

Deve-se, assim, almejar a constante inclusão dos princípios advindos do texto constitucional nas categorias antes diretamente ligadas ao direito privado, com a finalidade de propiciar tanto a criação quanto a aplicação de leis responsáveis por assegurar não somente o mundo físico, mas também o âmbito virtual. Assim, o Brasil não poderia mais manter-se desatento à importância da internet na vida da sociedade e como ferramenta de ampla utilização para a realização de contratos de consumo, refletindo dessa contratação a criação da Lei 12.965/2014. (BRASIL, 2014)

O Marco Civil da Internet dispõe em sua redação legislativa determinações sobre “acontecimentos específicos ao ambiente virtual como a neutralidade da rede, a responsabilidade dos provedores e, também, ocasiões que são verificadas em casos “offline” como a privacidade, a imagem, a liberdade de expressão, etc.” (MARCACINI, 2016, p. 31)

No primeiro dispositivo da Lei 12.965/2014 é determinada sua incidência normativa, estabelecendo, de modo resumido, que rege a utilização da internet no âmbito nacional. Dessa forma, vale asseverar que o Marco Civil da Internet, além de regular as relações jurídicas entre usuários e os provedores de serviços por atos realizados online, também almeja determinar normas de conexão e utiliza como analogia inúmeros fatos que, inicialmente, acabaram por se desenvolver offline. (BRASIL, 2014)

Em conformidade às lições de Marcacini, o autor elucida ainda que o MCI, em seu âmbito normativo, repete princípios já determinados no texto constitucional, como os já referidos, princípio da liberdade de expressão, proteção à privacidade, defesa do consumidor, entre outros dispostos nos arts. 3º e 4º da mencionada lei. (MARCACINI, 2016, p. 35)

Em seu dispositivo 5º, I a VIII, observam-se definições essenciais relativas ao ambiente virtual, restando nítido que a internet corresponde ao sistema elaborado de um conjunto de protocolos lógicos, organizados em nível mundial para utilização pública e irrestrita, com o objetivo de permitir a comunicação de dados entre terminais através de distintas redes. (BRASIL, 2014)

Vale ressaltar que o Decreto nº 8.771/16, no dispositivo 2º, parágrafo único, I e II, reafirma o âmbito de incidência da Lei nº 12.965/14, deixando muito nítido que engloba os responsáveis pela transmissão, comutação ou pelo roteamento, assim como os provedores de conexão e de aplicações de internet. (MARCACINI, 2016, p. 36)

Nesse contexto, o referido Decreto não se estende aos serviços de telecomunicações que não se disponham ao provimento de conexão de internet, nem aos de natureza especializada, compreendidos como otimizados por sua qualidade, velocidade ou segurança, aferidos a determinados grupos de usuários com controle rigoroso de admissão. Os mencionados serviços, mesmo que utilizem protocolos lógicos TCP/IP ou similares, não estarão incluídos no âmbito de incidência do Decreto em motivo de sua individualidade e por estarem guiados por outras normas editadas pelos entes responsáveis.

Portanto, ante o exposto, é possível afirmar que o Marco Civil da Internet aperfeiçoou o ordenamento jurídico pátrio, estabelecendo uma segurança digital para provedores de internet e usuários, e viabilizou aos operadores do direito um direcionamento e aprofundamento da matéria, antes visivelmente superficial.

3.4 LEI Nº 13.709/2018 “LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS”

Diante da conjuntura de vazamento de dados, o caso mais emblemático envolve a empresa *Cambridge Analytica*, que apresentou os severos efeitos oriundos da utilização inadequada e não autorizada de dados pessoais, que transpassam a individualidade de cada pessoa, ao ponto de influenciar nos caminhos democráticos de um país. A partir do referido caso, em 2016, restou nítida a consequência da falta de normas específicas sobre a utilização de dados e de uma autoridade que as tornem concretas. (SAMADOSSI, 2018, p. 478)

No caso brasileiro, a emprega já almejava atuação futura, através do pleito eleitoral para a presidência da república, por meio do fornecimento de materiais e propagandas norteadas a eleitores pautados em suas preferências e interesses revelados através de dados pessoais alcançados e usados inadequadamente, com a finalidade de intervir e influenciar votos. Diante da reverberação do caso, o Ministério Público iniciou uma investigação para examinar se existiu ou não a coleta e a utilização indevida de dados pessoais para tais fins.

Assim, em observância às situações recentes nessa acepção, também é possível evidenciar a ação de robôs que propagam fake news e que podem surtir consequências extremamente nocivas para a população. Tais atuações também almejam diretamente impedir que os usuários se mantenham informados de forma

adequada. Outro mecanismo frequente dos perfis automatizados é a distribuição de links contaminados, que possuem a finalidade de roubar dados e informações pessoais. Tais informações, que podem ser desde fotos de usuário em redes sociais, por exemplo, podem ser usadas para a elaboração de outros perfis automatizados que possuam elementos característicos aptos a iniciar conexões nas redes com usuários reais sem a autorização dos titulares.

Nesse sentido, o elemento mais nocivo da falta de uma lei específica é o que não existe parâmetro interpretativo que prepondere quanto à legalidade da utilização de dados, tendo em vista que não existiria, em algumas conjunturas, limitações nítidas ao tratamento de dados. Assim, mostrou-se na época ainda mais latente a necessidade de uma Lei de Proteção de Dados no Brasil.

Dessa forma, após repercussão global sobre o tema e sob intenso influxo da publicação do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), o Senado Federal nacional proferiu aprovação, em 2018, do PLC 53/2018, concretizando-o assim como a Lei Geral de Proteção de Dados brasileira (LGPD). Obtendo seu sancionamento em 14 de agosto de 2018 e com início de vigência determinado em dezoito meses, a Lei nº 13.709 dispõe sobre a proteção de dados no território nacional e modifica a Lei nº 12.965/2014. (BRASIL, 2018)

Com o advento da Lei nº 13.709/2018, O Brasil passou a compor, com determinado atraso, a gama de países que possuem uma lei específica de proteção a dados pessoais. As consequências da demora na elaboração da supracitada lei são antagônicas, uma vez que, por um lado, a lei viabilizou que o tratamento de dados pessoais se comportasse em uma verdadeira “terra sem lei” e, por outro lado, admitiu ao legislador pátrio verificar a experiência internacional para constituir uma lei mais coesa e efetiva, mesmo que tenha que contemplar o cenário político e cultural brasileiro. (BRASIL, 2018)

Dessa forma, no cotidiano brasileiro, quando se deixava de utilizar determinada plataforma virtual, acreditava-se que com a desabilitação os provedores deixavam de deter os dados do usuário. Todavia, o verdadeiro contexto é que ainda excluídas as contas, os dados continuam disponíveis ou armazenados na plataforma. Com o advento da proteção de dados pelo Marco Civil da Internet, e com a ratificação pela Lei Geral de Proteção de dados, o usuário poderá solicitar a exclusão definitiva de seus dados pessoais ofertados à aplicação na seara digital, demanda esta que deverá ser suprida pelo provedor nos ditames da legislação.

Com base na intensa e elevada utilização da seara virtual pelos indivíduos, a circulação contínua de dados na rede se desenvolve em velocidade assustadora. O uso de smartphones e outros meios tecnológicos, possibilitado pela Internet das Coisas, o fluxo de informações e dados são expandidos e facilmente alcançados por organizações.

Para efetuar compras no mercado eletrônico, é necessário obter a disponibilização de relevantes dados pessoais, cartões de crédito, endereços, etc. Desse modo, as redes sociais possuem as mais variadas informações, preferências e posições dos usuários. As organizações, em geral, acumulam tais dados com determinadas informações, como nome, profissão, origem, transações profissionais, dentre outras informações de caráter sigiloso.

Nessa toada, o entendimento de Pereira (2018, p. 4) sustenta que:

> Para fins de aplicação prática, os dados pessoais coletados por estas empresas são toda e qualquer informação, como nome, CPF, RG, nacionalidade, estado civil, profissão, escolaridade, dentre outras. Dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Distintamente de Dado anonimizado, relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

A LGPD normatiza no Brasil, no plano público e privado, a utilização, proteção e transferência de dados pessoais, além de estabelecer quem são os sujeitos envolvidos e seus domínios de responsabilidade por incidentes. A supracitada Lei acarreta impactos diretos em organizações do ramo, tendo em vista que pode estabelecer multas por descumprimentos fundados no grupo econômico que a organização infratora se encontra incluída.

Nessa perspectiva, a LGPD possui como fundamentos as garantias previstas no texto constitucional de 1988 que tangem à privacidade e à liberdade, e ainda o desenvolvimento econômico e tecnológico. Todavia, evidencia-se em seus princípios o da transparência da finalidade, segundo o qual os dados só devem ser usados para objetivos específicos para os quais foram recolhidos e previamente informados aos seus titulares. Destaca-se, ainda, o princípio da necessidade, que comporta a limitação da utilização de dados ao mínimo necessário para que se possa alcançar o objetivo ensejado, da qual se eleva a imprescindível exclusão imediata de dados, após alcançado tal objetivo. (SOMADOSSI, 2018, p. 480)

A LGPD, em seu artigo 5º, conceitua dado pessoal como sendo “a informação relativa à pessoa natural identificada ou identificável”, e toda intervenção da operação envolvida, apontando os conceitos de titular, operador, controlador, transferência, compartilhamento, etc. (BRASIL, 2018)

O texto normativo estabelece que estão passíveis à aplicação da LGPD, sobretudo no plano digital, as pessoas naturais ou jurídicas de direito público ou privado que estejam localizadas em solo pátrio ou que possuam por objetivo o oferecimento de produtos ou serviços no Brasil, devendo a partir da LGPD deter o consentimento expresso do usuário para tal feito.

Sobre a definição de consentimento, compreende-se ao pé da lei, que é toda manifestação livre, informada e inequívoca do titular dos dados, apontando expressamente a sua concordância com o tratamento de seus dados pessoais para um objetivo específico, não sendo acatadas autorizações genéricas, sendo restrito o tratamento de dados, caso a autorização tenha sido alcançada mediante vício de consentimento.

No tocante ao consentimento, este transparece como a principal questão na conjuntura normativa, e a LGPD elenca diversos requisitos para sua validade. Dentre os referidos, verificam-se as informações sobre o tratamento de dados, como, por exemplo, a identificação do controlador e a relação dos dados obtidos, a responsabilidade dos agentes de tratamentos, objetivos e duração.

Portanto, por ser um assunto que eleva várias dúvidas, verifica-se ainda o procedimento de revogação do consentimento no uso de dados pela plataforma que não sejam condizentes os requisitos informados. A LGPD ainda dispõe o direito dos usuários ao acesso e alcance, conforme requisição, de todos os dados que foram manuseados e o adequado tratamento e retificação de informações, haja vista constituir em dever dos agentes a mantença de dados sempre corretos.

4 ESPÉCIES DE CRIMES CIBERNÉTICOS

4.1 CRIMES CONTRA A HONRA

Partindo-se ao enfoque das modalidades de crimes contra a honra realizados na internet, vale ressaltar a difamação, sendo esta recorrente, pois a internet é um local onde os indivíduos costumam expor sua vida profissional e pessoal, sendo, assim, um terreno fértil para a realização de crimes contra a honra. A difamação se define como o ilícito que alcança a reputação de uma pessoa, de modo a prejudicá-la no meio social, encontrando-se tipificada no art. 139 do CP.

O mencionado delito pode atingir como vítima qualquer indivíduo, onde o valor social resta prejudicado nesse ato, podendo ocasionar problemas e transtornos pessoais. A prática consiste em aferir um fato que seja considerado ofensivo à sua imagem perante a conjuntura social, existindo a exigência de que seja exposto para demais indivíduos para a caracterização do ilícito.

No plano virtual, tendo em vista este ser um amplo terreno para debates, muitas vezes tais discussões acabam indo para o lado pessoal, ocasionando delitos como o referido. Os sujeitos criminosos acreditam estarem acobertados pelo anonimato, se escondendo atrás de perfis fakes para tornar mais complexa a identificação. Visivelmente, o plano virtual se tornou um ambiente onde as pessoas se valem de todos os meios para não serem identificadas e, com isso, realizam delitos que afetam não apenas a vida da pessoa vitimada, como também da sociedade como um todo. (MONTEIRO NETO, 2008, p. 187)

Cumpre ressaltar que a difamação, já tipificada na legislação penal, não é uma base completamente segura para a coibição e punição de tais ilícitos, pois a maior barreira para os investigadores se encontra justamente na constatação dos autores. Assim, diversos crimes de difamação realizados na web impedem, muitas vezes, a vítima de efetuar a denúncia, justamente baseando-se no fato da ausência de recursos hábeis para que a polícia encontre o autor, sendo muitas vezes a eficiência do Poder Judiciário colocada em dúvida pela sociedade pela impunidade de delitos como estes.

Outro crime contra a honra que também pode ser realizado pela internet é a calúnia, alcançando essa espécie uma repercussão ainda maior por se referir a uma

imputação de crime à um indivíduo, ferindo tanto sua fé pública quanto sua imagem perante a sociedade.

Obtendo sua tipificação no art. 138 do CP, esta não coíbe totalmente que indivíduos mal-intencionados realizem tal ilícito, pois a conjuntura social, por diversas vezes, é o fundamento para tais condutas, como, por exemplo, em período de eleições é muito frequente manifestações criminosas direcionadas a um determinado candidato, aferindo-lhe muitas vezes delitos que não foram realizados, com visível interesse político no cometimento do crime. (BRASIL, 1940)

Considerando-se tal disposição, qualquer indivíduo pode ser o sujeito ativo desse crime, exceto a pessoa física. É possível separar essa tipificação em três acepções: a acusação de um estabelecido fato, a caracterização deste como delito e, por último, a falsidade do ato ilícito. Logo, nota-se que o fato aferido à vítima, nessa espécie, nunca existiu, o cometimento não precisa ser realizado diretamente à vítima, podendo se verificar diversos modus operandi, sendo efetuado por escrito, meios simbólicos, verbalmente, dentre outros.

A calúnia efetuada na internet é uma verdadeira preocupação, em virtude de atingir um extenso número de indivíduos. Em consideração a tal fato, as proporções acarretadas dos atos cometidos na rede são catastróficas, onde novamente, por intermédio do anonimado, muitos destes crimes não são devidamente coibidos e punidos.

A contínua elevação dessas situações é um vestígio de que cada vez mais os meios informáticos estão sendo utilizados para a realização de ilícitos, sendo observada uma real facilidade para que tais atos sejam cometidos, pois o usuário pode se cadastrar em redes sociais sem uma verdadeira confirmação de identidade, “bastando somente um e-mail e algumas informações que podem ser facilmente adulteradas, ocasionando, assim, uma intensa insegurança nos usuários. “(INELLAS, 2009, p. 64)

Por fim, verifica-se a injúria, que se refere à uma ofensa a outrem violando sua dignidade e ferindo sua honra subjetiva, relativa aos sentimentos que o próprio indivíduo possui e seus convencimentos morais, físicos e intelectuais. Nesse delito, qualquer pessoa pode ser o sujeito ativo, se tratando da modalidade realizada no plano virtual, os efeitos são ainda maiores também devido à elevada disseminação de informações.

A injúria possui tipificação no art. 140 do CP, todavia, mesmo disposto em norma, o delito é realizado com demasiada constância principalmente na internet. Neste ambiente, muitos casos passam sem a devida medida judicial, tal conjuntura se dá pela realização de tais crimes e com as poucas denúncias direcionadas às autoridades competentes. Desse modo, cumpre trazer sua tipificação literal:

O referido crime, diversamente da difamação e da calúnia, não afere a vítima do fato, mas sim, uma atribuição de qualidade negativa ou vaga onde não é estabelecida a conduta, podendo qualquer indivíduo ser sujeito ativo do ilícito, se tratando de crime comum. Desta feita, o decoro do indivíduo é ferido e desrespeitado e a pessoa jurídica não é passível de ser injuriada por se tratar de uma honra subjetiva.

Ainda, vale dizer que os mortos também não recaem a essa tipificação penal, tendo em vista a fala de norma expressa, ao contrário da difamação, que viabiliza os sucessores serem o sujeito passivo após o falecimento. Nessa conjuntura, só se consuma o delito quando a vítima possui conhecimento do ato, não sendo necessário que a prática do delito seja efetuada diante de sua presença e tenha que chegar a conhecimento de outros indivíduos como nos crimes de difamação e calúnia. (CRESPO, 2011, p. 83)

O crime de injúria realizado na web é um fenômeno que deve ser tratado e vislumbrado com muito cuidado, bem como outros delitos contra a honra, é sabido que a consequência que tem a exposição de conteúdo contendo inverdades, atacando um indivíduo, pode ter efeitos imensuráveis.

Portanto, a internet, por ser considerada um ambiente de troca de dados e informações que ultrapassa as barreiras físicas, não deixando de ser um elemento agravante para a realização dos crimes contra a honra e, com a elevação de tais casos, abre-se um debate relevante onde os atos realizados no plano virtual podem ter consequências ainda mais devastadoras no mundo real.

4.2 PORNOGRAFIA INFANTIL E PEDOFILIA

A pornografia infantil consiste em uma espécie de violência sexual realizada contra menores. No cenário brasileiro, a referida conduta encontra tipificação no Estatuto da Criança e do Adolescente (ECA), na legislação penal e também em alguns documentos internacionais, como é o caso da Convenção sobre os Direitos da Criança, realizada em 1989 pela Organização das Nações Unidas (ONU).

Nesse panorama, eleva-se que o delito de pornografia infantil não pode ser confundido com a pedofilia, que é considerada uma doença, um transtorno psicológico onde a pessoa exprime desejos sexuais por crianças e adolescentes. Desse modo, o pedófilo não é tido, a priori, como um criminoso, mas sim como um enfermo, todavia, quando este demonstra sua patologia e essa se encaixa em alguma tipificação disposta na legislação, o indivíduo se torna um criminoso. (CASTRO, 2003, p. 40)

Por seu turno, no cerne da pornografia infantil, não se vislumbra a exigência da realização de relação sexual, sendo o bastante para o enquadramento a comercialização e a divulgação (ou compartilhamento) de materiais pornográficos que englobem menores. A Lei nº 11.829/2008 promoveu uma modificação relevante no ECA, sendo esta a inclusão do art. 241-A, na intenção de criminalizar a obtenção e o porte de tais conteúdos, dentre outros atos relativos à pornografia infantil no plano virtual. (BRASIL, 2008)

O compartilhamento destes materiais na web torna dificultosa a identificação do primeiro indivíduo que a colocou na internet, sendo tal conduta constantemente realizada na Deep Web, ambiente este infactível de identificar o autor do delito, além disso, a viabilidade de propagação ofertada nas redes, bem como o envio e recebimento de conteúdos para qualquer local, contribui ainda mais para a existência desse crime.

O uso da internet por menores, sobretudo as redes sociais e os games, sem a devida observância dos genitores ou responsáveis, contribui ainda mais para a propagação de tais ilícitos, tornando crianças e adolescentes alvos certeiros para delinquentes, tendo em vista que muitos impulsionam redes sociais falsas para dialogar com as vítimas de modo facilitado e sem levantas muitas suspeitas.

Desse modo, é preciso que os genitores ou familiares responsáveis pelo menor observem com atenção o que este acessa e publica na internet, assim como as conversas e chats em redes sociais e de jogos que viabilizam o envio de arquivos como fotos e vídeos que, por um descuido ou ato impensado do menor ao tirar fotos ou gravar vídeos de cunho sexual, pode ter tais conteúdos violados por invasão de dispositivo e disseminados na rede.

A pedofilia, por seu turno, é compreendida como uma enfermidade que ocasiona um desejo sexual por menores, que deve ser devidamente tratada, em muitos casos de pedofilia o ato sexual não é realizado, todavia, existe uma conjuntura delineada como uma obsessão sexual por crianças e adolescentes. Em solo pátrio,

tais situações ocorrem com mais frequência na internet que, por ser um espaço aberto a todos, os criminosos se valem das facilidades tecnológicas para a satisfação de seus desejos sexuais. (PINHEIRO, 2009, p. 224)

O referido delito foi um dos que mais inovou com o advento dos meios tecnológicos e da internet pois, os pedófilos se valem do anonimato nesse plano e, por meio de algumas práticas, como a elaboração de fakes e a utilização de uma linguagem infantilizada, buscam vítimas que ganhem sua confiança, aproveitando-se da vulnerabilidade e inocência das mesmas. Desse modo, a pedofilia pode se caracterizar um delito cibernético quando os pedófilos compartilham entre si conteúdos pornográficos com menores.

A pedofilia na internet, ainda, tornou-se um mercado demasiadamente lucrativo, pois os criminosos se estruturam, por meio de uma rede internacional, na qual todos dissemina conteúdos de crianças e adolescentes e até mesmo a exposição de seu próprio corpo durante a prática de atos libidinosos com menores. Os instrumentos mais efetivos na coibição deste mal são as denúncias, assim, é de extrema relevância que os indivíduos comuniquem e denunciem todo e qualquer ato que envolva a exploração de menores. (PINHEIRO, 2009, p. 227)

Os delitos relativos à pedofilia e suas respectivas sanções estão elencados nos arts. 240 e posteriores do ECA, no qual o legislador deixa nítido que qualquer sujeito que realizar qualquer ato disposto no caput (produzir, fotografar, filmar, registrar, dirigir ou reproduzir material pornográfico de menores) será devidamente punido nos termos da lei, com a sanção de 4 a 8 anos e multa. Desta feita, nota-se que o ECA é uma legislação muito pertinente e completa, por incluir várias formas de comportamentos envolvendo a pedofilia e, consequentemente, dispondo tais penalidades. (CONDACK, 2011, p. 1195)

4.3 FRAUDES, ESTELIONATO VIRTUAL E JOGOS DE AZAR

A fraude virtual pode ser realizada quando o criminoso modifica, invade ou adultera dados constantes no plano virtual, programas ou um sistema de processamento, como, por exemplo, quando um indivíduo invade o equipamento de outro e divulga vídeos íntimos. Assim, no entendimento de Lima (2005, p. 199), as fraudes virtuais podem ser conceituadas como sendo:

> Uma invasão de sistema computadorizados e posterior alteração de dados, que tem como objetivo do autor alcançar vantagens sobre bens, seja esta física ou não, isto é, a adulteração de comprovantes bancários, aprovações em instituições de ensino, resultados financeiros, pesquisas eleitorais, etc.

Desse modo, no cerne das fraudes, os usuários são inseridos de modo manipulado a apresentarem seus dados pessoais e financeiros, por intermédio de sites, páginas, links ou propagandas fraudulentas nos meios de comunicação virtuais. É uma conduta eivada de intenção com a finalidade de atingir um benefício ou satisfação de ordem material ou financeira.

Vale ressaltar que a fraude virtual alcançou tipificação específica com o advento da Lei nº 14.155/2021, que incluiu o § 2º-A e § 2º-B no art. 171 do CP. Assim, dentre as fraudes mais recorrentes no plano virtual encontra-se o phishing, realizado quando os cybercriminosos ludibriam a vítima para o alcance de informações pessoais, como CPF, número e senha de cartões, utilizando-se de sites falsos ou promoções encaminhadas por WhatsApp que comumente são propagandas muito atrativas encobertas de interesses que, verdadeiramente, são apenas formas de se alcançar informações sobre a vítima. Tais fraudes se tornam cada vez mais frequentes, tendo em vista que a internet alcança um número exorbitante de usuários, vários destes propensos a serem vítimas de fraudes virtuais. (CASSANTI, 2014, p. 115)

Por sua vez, o estelionato virtual, igualmente com fulcro no artigo 171 do CP, também nomeado de estelionato digital, é um crime no qual o autor se vale de um meio de comunicação digital, como a internet, para atingir seu propósito de obtenção de vantagens patrimoniais ilícitas, norteando ou condicionando a vítima ao erro. Dessa forma, cumpre destacar a tipificação disposta no supracitado dispositivo.

Esse delito pode ser cometido tanto por um especialista no âmbito cibernético quanto por um leigo que porte o mínimo de conhecimento possível sobre tal seara. Uma das maneiras de se efetuar o crime é através da transferência de valores virtualmente, realizada por vítimas para a conta do autor, quando as mesmas são enganadas por intermédio de diálogos nas redes, como é a situação da simulação de um site de banco, por exemplo. Nota-se, também, a viabilidade de concretizar o crime através de mensagens enviadas para a caixa de e-mail do indivíduo, as quais induzem as vítimas para transferir determinado montante para a inclusão em sorteios, com impressão de que isso lhe acarretará benefícios. (CRESPO, 2011, p. 59)

Nessa conduta, os criminosos utilizam softwares de ponta para monitorar e alcançar a vantagem indevida, com a obtenção de dados e informações pessoais, como e-mails, links, cadastros, sites falsos, dentre outros., e acabam direcionando as vítimas ao erro e ao repasse de dados e informações bancárias e, para que outras pessoas caiam no crime, são efetuados diversos tópicos e assuntos no intento de atingir o maior número de indivíduos possível. (CASSANTI, 2014, p. 55)

Nesse panorama, a legislação pátria inovou trazendo modificações que são muito bem-vindas para o combate ao estelionato digital, como a Lei nº 14.155/2021. A supracitada trouxe algumas alterações no CP e no CPP, no propósito que tornar mais duras as penalidades atribuídas aos delitos de invasão de dispositivos informáticos (154-A do CP), furto (art. 155 do CP) e do estelionato propagado em ambiente cibernético, alterando o art. 171 do CP.

Também, a supracitada Lei inseriu o parágrafo 4º ao art. 70 do CPP tratando sobre a temática, alteração esta bastante almejada pois, na lei antecessora, pairava uma intensa insegurança jurídica no que diz respeito à existência de leis distintas para situações ocorridas no cerne virtual e da divergência jurisprudencial sobre a questão. (BRASIL, 2021)

De acordo com o dispositivo 70 do CPP, os delitos explanados no art. 171 do CP, quando efetuados mediante depósito, emissão de cheques sem a prova de fundos em poder do sacado ou com o pagamento frustrado por meio de transferência de montantes, a competência será determinada em respeito ao local de domicílio da vítima e, no caso da existência de múltiplas vítimas, a competência será determinada pela prevenção. (BRASIL, 2021)

No entanto, mesmo que a recente legislação disponha avanços no cenário brasileiro sobre os crimes cibernéticos, vale dizer que tais casos são cada vez mais comuns e os criminosos nesse âmbito estão sempre se atualizando sobre meios avançados para delinquir, aferindo, assim, a necessidade de uma Lei específica que comporte todos os delitos realizados no meio virtual.

As redes sociais, sobretudo, são alvos constantes de golpes e fraudes, pois é onde as pessoas estão cada vez mais presentes. E um dos lugares que concentra maior número de usuários é o Instagram. Por meio dele, criminosos encontram um terreno fértil para a proliferação de esquemas que explore as inseguranças das vítimas com promessas milagrosa, por exemplo. Recentemente, os jogos de azar no instagram têm ganhado força impulsionados por uma grande quantidade de

publicidade paga. Muita gente acaba se cadastrando em sites fraudulentos sem perceber o risco que está correndo e acabam perdendo dinheiro.

Desde o início da quarentena, devido à pandemia do coronavírus, muitas pessoas têm se entretido com jogos de azar virtuais nas redes sociais. No Brasil, algumas blogueiras famosas tem aproveitado o Instagram para promover esses jogos – que na maioria das vezes são fraudes. Quando os usuários participam desses jogos, eles acabam perdendo dinheiro de verdade sem nem ao menos saber.

Além disso, essa prática é extremamente perigosa já que as pessoas estão ficando cada vez mais expostas a golpes virtuais. Ainda que possa parecer inofensivo, participar desses jogos de azar virtuais é muito arriscado e pode acabar custando muito caro para quem cai nessa armadilha. Por isso, é extremamente importante que as pessoas fiquem atentas e evitem participar desses jogos impulsionados pela publicidade das redes sociais. Além de ser uma prática perigosa, também é ilegal no Brasil.

5 OS DESAFIOS DO DIREITO PENAL NO COMBATE AOS CRIMES CIBERNÉTICOS E SUAS POSSÍVEIS SOLUÇÕES

5.1 ASPECTOS RELATIVOS À INVESTIGAÇÃO DOS CYBERCRIMES

Como vislumbrado em momento anterior, a sociedade contemporânea se encontra delineada por várias inovações e riscos oriundos do advento tecnológico, sendo observada uma ampla propagação dos dispositivos informáticos dentro do contexto social, assim como uma elevada atenção com a integridade destes dados, informações e sistemas.

Dessa forma, com o propósito de respaldar os anseios sociais, demanda-se das autoridades competentes uma esperteza também no cerne dos meios tecnológicos, fazendo-se indispensável um aperfeiçoamento e uma gradativa especialização de sua equipe no tratamento de tais temas. Como não poderia ser diferente, a criminalidade cibernética se demonstra naturalmente desenvolta, sendo muito criativa nas formas de se utilizar os dispositivos informáticos no cometimento dos variados crimes possíveis no âmbito. (SOARES, 2014, p. 206)

Assim, demanda-se que similarmente seja a operacionalização das estruturas de persecução penal, baseada em uma acepção de contínuo conhecimento e aperfeiçoamento. Evidencia-se que a hodierna conjuntura tecnológica viabiliza o acesso à internet por intermédio de diversos equipamentos eletrônicos, desde notebooks e computadores até celulares e carros. Por tais razões, resta nítida a indispensabilidade de que as investigações criminais sejam realizadas de modo célere, levando-se em consideração as peculiaridades dos mecanismos usados na realização do ilícito.

Tendo em vista a multiplicidade de tais mecanismos, ressalta-se que plural também pode ser a edificação de provas no seio das investigações de crimes virtuais, como, por exemplo, arquivos, históricos de computador, e-mails e cookies são algumas das muitas informações que podem ser extraídas para a elucidação dos fatos. De toda sorte, nota-se que as referidas evidências no plano virtual poderiam ser pesquisadas de forma conjunta, levando-se em conta as especialidades que detêm em comparação àquelas oriundas de delitos tradicionais.

Em virtude de estarem intrinsecamente ligadas ao plano digital, a doutrina assenta, a priori, a vulnerabilidade característica de tais evidências. Em conformidade

aos estudos de Seger, não se demandam maiores esforços para que estas venham a ser deterioradas ou limadas, até mesmo no decorrer do processo de colhimento e valoração. (SEGER, 2010, p. 68)

Similarmente, é possível verificar o elevado nível de volatilidade das evidências colhidas no cerne virtual, as quais podem ser facilmente alteradas, tanto pelo delinquente, no intento de ocultar seus vestígios, quando por próprias autoridades mal intencionadas, se não observados e respeitados os cuidados essenciais ao seu tratamento.

Dentre outros elementos característicos, observa-se ainda a facilidade de disseminação de tais dados ou informações, motivo pelo qual se eleva a adoção de medidas apropriadas e atuais de filtragem no decorrer do exame dos dispositivos investigados, de maneira a reduzir os dispêndios e amplificar a eficiência do trabalho efetuado.

Em observância às peculiaridades esboçadas, constata-se a essencialidade de a investigação dos cybercrimes ser realizada minuciosamente, muitas vezes com a disposição de profissionais capacitados, aptos a aferir o adequado tratamento a tais evidências digitais. Assim, a doutrina de Wendt e Jorge elucida que as supracitadas investigações frequentemente se utilizam de duas etapas distintas, sendo a primeira a etapa técnica, isto é, de campo, existindo a concreção de medidas e diligências prévias à atuação da polícia, com o propósito de identificar a forma usada para o cometimento do ilícito, assim como a localização precisa do instrumento que aferiu vazão ao delito. (WENDT; JORGE, 2013, p. 69)

Assim, na fase técnica são materializadas uma diversidade de medidas e procedimentos investigativos, como, por exemplo, o exame das informações aferidas pela vítima, a formalização do ilícito através de um registro ou boletim de ocorrência, a investigação prévia sobre os possíveis autores, a identificação do equipamento usado e, por último, o requerimento da autorização judicial de quebra dos dados de acesso dos acusados à rede. (WENDT; JORGE, 2013, p. 70)

O alcance de tais registros é uma fase primordial para a elucidação dos fatos, uma vez que, por intermédio destes, torna-se factível ter acesso aos logs de conexão e de acesso da pessoa no meio virtual, isto é, ao emaranhado de informações concernentes à forma como ele se usou da rede, por exemplo, IP, datas, horários, duração da conexão, dentre outros.

Nessa linha, Wendt e Jorge (2013, p. 68) ainda explanam que:

> É indispensável trazer à tona a observação técnica de que, quando realizada a conexão de um computador ou dispositivo similar à internet, o endereço de IP (Internet Protocol) é aferido exclusivamente para quele usuário. Do mesmo modo que dois corpos não ocupam o mesmo local no espaço, não existem internautas com o mesmo IP no decorrer da navegação pela rede.

No entanto, além de sua exclusividade, nota-se que o IP também se demonstra dinâmico, uma vez que com o final da conexão de certo usuário à internet, o protocolo até então atribuído a este torna-se mais uma vez disponível, podendo ser repassado para outro usuário. Assim, o IP, propriamente dito, não é apto a contribuir significativamente com a investigação, em decorrência de que dado endereço de IP pode estar conexo a múltiplos usuários distintos por um lapso de semanas ou até mesmo meses.

Sendo assim, evidencia-se a relevância da colaboração entre as autoridades policiais e os provedores de internet na observância de tais delitos, uma vez que somente mediante o acesso ao compilado de registros dos provedores é que se torna factível a ligação do número de IP a certa pessoa, determinando-se qual o dispositivo informático vinculado a tal protocolo na exata data do delito.

Desta feita, antes mesmo que a autoridade policial possa se utilizar de diligências presenciais, a referida “etapa de campo”, com possível uso da busca e apreensão de dispositivos do indivíduo investigado, denota-se a concreção dessa investigação prévia, especializada e embasada no recolhimento de informações constantes na própria internet e no registro de seus provedores.

Portanto, no tocante às particularidades da investigação dos crimes cibernéticos, demonstra-se ser essencial a busca por um contínuo aperfeiçoamento pessoal e instrumental por parte das autoridades responsáveis. No entanto, verifica-se que a dinamicidade de tais evidências (no plano virtual) exige que tal procedimento também se utilize de uma comunicação mais próxima com os agentes privados, sobretudo os provedores.

5.2 A DIFICULDADE NA IDENTIFICAÇÃO DO CYBERCRIMINOSO

É de conhecimento notório que a finalidade precípua da prova judiciária é o reestabelecimento dos fatos almejados, sendo esta o intento pela conexão observada entre os fatos investigados no processo e a verdade entorno da realização do ato no tempo e no espaço. O conteúdo probatório recolhido no decorrer da demanda é de

extrema relevância para o convencimento do juiz sobre a concreção dos fatos objetos da lide. A condenação somente será alcançada mediante a nitidez de culpabilidade, e esta não poderá ser atingida somente por intermédio de suposições, mas sim através de um emaranhado de provas sólidas. (OLIVEIRA, 2011, p. 326)

Para que a punição da legislação penal seja aferida ao indivíduo figurado como imputado, é indispensável a constatação de que esta pessoa tenha realizado o ilícito cibernético. Assim, verifica-se que não vale somente a pura suposição, influxo ou conhecimento escasso sobre a autoria do crime. Especialmente no cerne dos crimes cibernéticos, a adequada constatação do sujeito acusado é um grande intento para que a pretensão punitiva seja adequada e norteada àquele que de fato realizou o ilícito no plano virtual.

Ainda, demonstra-se elevada a preocupação no tocante à identificação do autor, quando levada em consideração, por exemplo, a facilidade que os delinquentes têm de se apoderar de senhas e códigos de acesso de outras pessoas e usá-los para o cometimento de golpes no âmbito financeiro ou na invasão de sistemas através destes dados.

Quando a arguição do crime virtual é estabelecida apenas por meio do apontamento do possível suspeito que realizou o ilícito, não poderá ser instituído um juízo. Assim, verifica-se que a individualização de do sujeito que infração, sua adequada constatação e qualificação, são condições necessárias para a instauração da instrução processual penal. Segundo Malaquias (2012, p. 155) “o ente estatal não pode demarcar o indivíduo, muito menos atingir pessoas indeterminadas com puras inferências.”

Dessa maneira, a identificação de uma pessoa no mundo físico e virtual é realizada de maneira similar. No plano físico, a constatação de um indivíduo na sociedade mistura uma forma de concretização qualitativa, que diz respeito à uma identificação baseada nos aspectos visuais, por meio do reconhecimento de algumas características da pessoa, como altura, traços físicos, voz, dentre outros, capazes de acarretar um reconhecimento e uma constatação legal, por intermédio do número de documento oficial, como CNH ou RG. No plano virtual, a constatação do IP, como demonstrado, concerne à concreção numérica, todavia, a distinção notável é que tal número identifica somente o dispositivo utilizado e não um indivíduo.

Quando equiparados o plano virtual e o físico, no que tange à coleta probatória, verifica-se que a prova alcançada nos meios digitais é mais facilmente observada do

que as do mundo físico, tendo em vista que os peritos responsáveis, por meio de um exame da memória do equipamento ou software, podem identificar um delinquente em qualquer lugar do mundo através do IP.

Contudo, apesar da referida facilidade de monitoramento, viabilizando que o equipamento usado para o ilícito seja corriqueiramente observado e constatado, o grande óbice observado na seara de identificação do autor advém da associação realizada entre o dono do dispositivo e o indivíduo que praticou o delito.

Assim, a constatação do cybercriminoso não é tão simples quanto aparenta, quando se leva em conta que a localização através do IP torna factível a identificação de uma máquina e não, concretamente, do autor do crime. Em suma, o grande impasse vislumbrado nessa etapa está em relacionar a máquina e o indivíduo que a utiliza em determinado lapso temporal. Colli afere como exemplificação para apontar essa complexidade na identificação da autoria quando o delito é cometido em uma máquina de utilização coletiva, como lan houses ou em um dispositivo compartilhado por um grande número de pessoas.

Dessa maneira, os obstáculos entorno da identificação do autor não concernem à identificação do equipamento onde surgiu o crime ou do responsável por tal dispositivo, diz respeito, especialmente, à identificação do indivíduo que agiu com o intento de realizar o crime ou que colaborou para o cometimento deste.

Nas lições de Peck, explana-se que a questão probatória que circunda a autoria é um dos difíceis desafios do Direito na sociedade da informação. A constatação do cybercriminoso, estritamente, só é factível por meio da utilização de biometria correspondente ao uso de características fisiológicas apreciáveis para validar um usuário, como, por exemplo, reconhecimento facial ou impressões digitais. (PECK, 2013, p. 93)

A questão acerca da identidade virtual obrigatório poderia ser considerada como um dos temas mais relevantes do Direito contemporâneo. A falta de uma legislação para acarretar prova de autoria e de um entendimento uniforme incorre em diversas perspectivas de entendimento por parte do magistrado quando se depara com delitos virtuais. Existem magistrados que compreendem que a senha é o bastante para a constatação da identidade do autor do fato; outros, por sua vez, aferem isso somente quando existe o certificado digital, e existem ainda os que sustentam que só com a assinatura do papel. (PECK, 2013, p. 94)

Desta feita, o único modo realmente confiável de prover a identificação do autor em crimes cibernéticos é aquela que possui como embasamento a observância do infrator penal, quando este se vale de elementos corporais para alcançar o acesso à rede e aos dispositivos. Resumidamente, apesar da pseudo facilidade na identificação de um criminoso, através de seu IP, qualquer autoridade policial englobada na investigação de um delito virtual terá que ultrapassar duas barreiras, sendo a primeira a forma de correlacionar o IP constatado com a máquina usada para a realização do crime; e posteriormente encontrar uma forma de relacionar o dispositivo com o indivíduo que a utiliza.

A implementação de uma investigação eivada apenas na pura presunção de suspeição oriunda da autoria de um contrato de acesso à rede, por exemplo, estaria direcionada pela responsabilização objetiva do Direito Penal que, em consonância à Colli, deve ser afastada de qualquer maneira. (COLLI, 2010, p. 92)

Assim, no intento de resolver o impasse que circunda a identificação do cybercriminoso, o autor propõe que o indivíduo que realizou o crime a partir de um equipamento apenas poderá ser responsabilizado na hipótese de prisão em flagrante com essa máquina em operação (ligada). Para Colli, tal resolução pode ser usada tanto na investigação prévia, vislumbrada como a forma de se alcançar os indícios de materialidade e autoria, quanto na ação penal dela oriunda. (COLLI, 2010, p. 92)

5.3 POSSÍVEIS SOLUÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS

A fim de se debater a realização de crimes virtuais sob o enfoque do princípio da extraterritorialidade, eleva-se a teoria da norma penal que possui, dentre seus objetivos, analisar possíveis conflitos de incidência da Lei penal no tempo e no espaço. As disposições penais são enquadradas em normas incriminadoras e não incriminadoras, onde a primeira detém o encargo de estabelecer as infrações penais, demandando condutas ou as vedando, sob pena de sanções ao infrator. Ao verificar os tipos penais incriminadores, nota-se a existência de duas premissas, a primária, com a função de descrever com detalhes o ato que se almeja vedar ou impor; e a secundária, que intenta e função de individualizar a pena. (GRECO, 2015, p. 151)

Por sua vez, as normas não incriminadoras têm por escopo tornar lícitas algumas condutas, distanciar a culpabilidade do agente, aclarar determinadas definições e promover os princípios gerais para a aferição da legislação penal. Estas,

podem ser desdobradas em permissivas, explicativas e complementares. Onde as primeiras se subdividem em justificantes, aquelas com o intento de distanciar a ilicitude da conduta do indivíduo; exculpantes, que almejam extirpar a culpabilidade, isentando o indivíduo de sanções. (GRECO, 2015, p. 152)

Nesse diapasão, o princípio da extraterritorialidade se inclui na modalidade de norma penal não incriminadora explicativa, tendo em vista que viabiliza elencar a possibilidade da aferição da lei penal brasileira em delitos em outros países. Cumpre evidenciar que a norma penal incriminadora será aferida aos fatos que ocasionam reprovação da sociedade, pois a finalidade do Direito Penal é tutelar valores fundamentais essenciais para a existência dos indivíduos, sendo os bens mais importantes, aqueles que não podem ser quantificados por pecúnia, tendo em vista a possibilidade dos demais âmbitos do Direito não assegurarem de modo efetivo a proteção destes.

A fim de concretizar a relação dos crimes virtuais com o princípio da extraterritorialidade, é preciso estabelecer o debate entorno das hipóteses legais em que a norma penal atinge fatos praticados no exterior, norma que almeja determinar regras para um impasse de leis no espaço. Na seara do conflito de leis no tempo, a seara de validade da lei penal pátria é delimitada pela legislação penal em respeito a dois elementos, quais sejam: a territorialidade, disposta no art. 5º do CP, e a extraterritorialidade, com fulcro no art. 7º, § 3 do mesmo Diploma. (MASSON, 2019, p. 283)

Levando-se em consideração que o local onde o delito foi cometido é o ponto que diferencia os dois elementos referidos, é preciso conhecer a norma estabelecedora do local do crime nos termos do Código Penal pátrio. Assim, elevam-se três teorias que abordam sobre o local onde o crime foi realizado. A primeira, chamada teoria da atividade, estabelece que o lugar do delito é onde a ação ou omissão proferida em norma incriminadora se edificou, assim, a execução do ilícito é o âmago central da referida teoria. (MASSON, 2019, p. 285)

Em seguida, a teoria do resultado aponta que é considerado o lugar do delito aquele onde o resultado se dispôs. Por último, verifica-se a teoria da ubiquidade, que estende a determinação do lugar do delito ao unir as teorias explanadas anteriormente. Nesse panorama, a legislação penal adotou a teoria da ubiquidade como norma penal não incriminadora e explicativa do fato determinante para

diferenciar a aferição dos princípios de conflito de leis no espaço, territorialidade e extraterritorialidade.

Nesta senda, o princípio da territorialidade possui disposição no art. 5º, caput, do CP. Sendo regra quando se discute a aplicação da lei nacional. A norma estabelece a aplicação da lei nacional aos delitos realizados no território brasileiro, sem prejuízo de convenções, regras ou tratados de direito internacional. Diversamente, o princípio da extraterritorialidade alcança fulcro no art. 7, § 3, do CP, sendo contrário à concepção do princípio anterior e tem por propósito debater situações em que a legislação pátria será aferida a ilícitos penais realizados em outros países. (BRASIL, 1940)

A denominada extraterritorialidade possui tanto forma incondicionada quanto condicionada, sendo a primeira relativa ao fato de a norma nacional não se sujeitar a qualquer pressuposto para atingir o delito realizado em território brasileiro e cujas hipótese são elencadas no inciso I do art. 7º. A condicionada, no entanto, aduz que a lei brasileira poderá ser aplicada aos ilícitos realizados no exterior desde que observadas e respeitadas as condições vislumbradas no parágrafo segundo e nas alíneas ‘a’ e ‘b’ do parágrafo terceiro do artigo mencionado. (CAPEZ, 2012, p. 352)

Assim, verifica-se quando e como a legislação penal pátria será aferida ao indivíduo que se encontra no exterior, no entanto, resta ponderar como os crimes cibernéticos denotará a aferição da lei ao agente que o comete. Desse modo, nos crimes virtuais, como exposto, é muito dificultosa a tarefa de identificar com clareza o autor do ilícito e, para resolver tal impasse, foi indispensável esboçar um perfil da pessoa ou dos grupos que realizam tais delitos.

Desse modo, vale destacar que a pura ocorrência de o crime ter sido realizado através da internet não acarreta o reconhecimento da Justiça Federal. A competência da JF possui fulcro no art. 109, V, da CF/88, e assim, salvo melhor juízo, não delineia competir a esta deliberar os crimes cibernéticos “V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente.”

Em conformidade à jurisprudência do Superior Tribunal de Justiça, se exige a presença simultânea de dois pressupostos, sendo o primeiro a inexistência de convenção ou tratado internacional por meio do qual o brasil se obrigou a repelir o delito; e o segundo a transnacionalidade da conduta, ou seja, que o delito possua capacidade para emanar efeitos no exterior. Como exemplo, verifica-se o crime de

pedofilia, determinado em seu art. 241-A, do ECA, no qual a pessoa divulga conteúdos que envolvem a pornografia infantil em redes sociais, como, por exemplo, o WhatsApp. (BARROS, 2013)

Nesse panorama, o Brasil é signatário de um tratado internacional que coíbe a pedofilia e as imagens que podem ser observadas por qualquer indivíduo, em qualquer local, edificando-se a competência para a Justiça Federal, de acordo com o entendimento do Superior Tribunal de Justiça, no Conflito de Competência nº 120.999-CE.[2]

No sentido de não existir convenção internacional ou tratado, o crime será de competência da Justiça Estadual, ainda que detenha disposição para propiciar efeitos em outro país. Portanto, é possível notar que não existe uma competência especificamente determinada para o processamento dos delitos cibernéticos, pois é indispensável que exista a adição entre o tratado ou convenção e a transnacionalidade do delito, devendo ser analisado casa situação quando passível de julgamento.

Eleva-se, assim, a figura do hacker, que é o sujeito com amplo conhecimento no âmbito informático, substancialmente apto em programar ou utilizar dispositivos. No entanto, a expressão hacker diz respeito, somente, a um gênero, as espécies são muitas em conformidade com as condutas. Dentre as referidas espécies, verifica-se a

[2] CONFLITO NEGATIVO DE COMPETÊNCIA. DIVULGAÇÃO DE IMAGENS PORNOGRÁFICAS DE MENORES POR MEIO DA INTERNET. CONDUTA QUE SE AJUSTA ÀS HIPÓTESES PREVISTAS NO ROL TAXATIVO DO ART. 109 DA CF. COMPETÊNCIA DA JUSTIÇA FEDERAL. 1. A competência da Justiça Federal para processar e julgar os delitos praticados por meio da rede mundial de computadores é fixada quando o cometimento do delito por meio eletrônico se refere a infrações previstas em tratados ou convenções internacionais, constatada a internacionalidade do fato praticado (art. 109, V, da CF), ou quando a prática de crime via internet venha a atingir bem, interesse ou serviço da União ou de suas entidades autárquicas ou empresas públicas (art. 109, IV, da CF). 2. No presente caso, há hipótese de atração da competência da Justiça Federal, uma vez que o fato de haver um usuário do Orkut, supostamente praticado delitos de divulgação de imagens pornográficas de crianças e adolescentes, configura uma das situações previstas no art. 109 da Constituição Federal. 3. Além do mais, o Brasil comprometeu-se perante a comunidade internacional a combater os delitos relacionados á exploração de crianças e adolescentes em espetáculos ou materiais pornográficos, ao incorporar no direito pátrio, por meio do decreto legislativo nº 28 de 14/09/1990, e do Decreto nº 99.710 de 21/12/1990, a Convenção sobre direitos da Criança adotada pela Assembleia Geral das Nações Unidas. 4. Ressalte-se, ainda, que a divulgação de imagens pornográficas, envolvendo crianças e adolescentes por meio do Orkut, não se restringe a uma comunicação eletrônica entre pessoas residentes no Brasil, uma vez que qualquer pessoa, em qualquer lugar do mundo, desde que conectada à internet e integrante do dito sítio de relacionamento, poderá acessar a página publicada com tais conteúdos pedófilos-pornográficos, verificando-se, portanto, cumprido o requisito da transnacionalidade exigido para atrair a competência da Justiça Federal. 5. Conflito conhecido para declarar competente o Juízo Federal da 16ª Vara de Juazeiro do Norte - SJ/CE, ora suscitado. (STJ - CC: 120999 CE 2012/0020851-7, Relator: Ministra ALDERITA RAMOS DE OLIVEIRA (DESEMBARGADORA CONVOCADA DO TJ/PE), Data de Julgamento: 24/10/2012, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 31/10/2012)

existência dos crackers, que atuam criminosa e premeditadamente, onde seu propósito é o alcance de vantagens ilícitas. (ALMEIDA et. al., 2015, p. 120)

Quando o delito é cometido no plano cibernético, devem ser tomadas algumas medidas para o exame dos fatos. A priori, é preciso constatar qual a forma usada para o seu cometimento, seja por intermédio de e-mails, sites, aplicativos, sistemas, dentre outros, onde cada um dos citados comporta particularidades intrínsecas, desse modo, as providências a serem tomadas também serão distintas.

Segundo os ensinamentos de Rocha (2013, p. 58) é possível aferir que as evidências dos crimes virtuais possuem determinadas características, como “a) formato complexo; b) volatilidade, o que viabiliza sua alteração, eliminação ou perda; e c) costumam estar misturadas com uma extensa quantidade de informações ou dados verdadeiros, o que demanda uma investigação dos fatos ainda mais apurada”.

Dessa maneira, através da identificação do número de IP relativo ao ilícito na internet é possível chegar ao lugar de origem do registro, no entanto, existem formas para ludibriar tais provas, como, por exemplo, wifis abertos e o uso de documentação cadastral inverídica, o que também demanda das autoridades investigadoras elevada atenção para a existência de tais formas de se burlar ou obstaculizar a apuração do crime. (ROCHA, 2013, p. 60)

Por meio da investigação e da adequada análise dos fatos, o Estado entra em pauta para aferir a norma penal ao indivíduo que realizou o delito e, mediante a circunstância de o criminoso estar fora do território brasileiro, passa a ser aferido o princípio da extraterritorialidade.

Assim, conforme já esboçado no estudo, o uso dos dispositivos informáticos para a realização de ilícitos tem sido uma prática cada vez mais corriqueira e, tal fato, ocasiona um grande desafio ao Direito Penal no que tange à adaptação dessa nova conjuntura, desse modo, notoriamente o Direito em si não tem dado conta de acompanhar o intenso avanço dos meios tecnológicos, pois, apesar de já existir algumas legislações específicas sobre o tema, na prática, a impunidade em tais delitos ainda se demonstra extensa em virtude da dificuldade de identificação do autor.

Nesse contexto, é possível perceber que a internet é um fenômeno que ultrapassa fronteiras e que ocasiona ao usuário uma liberdade que foi responsável pela desenvoltura de uma nova forma de se cometer crimes, sendo esta revelada nos delitos cibernéticos, onde indivíduos se valem do presumido anonimato da internet para realizar condutas tipicamente reprováveis.

Diante do exposto, verifica-se uma situação alarmante, que precisa de aperfeiçoamentos e adequações na legislação e seus princípios para o combate da criminalidade cibernética. Sendo assim, o princípio da extraterritorialidade se eleva como instrumento de aferição e alcance da norma ao indivíduo que se encontra em território estrangeiro.

Portanto, em observância aos desafios e empecilhos expostos, é indispensável que exista uma força estimuladora para que a norma passe a ser interpretada de maneira mais extensa e cujo o alcance também seja amplificado. A concepção da extraterritorialidade encontra fulcro na legislação penal pátria, como verificado, e é incontestável que o referido princípio é de suma relevância para o combate dos crimes cibernéticos, além de ser um importante mecanismo para que a lei alcance seu propósito e disponha a proteção adequada aos bens juridicamente tutelados.

CONCLUSÃO

Através da realização do presente estudo, verificou-se que os crimes cibernéticos já são observados há algum tempo no país. Desse modo, com o passar dos anos, tais crimes foram se aperfeiçoando por meio das novas tecnologias, transformando-se em uma grave questão tanto para os especialistas em informática, quanto para os operadores do direito e para os usuários. Sendo possível aferir que os diversos obstáculos ultrapassados com a informatização e o advento tecnológico ressaltaram visíveis adversidades no plano virtual.

Ainda, examinou-se as disposições e a relevância do Direito Digital, do Marco Civil da Internet e da LGPD e observou-se a nítida evolução social e a relação entre a sociedade e tecnologia, elevada por avanços técnicos e adequação de instrumentos e mecanismos que se tornam indispensáveis para melhor qualidade de vida do homem moderno, o desenvolvimento social e a economia.

Com o desenvolvimento da sociedade, relevante se demonstrou o estudo e o entendimento do atual Direito Digital, assim como sua desenvoltura e aplicação. São integrantes deste e como consequência da interação humana com os meios tecnológicos, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, que foram abordados no decorrer do presente estudo, sendo intencionada a observância dos benefícios e necessidades das referidas legislações.

Com o estudo, também se verificou que o compartilhamento e o vazamento de dados pessoais se demonstra um caso complexo e preocupante no ordenamento jurídico, em razão dos desdobramentos do plano digital e da extensa e veloz troca de informações e armazenamento de dados por empresas, acentuando-se ao passo que mais equipamentos possuem a possibilidade de interação virtual, que podem impactar diretamente o direito fundamental à privacidade, com a coleta de preferências, locais, rotinas e informações pessoais.

Verificou-se como e quando a lei penal será aplicada à pessoa fora do país, demonstrando-se necessário ponderar como os delitos cibernéticos ensejam a aferição da lei ao agente que o realiza. Assim, no cerne dos crimes virtuais, é muito complexa a atividade de identificar com nitidez o cybercriminoso e, para resolver tal problema, demonstrou-se essencial delinear o perfil do indivíduo ou dos grupos que efetuaram o ilícito. Assim, através da investigação e da pertinente análise dos fatos, o Estado entra em pauta para aferir a norma penal ao indivíduo que realizou o delito e,

mediante a circunstância de o criminoso estar fora do território brasileiro, passa a ser aferido o princípio da extraterritorialidade, com fulcro no art. 7 do CP.

Portanto, conclui-se que o Direito pátrio tenta acompanhar as alterações sociais e tem aferido passos importantes para o aprimoramento do Direito Digital e sua aplicação. Assim, verifica-se que o Brasil em muito avançou com a promulgação do Marco Civil da Internet e da LGPD, conferindo proteção norteada aos usuários da internet. No entanto, por ser uma matéria ainda recente no âmbito jurídico, muito ainda deve ser aprofundado sobre o assunto, ao passo que este ainda necessita de muitos materiais doutrinários e jurisprudenciais para a devida uniformização e solidificação de entendimentos práticos sobre o tema.

REFERÊNCIAS

Graduação - Ciências Humanas e Sociais UNIT, Aracaju, v. 2, n. 3, 2015.

AMÂNCIO, Tania Maria Cardoso. **O impacto da informática na sociedade e o direito no Brasil.** São Paulo: Revista Jurídica Consulex, 2013.

ASCENSÃO, Oliveira. **Sociedade da informação e mundo globalizado**. 2012. Disponível em: < http://www.apdi.pt/pdf/GLOBSOCI.pdf >. Acesso em: 05 out. 2021.

BARROS, Bruno. **A competência federal e os crimes praticados pela internet**. 2013 Disponível em:< http://blogdobrunobarros.blogspot.com/2013/04/a-competencia-federal-e-oscrimes.html >. Acesso em: 29 out. 2021.

BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. São Paulo: Editora 34, 2010.

BRASIL. **Decreto-lei nº 2.848, de 07 de dezembro de 1940**. Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm >. Acesso em: 20 ago. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm. > Acesso em: 21 ago. 2022.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8069.htm > Acesso em: 25 set. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm > Acesso em: 25 set. 2022.

BRASIL. **Lei nº 11.829, de 25 de novembro de 2008**. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm > Acesso em: 05 set. 2022.

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. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm > Acesso em: 23 set. 2022.

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. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm > Acesso em: 03 out. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 22 set. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 22 set. 2022.

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. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm > Acesso em: 06 set. 2022.

BRASIL. Superior Tribunal de Justiça. **CC: 120999 CE 2012/0020851-7**, Relator: Ministra Alderita Ramos de Oliveira. Data de Julgamento: 24/10/2012, S3 – Terceira Seção. Data de Publicação: DJe 31/10/2012.

CAPEZ, Fernando. **Curso de direito penal:** parte geral. volume 1. 16. ed. São Paulo: Saraiva, 2012.

CAPEZ, Fernando; GARCIA, Maria Stela Prado. **Código penal comentado.** 4. ed. – São Paulo: Saraiva, 2013.

CAPEZ, Fernando. **Curso de direito penal**, volume 1, parte geral – 23ª ed. – São Paulo: Saraiva Educação, 2019.

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

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.

COLLI, Maciel. **Cibercrimes**. Limites e perspectivas à investigação policial de crimes cibernéticos. Juruá Editora, 2010.

CONDACK, Cláudia Canto. **Curso de Direito da Criança e do Adolescente**: Aspectos Teóricos e Práticos. 5ª ed. Rio de Janeiro: Lumen Juris, 2011.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011.

DE LUCCA, Newton; SIMÃO FILHO, Aldalberto (coords.). **Direito e internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

DELMANTO, Celso. DELMANTO, Roberto. **Código penal comentado**. 9. ed São Paulo: Saraiva, 2016.

GRECO, Rogério. **Curso de direito penal**. 17. ed. Rio de Janeiro: Impetus, 2015.

INELLAS, Gabriel Cesar Zaccaria de Inellas. **Crimes na Internet**. São Paulo. Editora Juarez de Oliveira. 2009.

JESUS, Damásio De. ARAS, Vladmir. **Crimes de informática**: Uma nova criminalidade. Disponível em < https://jus.com.br/artigos/2250/crimes-de-informatica >. Acesso em: 25 set. 2022.

JUSTINO, Patricy Barros. Criminologia. 1 ed. Rio de Janeiro: Editora Estácio. 2016.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.

LIRA, Leide de Almeida. **Lei Carolina Dieckmann eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos.** Disponível em: <https://conteudojuridico.com.br/open-pdf/cj048868.pdf/consult/cj048868.pdf>. Acesso em: 28 set. 2022.

MAÍLLO, Alfonso Serrano. **Introdução à criminologia** (tradução de Luis Régis Prado). 1. ed. São Paulo: Revista dos Tribunais, 2007.

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova**: a investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012.

MARCACINI, A. **Aspectos fundamentais do Marco Civil da Internet**: Lei nº 12.965/2014. São Paulo: Edição do autor, 2016.

MASSON, C. **Direito penal**: parte geral. Vol. 1. 16. ed. Rio de Janeiro: Forense, 2019.

MONTEIRO NETO, J. A. **Aspectos Constitucionais e Legais do Crime Eletrônico**. Fortaleza, 2008.

OLIVEIRA, Eugênio Pacelli. **Curso de Processo Penal**. Rio de Janeiro: Lúmen Júris, 2011.

ONU. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em < http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf > Acesso em: 01 out. 2022.

PEREIRA, Luiz Fernando. **A Lei Geral de Proteção de Dados Pessoais:** uma teoria finalística. Revista Jus Navigandi, set. 2018. Disponível em: < https://jus.com.br/artigos/68967/a-lei-geral-de-protecao-de-dados-pessoais-uma-teoria-finalistica >. Acesso em: 26 set. 2022.

PINHEIRO, Patricia Peck. **Direito Digital.** 3ª ed. São Paulo: Saraiva, 2009.

PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. **A nova lei de crimes digitais**. 2013. Disponível em: < www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432 >. Acesso em: 10 set. 2022.

PRADRO. Luiz Regis. **Curso de direito penal brasileiro**: parte especial, São Paulo: Revista dos Tribunais, 2013.

REIS, Wanderlei José dos. **Delitos cibernéticos**: Implicações da Lei n.º 12.737/12. São Paulo: Revista Jurídica 2013.

ROCHA, Carolina Borges. **A evolução criminológica do direito penal**: aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. Jus Navigandi, v. 18, n. 3706, 2013.

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

SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos:** a tutela penal do discurso de ódio nas redes sociais. Revista dos Tribunais. vol. 997. ano 107. São Paulo: Editora RT. 2018.

SEGER, Alexander. **Cybercrime Training for Judges**: training manual. – Strasbourg: Economic Crime Division, Council of Europe, 2010, p. 67. Disponível em: < http://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/eventos-2/eventosinternacionais/conteudo-banners-1/crimes-ciberneticos/cybercrime-training-for-judges-trainingmanual/view. > Acesso em: 27 set. 2022.

SILVA, Patrícia Santos da. **Direito e crime cibernético**: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas**: perspectivas e limites. Tese de doutorado. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014.

SOMADOSSI, Henrique**. O que muda com a Lei Geral de Proteção de Dados (LGPD)**. Revista Migalhas, n. 4.478, 2018.

SUMARIVA, Paulo. **Criminologia:** teoria e prática. 3 ed. São Paulo: Editora Impetus. 2010.

VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos**: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso. Revista da ESMAPE. Recife. v. 15. n. 32. 2010.

SILVA, Patrícia Santos da. **Direito e crime cibernético**: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

VIANA, Eduardo. **Criminologia**. 5 ed. Salvador: Editora: JusPodivm, 2018.

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