LUIZ INÁCIO BARBO DE SIQUEIRA FILHO

CIBERCRIMES E A TIPIFICAÇÃO DAS CONDUTAS PERANTE O ORDENAMENTO JURÍDICO BRASILEIRO

CURSO DE DIREITO – UNIEVANGÉLICA
2022

LUIZ INÁCIO BARBO DE SIQUEIRA FILHO

CIBERCRIMES E A TIPIFICAÇÃO DAS CONDUTAS PERANTE O ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada ao Núcleo de Trabalho de Curso da UniEvangélica, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação da Professora Me. Karla de Souza Oliveira.

ANÁPOLIS – 2022

LUIZ INÁCIO BARBO DE SIQUEIRA FILHO

CIBERCRIMES E A TIPIFICAÇÃO DAS CONDUTAS PERANTE O ORDENAMENTO JURÍDICO BRASILEIRO

Anápolis, _____ de _____ 2022.

Banca Examinadora

_____

_____

AGRADECIMENTOS

Agradeço primeiramente a Deus.

Agradeço aos meus pais que desde o início estiveram ao meu lado me apoiando.

Agradeço também a minha orientadora Karla, que teve toda paciência e dedicação contribuindo para a conclusão desta monografia.

Agradeço também aos meus amigos, que fizeram com que esta reta final se tornasse menos tensa.

RESUMO

O presente trabalho monográfico tem por finalidade o aprofundamento da questão que versa acerca dos cibercrimes e a tipificação das condutas perante o ordenamento jurídico brasileiro. O objetivo deste consiste em descrever o que é considerado cibercrime, destacando a tipificação das condutas e fornecendo análise acerca do ordenamento jurídico brasileiro. A metodologia é respaldada em um plano científico, sendo aplicado o método interpretativo-jurisprudencial, uma abordagem dedutiva e procedimentos bibliográfico, documental e historiográfico. Para finalizar o referido Trabalho de Conclusão de Curso será discorrido em breves parágrafos uma conclusão a fim de demonstrar em síntese o que se pode extrair acerca dos cibercrimes em geral e a tipificação das condutas empregadas pelos sujeitos ativos dos crimes.

Palavras-chave: Cibercrime; Doutrina; Ordenamento jurídico; Tipificação; Condutas.

SUMÁRIO

INTRODUÇÃO

A presente monografia tem por objetivo analisar e estudar cibercrimes e a tipificação das condutas perante o ordenamento jurídico brasileiro, vez que estes são uma novidade para o milênio e possuem diversas atualizações doutrinárias que desencadearam no surgimento de jurisprudências relevantes para o estudo jurídico.

Para tanto, faz-se necessária a análise de todo o histórico de desenvolvimento da internet desde os primeiros crimes praticados por meio da rede mundial de computadores e dispositivos eletrônicos conectáveis até os dias atuais de forma a observar como a evolução da tecnologia tornou propicia a evolução criminosa perante a rede.

A partir desta análise urge para tanto a exposição destes avanços de forma concomitante com o avanço da inteligência criminosa, para que assim possam restar demonstradas quais são as condutas tipificadas no ordenamento jurídico pátrio, resultantes das práticas de crimes cibernéticos.

Nos últimos anos o Brasil tem se apoiado na Lei nº 12.735/2012 (Lei Azeredo), Lei nº 12.373/2012 (Lei Carolina Dieckmman), Lei nº 12.965/2014 (Marco Civil da Internet) e Lei nº 14.155/2021, para reprimir os crimes cibernéticos, pois são os principais fundamentos jurídicos que a legislação possui para a condutas criminosas desta natureza.

Destaca-se que os cibercrimes possuem tipificação perante o Código Penal através da introdução trazida pela legislação e visam tutelar, dentre tantos bens

jurídicos, a honra, a dignidade e até mesmo o patrimônio vez que os crimes praticados nestes ambientes oferecem risco a estes bens jurídicos.

Por fim, tecidas breves considerações acerca dos principais pontos a serem abordados nesta monografia, dessa maneira e de forma imparcial, o trabalho monográfico que se realizará tem por interesse e objetivo analisar os aspectos dos cibercrimes em todas as suas nuances, sempre atento a mais alta e mais recente discussão doutrinária e jurisprudencial do Tribunal de Justiça de Goiás sobre o tema.

CAPÍTULO I – DIREITO DIGITAL

Este capítulo visa tratar de temas que se relacionam ao direito digital. Os tópicos abordarão de forma objetiva o histórico e evolução do direito digital, conceito e a legislação, e ainda o vínculo entre o direito e a Lei Geral de Proteção de Dados (LGPD).

O direito digital se traduz na evolução do próprio direito, abrangendo princípios e instituições fundamentais que são válidos e aplicáveis até os dias de hoje, além do fato de introduzir novas instituições e elementos do pensamento jurídico em todos os seus campos.

Segundo a análise de NOVO (2019, *online*) este ramo do direito é o resultado da relação entre a ciência do Direito e a ciência da Computação, sempre empregando novas tecnologias. Correspondendo assim ao conjunto de normas que visam tutelar as relações humanas e as violações comportamentais em ambientes digitais.

Ou seja, como usando a tecnologia, as pessoas enviam e recebem informações, realizam negócios, expressam opiniões, entre outros, deve haver regras e condutas de convivência para que direitos e princípios sejam respeitados nestas comunidades, a fim de orientar o comportamento para que ninguém seja lesado.

Em que pese a Lei Geral de Proteção de Dados, que também será abordada neste capítulo, esta surge como reguladora, em parte, deste direito, uma vez que proteger os dados dos usuários da internet e preservar a privacidade de cada um, através da aplicação de normas e exigência de termos para o uso das redes.

Com o nascimento da LGPD nasce também a necessidade de um órgão que a aplicasse e regulasse sua utilização, o que por sua vez deu origem a Autoridade Nacional de Proteção de Dados Pessoais – ANPD. Todo esse desenvolvimento trouxe pressa ao mundo jurídico em razão da necessidade de organização das empresas e alinhamento direto entre profissionais de tecnologia da informação e advogados especialistas da área.

1.1 Histórico e evolução

O mundo virtual utilizado através da *internet* tornou-se um elemento essencial do dia a dia da humanidade, e é inimaginável contar atualmente com uma sociedade sem contato a internet. Faz necessário desta forma compreender que a tecnologia, independentemente de sua forma ou nível de evolução, sempre delineia o progresso coletivo para moldá-lo, transformá-lo e guiar o cotidiano humano em torno de novas conquistas tecnológicas, a fim de trazer evolução social.

A humanidade sempre teve como alvo a evolução e a busca por meios que tornassem as atividades diárias mais fáceis, foi assim desde as descobertas pré-históricas sobre como controlar o fogo, a criação de utensílios básicos que originaram a Revolução Neolítica, até as Revoluções Industriais do século XX que, inovaram o sistema de produção e também a exploração de recursos naturais, sendo ainda relevante apontar os desempenhos importantíssimos da internet na mudança de estilo de vida da humanidade e na jornada trabalhista (SILVA, 2021, *online*).

Neste sentido, a *Internet*, atua como principal ponto de avanço contemporâneo alavancando assim a sociedade para a inserção no meio digital, exercendo a mesma conduta de desenvolvimento de outras “revoluções” tecnológicas, talvez ainda maior do que qualquer outra pré-existente, em razão da facilidade de conexão e o acesso ilimitado que proporcionam uma transformação radical na esfera social (SILVA, 2021, *online*).

Assim, é possível notar que “o direito digital surge como resultado da relação entre as ciências de Direito e Computação, para acompanhar o mundo digital.

Logo, a partir do momento que o ambiente virtual existe, é lógica a necessidade de que exista para este ambiente um poder moderador que, controle e regule as relações ali existentes, qual seja o Direito Digital.” (NOVO, 2019, *online*).

Desta forma, partindo da realidade de que “o Direito Digital decorre de relações sociais e do alcance interno e externo de seu meio de atuação, as mudanças muito rápidas e em curto espaço de tempo forçam uma característica a ser construída, qual seja, a celeridade de leis em torno das sociedades altamente informatizadas com fim de acompanhar o desenvolvimento das problemáticas da sociedade moderna e buscar saná-los.” (PAIVA, 2002, *online*).

Em razão desta necessidade de velocidade de transformação da lei e constante atualização para limitar comportamentos perante o mundo digital, considerando este mundo como uma esfera autônoma, passou-se a considerar este ramo do direito também como autônomo, tal como o Direito Civil, o Direito Penal, o Direito Empresarial, o Direito Tributário, e demais.

Importante ressaltar que toda esta autonomia adquirida pelo direito digital repousa em sua variedade de fontes próprias, conforme entendimento de Marcelo Cardoso Pereira:

> O Direito Digital possui todas as características para ser considerado uma disciplina autônoma, justificando a sua posição através de três argumentos: possui um objeto delimitado, qual seja a própria tecnologia, dividido em duas partes, sendo a primeira o objeto mediato, ou seja, a informação, e o segundo o objeto imediato, ou a tecnologia; a existência de uma metodologia própria, a qual visa possibilitar uma melhor compreensão dos problemas derivados da constante utilização das novas tecnologias da informação (informática) e da comunicação (telemática); tal tarefa se realiza mediante o uso de um conjunto de conceitos e normas que possibilitam a resolução dos problemas emanados da aplicação das novas tecnologias às atividades humanas; a existência de fontes próprias, ou seja, fontes legislativas, jurisprudenciais e doutrinárias; não havendo como negar a existência dessas fontes no âmbito do Direito Digital; foi justamente a existência de ditas fontes que possibilitaram, em um grande número de países, principalmente os mais desenvolvidos, a criação da disciplina do Direito Digital nos meios acadêmicos. (2003, *online*)

Os questionamentos acerca da autonomia do direito digital estão relacionados às realidades jurídicas, vez que muitas relações praticadas no âmbito digital já eram tratadas em temas de direito civil e penal, por exemplo. Porém, ao desenvolver esta disciplina regulatória buscou-se segurança diante da constante construção de relações *online* e inovações por meio de diversas formas de condutas que podem ser lesivas aos usuários, criando assim tipificações especificas com fim de combater práticas que afrontem os direitos dos usuários (SILVA, 2021, *online*).

É claro que a evolução social está ligada diretamente a evolução do direito e por óbvio ao surgimento do direito digital, tendo em vista que o ser humano buscou por anos sua evolução até alcançar o sistema digital pelo qual realizam-se a maioria das atividades diárias na vida das pessoas atualmente, facilitando a vida destes (LEAL, 2014, *online*).

Desta forma é possível perceber que evoluir para o mundo digital possuiu suas vantagens, mas também existiu a necessidade de regular essa evolução para que os direitos já conquistados até então não fossem violados nesta nova modalidade de comunicação. O direito digital surgiu para que fossem mais bem geridas as relações online, desde conversas informais até mesmo negócios e assinaturas contratuais.

1.2 Conceito e a legislação

Conforme tratado anteriormente, “o direito digital é o ramo do direito que possui por objetivo fornecer regras, normas e princípios para uso dos ambientes digitais pelos seus usuários, com fim de oferecer e garantir proteção de informações contidas nesses espaços e em aparelhos eletrônicos diversos pelos quais estes indivíduos se conectam com o mundo digital.” (FACHINI, 2021, *online).*

Observa-se deste modo que, é um ramo bastante recente do direito, vez que lida de forma direta com o emprego da tecnologia na execução de tarefas diárias, em especial por meio do uso da internet. A tecnologia e o uso da internet são cada vez mais o ponto de início de todas as relações humanas, desta forma o direito digital se torna cada vez mais relevante para a proteção das informações das pessoas, além

de ser, uma área cada do direito cada vez mais importante e frutífera no mundo jurídico (FACHINI, 2021, *online*).

Através da era digital e por meio da informatização das coisas, surge para este desenvolvimento um problema natural e até mesmo estrutural, pois “onde há mais tecnologia, existem também mais riscos de ataques virtuais, roubo, vazamento e destruição de dados e até mesmo hackeamento de informações relevantes para indivíduos, empresas e governos, que seja usuários da rede mundial de computadores.” (PINHO, 2022, *online*).

Deste modo, “o desenvolvimento de leis e procedimentos que visam a segurança e proteção dos usuários atacados ou não, e a punição de condutas que prejudiquem terceiros digitalmente, deve ser considerada como um caminho natural a seguir seguido, para não dar margem a impunidade digital.” (PINHO, 2022, *online*).

No Brasil o arcabouço normativo conta com pouca legislação voltada especificamente para o direito digital, sendo possível elencar três leis que foram aprovadas nos últimos dez anos e que foram consideradas como fundamentais para a consolidação desse ramo do direito no país, quais sejam: a Lei Carolina Dieckmann, publicada em 30, Nov. de 2012, o Marco Civil da Internet, publicado em 23, abr. de 2014 e ainda a Lei Geral de Proteção de Dados Pessoais, publicada em 14, ago. de 2018.

A Lei Carolina Dieckmann, como é informalmente conhecida a lei nº 12.737/12, traz em seu texto a tipificação de crimes informáticos, alterando o Código Penal de acordo. Esta lei versa acerca da aplicação de penas para crimes como, invasão de aparelhos eletrônicos, interrupção de serviços digitais ou de conexão, falsificação de documentos ou de cartões de crédito ou débito, crimes estes bastantes comuns no dia a dia dos brasileiros (BRASIL, 2012, *online*).

O referido texto legislativo traz esse nome considerado mais informal “em razão de ter sido aprovada no mesmo ano em que a atriz Carolina Dieckmann teve fotos e conversas íntimas vazadas por uma pessoa que havia recebido aparelhos

eletrônicos dela para conserto, expondo assim a intimidade da atriz de forma pública.” (SILVA, 2021, *online*).

Já o Marco Civil da *Internet*, que é assegurado pela Lei nº 12.965 do ano de 2014, “estabelece princípios, garantias, direitos e deveres para o uso seguro da internet no Brasil, além de estipular e definir as diretrizes para a ação do Estado dentro das redes, sem cerceamento da liberdade de expressão.” (BRASIL, 2014, *online*).

“A legislação em questão traz temas de extrema relevância sobre como a internet deve ser utilizada em território nacional, preservando sempre a liberdade de expressão, neutralidade e privacidade. Esta estabelece ainda critérios de direitos e deveres de usuários, além de trazer regras para a manutenção da privacidade deles por terceiros, como provedores de serviços de internet e demais empresas.” (BRASIL, 2014, *online*).

A Lei Geral de Proteção de Dados, por sua vez, foi desenvolvida a partir da Lei nº 13.709 do ano de 2018, e é provavelmente a lei a mais relevante dentro do campo do direito digital. Como o próprio nome já traz, essa lei tem como objetivo específico resguardar os dados pessoais de pessoas e empresas que estão dentro da internet, conforme aponta o seu artigo 1º:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018, *online*)

Essa lei trouxe enorme impacto para as relações comerciais de empresas que adquiriam e utilizavam dados de usuários, sem seu devido consentimento com fim de prospectar clientes, uma vez que passou a exigir maior transparência das empresas para com o público, mostrando como utilizam dados pessoais dos usuários (BRASIL, 2018, *online*).

“A proteção de dados é uma das discussões mais relevantes a respeito do direito digital no mundo inteiro. Ter uma legislação específica para essa proteção, que

garante maior transparência na manipulação desses dados pelas empresas, foi um passo fundamental para a área no Brasil” (FACHINI, 2021, *online*).

Todas essas leis supramencionadas são de enorme importância para a segurança digital dos usuários da rede mundial de computadores, vez que estas leis contam com aparato tecnológico para localização, identificação e devida punição para aqueles que praticam atos contra a comunidade de usuários e acabam por lesar estes.

1.3 Direito e a LGPD

Atualmente na sociedade brasileira existe uma certa preocupação para com os dados e identidade das pessoas no mundo digital, essa preocupação surge do fato de dados sensíveis serem coletados diariamente pela rede mundial de computadores para que tarefas simples do dia a dia sejam realizadas, como é o caso de compras online, entre outros.

Toda essa preocupação deu origem a Lei nº 13.709 publicada em 14, agosto de 2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que trouxe imposição normativa para que instituições públicas e privadas, que realizem tratamento de dados pessoais, para que estas se adequassem à referida Lei, com fim de proteger dados pessoais dos usuários (BRASIL, 2018, *online).*

Este recente norteador do direito digital aplicado através de legislação esparsa é destinado à tutela de direitos fundamentais de liberdade e privacidade de todos os cidadãos usuários, e adotou um cunho didático ao trazer definições e conceitos a princípio compreensíveis por toda sociedade.

“A Lei Geral de Proteção de Dados possui 10 capítulos e 65 artigos que se encontram distribuídos da seguinte forma: Capítulo I - apresenta as disposições gerais e traz no art. 2º os princípios que fundamentam a proteção de dados pessoais, no art. 3º a territorialidade de aplicação da lei, no art. 4º é trazido a inaplicabilidade da lei, e no art. 5º temos os conceitos gerais.” (TEPEDINO, 2019, *online*).

A referida lei pode ser vista como uma espécie de freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância, a fim de conter a maciça extração de dados e as diversas aplicações e utilizações que a eles podem ser dadas sem a ciência ou o consentimento informado dos usuários (PINHEIRO, 2018, *online*).

Em seu texto legal a LGPD dispõe acerca do "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (PINHEIRO, 2018, *online*).

A conformidade à Lei nº. 13.709/2018 Lei Geral de Proteção de Dados Pessoais, é hoje o grande objetivo das organizações, e ela deve estar elencada no plano estratégico das corporações, isto se deve ao fato de que estas grandes empresas têm grandes números de clientes e um vazamento de dados destes clientes poderia trazer inúmeros problemas (BRASIL, 2018*, online*).

A Lei Geral de Proteção de Dados também trata em seu rol acerca de "uma política repressiva, educativa e punitiva, a fim de que aqueles que não se adequarem a esta sejam multados e corrijam suas falhas sistêmicas que expõe indivíduos a vazamentos de informações" (BRASIL, 2018*, online*).

Dentre as sanções previstas na LGP as multas previstas para as empresas que violarem as regras podem ser bastante pesadas. É o que nos traduz o artigo 52 da referida lei, no qual são estipuladas as sanções e multas aos infratores conforme os incisos I ao VI:

> Art.52. (...)
> I – advertência, com indicação de prazo para adoção de medidas corretivas;
> II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III – multa diária, observado o limite total a que se refere o inciso II;

> IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI – eliminação dos dados pessoais a que se refere a infração. (BRASIL, 2018*, online*)

Toda essa rigidez em aplicar multas de valor elevado se justifica pela seriedade com que os dados devem ser tratados pelas pessoas jurídicas que passam a ter acesso a estes. Os dados de um indivíduo podem causar danos irreversíveis a sua vida e principalmente expor a maiores riscos em golpes.

É importante destacar que o órgão que é responsável por fiscalizar e aplicar estas sanções e multas é a Autoridade Nacional de Proteção de Dados Pessoais - ANPD, além destas funções, o art. 55-J da LGPD estabelece algumas outras funções da ANPD, dentre as quais s destacam as seguintes:11

> Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
> Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
> Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
> Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
> Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
> Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à Lei;
> Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos;

> Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;
> Programar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (BRASIL, 2018*, online*)

No que se refere aos poderes sancionatórios, a LGPD passou a determinar que a ANPD deverá publicar seu próprio regulamento de aplicação de sanções, incluindo a metodologia utilizada para o cálculo da base de multa. Este assunto ainda passa por algumas consultas públicas para ser discutido e melhor aplicado à sociedade (BERTINI, 2022, *online*).

A ANPD deve ainda aprimorar e intensificar o trabalho e continuar a realizar publicações sobre temas setoriais, bem como adotar normas, diretrizes e melhores práticas para adequar as leis a situações específicas que podem vir a surgir e depender de legislação própria para ser colocado em prática (BERTINI, 2022, *online*).

Logo, a partir disto é possível considerar o Brasil como um dos países pioneiros em LGPD em todo território latino-americano em termos de legislação digital, dividindo o posto com países como Argentina e Chile, onde a lei de proteção de dados já havia chegado há algum tempo.

CAPÍTULO II – CIBERCRIMES E O DIREITO COMPARADO

Diante de toda a evolução social e tecnológica empenhada ao longo dos anos, conforme abordado em capítulo anterior, surge para a sociedade moderna a problemática dos crimes virtuais, ou como são conhecidos, os *cibercrimes*. Estes restaram caracterizados como crimes praticados no mundo virtual que envolva qualquer atividade ou prática ilícita na rede.

Neste sentido, pretende-se abordar no presente capítulo as definições de *cibercrimes* e ainda casos emblemáticos que marcaram a sociedade envolvendo crimes praticados no mundo virtual sejam estes por meio de vírus ou até mesmo desvio de dados.

Em que pese o direito comparado fica a cargo de este capítulo retratar também a evolução e os sujeitos dos crimes, a *internet* das coisas e para concluir uma leitura mais aprofundada acerca da inteligência artificial (IA), tendo como objeto de estudo as moedas digitais como a criptomoeda *bitcoin.*

Por resumo a internet das coisas se refere a facilidade dos moveis eletrodomésticos e de outros aparelhos utilizados na sociedade atual, vez que este tipo de mecanismo funciona de forma prática e pode automatizar funções do dia a dia por meio de *Wi-Fi*, dados móveis ou até mesmo *Bluetooth*.

A inteligência artificial possui um papel de grande importância na sociedade moderna e é através dela que diversos investidores têm conseguido realizar movimentação de criptomoedas no mundo virtual. Todo processo de investimento e

acompanhamento das moedas é administrado pelo mecanismo de forma autônoma, trazendo conforto para aquele que possui a vontade de investir.

2.1 Casos emblemáticos de cibercrimes

O desenvolvimento da tecnologia sempre foi considerado como importante força motriz na vida em sociedade, tanto pessoal quanto profissionalmente. No local de trabalho, a tecnologia simplifica processos e auxilia empresas no ato de reduzir custos e aumentar a eficiência nas demandas.

Porém, tudo possui seu lado bom e o ruim e com a internet não seria diferente. À medida que a tecnologia se desenvolve, trazendo benefícios para todos os aspectos da sociedade como um todo, ela também abre espaço para que criminosos ajam anonimamente, roubem dados vitais e causem danos financeiros a diversas organizações por meio dela (NASCIMENTO, 2014, *online*).

Com o passar dos anos foi possível perceber um aumento no nível dos casos de crimes cibernéticos, a história nos mostra que até as grandes empresas, que investem pesado em segurança, estão sujeitas a esse tipo de ataque e que por mais que haja busca incessante para prever possíveis ataques, estes podem surgir de onde menos se espera.

O termo *cibercrime* surgiu pela primeira vez em um painel do grupo G-8 (composto por sete dos países mais ricos do mundo e a Rússia, por sua importância histórica e militar), próximo ao final dos anos 1990. A conferência discute exatamente as formas e meios utilizados para combater as condutas ilegais na *Internet* (NASCIMENTO, 2014, *online*).

Segundo Anderson Nascimento (2014) dentre os temas discutidos a época da conferência, tratou-se acerca das características do *cibercrime*, dentre elas seu domínio transnacional, o que dificultava e ainda dificulta a investigação e a coleta de provas contra os réus. E, ainda a proliferação de computadores pessoais, que permitiram que qualquer pessoa no mundo cometesse crimes contra indivíduos em qualquer lugar do planeta, sem sequer sair de casa.

Um dos primeiros vírus a serem detectados no mundo virtual ficou conhecido como Vírus Melissa, este vírus começou a ser encaminhado no ano de 1999, por meio de um anexo e cada usuário que abrisse o anexo encaminharia o mesmo e-mail para toda a lista de contatos. Apesar de não ter um propósito financeiro, o vírus chegou a causar um impacto aproximado de 80 milhões de dólares em computadores e sistemas de rede, tanto privadas quanto públicas (HARAN, 2018, *online).*

Algum tempo depois a empresa *Sony* no ano de 2011, segundo Wakefield (2014), se tornou algo de um grupo hacker que invadiu e roubou dados pessoais de mais de 70 milhões de usuários de sua plataforma online. Desta forma, com os dados vazados, a empresa ficou fechada para tentar reparar e corrigir as falhas do sistema e ainda foi condenada a pagar 15 milhões de dólares em taxas judiciais pela exposição dos dados dos usuários. (WAKEFIELD, 2014, *online*)

A justificativa da empresa para a invasão e de que está se deu por meio de uma falha simples na vulnerabilidade da rede, onde seu código fonte, que não era criptografado, poderia ser descoberto com uma simples invasão do banco de dados, assim como ocorreu, demonstrando assim a fragilidade do sistema de segurança do banco de dados da empresa (WAKEFIELD, 2014, *online*).

No ano de 2013, a maior fabricante mundial de software de edição de imagens, Adobe, sofreu um grande ataque cibernético. O *hacker* acabou por roubar dados de quase 150 milhões de contas, dentre eles dados pessoais e bancários de seus usuários. Felizmente, os dados bancários na plataforma online da empresa eram criptografados antes de ser armazenado na nuvem, tornando os dados inutilizáveis para crimes bancários, o que amenizou o estrago da situação, mas que não deixou de preocupar a todos os seus usuários (HIGA, 2013, *online*).

Outro caso bastante conhecido e que causou enormes transtornos foi o “pesadelo sul coreano”, no ano de 2014, mais de cem milhões de sul-coreanos tiveram seus dados roubados, GOGONI narra a ação:

> A ação foi rápida e simples, um consultor do KCB (Korea Credit Bureau), banco coreano, copiou os dados para um HD externo sem dificuldades enquanto prestava serviços de consultoria interna ao banco, ele então apenas vendeu os dados online para telemarketing e revendedores de crédito, e mais de 20 milhões de sul-coreanos tiveram que cancelar seus cartões de crédito. (2014, *online*)

Logo, os crimes acima referenciados poderiam ter sido evitados caso houvesse uma política de segurança de dados mais minuciosa e segura, mas, destaca-se que foi a partir desses casos que o sistema internacional buscou instaurar a obrigatoriedade de uma lei para proteção de dados, que no caso do Brasil é conhecida como Lei Geral de Proteção de Dados (LGPD).

2.2 Evolução e sujeitos dos cibercrimes

Diante da crescente variedade de crimes surgiram para o âmbito virtual com o passar do ano, faz-se necessário entender o processo desta evolução, desde o seu início até os dias atuais. Atualmente, *cibercrime* é o termo mais utilizado para especificar condutas ilícitas que utilizam meios de informática para a prática de crimes.

Nos raciocínios de Erick Teixeira Barreto a terminologia de cibercrime mais aceita no momento é:

> O cibercrime é no momento o termo mais frequentemente usado para rotular as atividades em que os delinquentes usam computadores, ou outros dispositivos eletrônicos de TI, através de sistemas de informação, para facilitar comportamentos ilegais. Em essência, o cibercrime envolve o uso de aparelhos eletrônicos para acessar, controlar, manipular ou utilizar os dados para fins ilegais. (2020, p. 55).

Neste sentindo, é de se destacar, portanto, que mesmo havendo diversas maneiras de caracterizar as condutas criminosas praticadas em meio ao mundo digital, o objetivo maior é saber que, são crimes que manuseiam aparelhos eletrônicos para praticar atos que passam a compor uma conduta considerada como digitalmente criminosa (BARRETO, 2020, *online*).

Assim, como em todo crime, é necessário que haja a identificação de agente ativo e agente passivo do crime, no caso do cibercrime não é diferente. O sujeito passivo, ou vítima dos crimes virtuais, são aqueles sobre os quais é possível

identificar que foram vítimas de uma conduta ilícita ou comissiva do sujeito ativo (LIMA, 2005, p. 237).

Insta salientar que em relação aos crimes informáticos, pode o sujeito passivo ser uma pessoa civil, instituições de créditos, o governo e outras personalidades que utilizem sistemas automatizados de informação, estejam conectados ou não à internet, fazendo com que o público passível de se tornar vítima se estenda a todos aqueles que são usuários da rede mundial de computadores (LIMA, 2005, p. 237).

Em que pese os sujeitos ativos do cibercrime, estes são considerados como os criminosos, aqueles que praticam o delito no âmbito virtual causando danos aos sujeitos passivos. Por muitas vezes o criminoso usa de um conhecimento específico para causar o dano ou tão somente causa a perturbação dos usuários no mundo virtual (CRESPO, 2005, *online)*.

Conforme conceitua Crespo, os tipos de sujeito ativos podem ser:

> I – Hackers: que é um nome genérico, define os chamados “piratas” de computador, sendo que a melhor tradução para a palavra da língua inglesa é fuçador.
> II – Crackers: considerados os verdadeiros criminosos da rede, ocupam-se de invadir e destruir sites, nesta categoria está presente também ladrões, valendo-se da internet para subtrair dinheiro e informações, sendo o termo Cracker, a expressão consagrada para denominar os criminosos que utilizam os computadores como armas. (2011, p. 95-98).

Assim como demonstra o autor, existe uma notável distinção entre os dois tipos de sujeito ativo, sendo que os hackers são aqueles fazem por curiosidade, para detectar falhas e afins, já os crackers são aqueles que agem com a intenção de causar dano aos usuários, pois realizam a invasão para a obtenção de alguma vantagem (CRESPO, 2011, p. 95-98).

Segundo Nathan Guerrieri (2016) além do hacker e do cracker como sujeitos ativos dos cibercrimes é possível identificar ainda as figuras dos defacers e Phreakers. Para o autor, os defacers são pessoas ou grupos que, através de certo

conhecimento informático, passam a modificar ou simplesmente causar danos a sites na Internet, pois devido a grande quantidade de tempo utilizado na Internet, estes passam a procurar sites vulneráveis para atingi-los, desta forma a gama de atuação destes agentes tem crescido muito nos últimos anos.

Em relação aos phreakers, o autor identifica-os como “pessoas com conhecimento específico em frequência de linha telefônica e computação que utilizam sua inteligência para fazer usos indevidos de linhas telefônicas”, mas este conhecimento não se dá somente em linha fixa como também em celulares, onde os phreakers conseguem realizar ligações sem custo algum ou até mesmo grampear telefones para roubo de informações (GUERRIERI, 2016, *online*).

Assim, o sujeito ativo dos crimes cibernéticos nem sempre será um gênio nas telecomunicações, mas aquele que pratica este tipo de crime adquiriu algum conhecimento específico para praticá-lo vez que essa atividade exige destreza para lidar com o manuseio de computadores e dispositivos informáticos.

2.3 Internet das coisas

A internet das coisas, conhecida através da sigla em inglês IoT, que significa *Internet of Things*, é um termo que está cada dia mais em uso, sendo possível localizá-lo em notícias, cursos, em eletrodomésticos, sendo possível identificá-lo também na comunicação entre os usuários da rede de computadores.

A internet das coisas pode ser conceituada, segundo KIANE (2019, online) como “aquilo que tem o potencial de impactar não só como vivemos, mas também como trabalhamos e estudamos.”, neste sentido é possível compreender que a internet das coisas tem por intenção promover a reformulação da vida em sociedade, causando mudanças consideráveis no dia a dia dos indivíduos usuários da tecnologia da informação.

A popularização, ou seja, o acesso facilitado a internet e aos aparelhos de conexão via rede *Wi-fi*, *Bluetooth* ou dados móveis nos últimos anos, acabou por propiciar maior desenvolvimento tecnológico para o mundo, gerando maior

acessibilidade e automatização dos lares e das atividades que compreendem o dia a dia de seus usuários (MOREIRA, 2022, *online*).

Na prática a internet das coisas versa tão somente acerca de um dispositivo que, realiza diversas tarefas pertinentes ao dia a dia do indivíduo, promovendo a automatização do item equipado com alguns mecanismos que possibilitam a conexão a uma rede, podendo ser tanto *Wi-Fi* como *Bluetooth* e dados móveis (3G, 4G e 5G) (ALECRIM, 2022, *online*).

Destaca-se, porém, que desde a sua criação até o atual cenário, a internet das coisas, passou por diversas atualizações e acabou por agrupar diferentes funções de outras tecnologias aos seus mecanismos de funcionamento, entre essas, a Inteligência Artificial (IA). Desta forma, os dispositivos conectados conseguem acessar diversas informações armazenadas em nuvens e aprendem com esses dados a realizar tarefas básicas do dia a dia que economizam tempo aos seus usuários (CARVALHO, 2021, *online*).

Os recursos ofertados pela internet das coisas, ou IoT, possuem diferentes modelos de tecnologia presentes em diversas áreas do cotidiano, dentre essas, CARVALHO (2021, *online)* destaca:

> - Casa: existem inúmeros aparelhos baseados em IoT, por exemplo, a Smart TV, termostatos, geladeiras e fechaduras inteligentes.
> - Wearable: são equipamentos “vestíveis”, ou seja, acessórios que utilizamos no corpo, como os smartwatches e fones de ouvido.
> - Saúde: a tecnologia ajuda na integração com o prontuário do paciente. Com isso, alterações no estado clínico, como alteração na pressão sanguínea e frequência cardíaca, são rapidamente atualizadas no registro, otimizando o atendimento médico.
> - Agricultura: os sensores IoT ajudam no monitoramento da temperatura, umidade do solo e do ar, ativando automaticamente os sistemas de irrigação, quando necessário.

Estes são apenas alguns dos recursos mais influentes na rotina dos usuários da IoT. Faz-se importante destacar que a IoT não promove a automatização apenas de usuários pessoas físicas, promove também a automatização de empresas,

grandes negócios e até mesmo de hospitais, garantindo a todos aqueles que a utilizam conforto e segurança (ALECRIM, 2022, *online*).

Deste modo, no contexto apresentado, resta claro que, na atualidade já é possível encontrar dispositivos IoT que são utilizados em situações comuns no dia a dia e nas esferas profissionais. Dessa forma, essas ferramentas tecnológicas estão contribuindo para a transformação digital que está acontecendo no mundo, sendo possível visualizar de forma concreta a internet das coisas.

2.4 Inteligência Artificial (Moedas Digitais e Bitcoin)

A Inteligência artificial ou IA, como é conhecida por sua sigla, versa sobre um modelo de tecnologia que permite aos sistemas conectados a ela a captação de informações e dados digitais, de forma a adquirir inteligência suficiente a ponto de desenvolver as atividades de modo autônomo, sem a necessidade de influência ou comando humano.

Os historiadores acreditam que o desenvolvimento da ciência da computação se deu em meados da década de 1940, quando o mundo estava mergulhado na Segunda Guerra Mundial e os países precisavam investir em tecnologia de guerra e inteligência investigativa. Então, durante a Guerra Fria, as nações mais uma vez entraram em uma grande corrida tecnológica que impulsionou todos os tipos de soluções inovadoras em biologia, medicina, espaço e, claro, computação (LAVAGNOLI, 2019, *online*).

Deste modo, em meio ao caos das guerras, no ano de 1956, o professor John McCarthy da Universidade de Dartmouth, em Hanover nos Estados Unidos, selecionou um grupo de cientistas para buscar uma forma de “ensinar” as máquinas a compreender e repetir atividades, da mesma forma que o cérebro humano atua. Para tanto, seria estritamente necessário descrever de forma precisa todos os aspectos do aprendizado e outras características da inteligência humana, e só assim então as máquinas seriam capazes de utilizar a linguagem, resolver problemas e aperfeiçoar-se gradativamente (LAVAGNOLI, 2019, *online*).

Este grupo de estudos do então professor McCarthy apontou os principais aspectos da problemática da inteligência artificial e elaborou um plano de estudos voltados para o desenvolvimento da IA como mecanismo tecnológico do futuro. Anos mais tarde essa ferramenta foi fortemente desenvolvida e passou a ocupar espaços importantes na vida dos seres humanos (LAVAGNOLI, 2019, *online*).

Essa tecnologia é considerada como um divisor de águas para o desenvolvimento da comunidade cientifica, vez que foi projetada para imitar as habilidades cognitivas e de raciocínio humanas. Neste sentido, BRITO (2021, *online*) afirma que:

> Esse mecanismo tecnológico deve ser encarado como uma criança pequena, cujo sistema cognitivo não está totalmente formado, sempre observando as pessoas ao seu redor, como se comportam, como se pronunciam, como realizam tarefas, começando pelas mais simples de andar, beber, comer, e até mesmo as coisas mais difíceis, como tomar decisões sobre uma determinada situação, ou mesmo como reagem a diferentes ambientes.

Insta salientar que, o mesmo acontece com as máquinas portadoras desta inteligência artificial, pois é a partir dos dados que estas coletaram, que seus próprios sistemas desenvolvem uma compreensão de tudo que foi memorizado e que sobre o tratamento destes dados que passaram por um intenso processo de análise, classificação e organização. Possibilitando que essas máquinas saibam distinguir entre gosto, comportamento, o que é padrão, o que é humano, o que é objeto e assim por diante (BRITO, 2021, *online)*.

Os seres humanos têm usado essa inteligência para se beneficiar há anos, em especial os investidores que agora passam a se utilizar da IA para obter informações mais rápidas e, assim, identificar as melhores oportunidades de negócios com as moedas digitais, ou criptomoedas como são conhecidas (CABRAL JÚNIOR, 2022, *online*).

As informações financeiras, tanto sobre criptomoedas quanto a respeito do mercado tradicional, ficam disponíveis na internet. Os investidores se utilizam muitas vezes da ferramenta *Deep Learning*, nome dado a uma técnica de inteligência artificial

que, através das informações fornecidas e memorização de dados cadastrados junto a plataforma, passa a imitar o pensamento humano dentro de suas limitações como robô (CABRAL JÚNIOR, 2022, *online*).

Esta inteligência artificial acaba por captar e gerir as informações automaticamente, para que assim aprenda com elas e possa realizá-las de forma autônoma, sem envolvimento de um ser humano. Esta ferramenta também é capaz de incluir maiores análises em seu processo como a de sentimentos, para que seja possível indicar que um país vai começar a utilizar o Bitcoin, por exemplo, (ALKUDMANI, 2020, *online)*.

Em resumo, a inteligência artificial é a tecnologia que fornece permissão às máquinas para que estas pensem como seres humanos, segundo BRITO (2021, online) “este é o ponto em que se unem as tecnologias físicas, biológicas e digitais.”, gerando a partir dessa nova tecnologia máquinas que são capazes de aprender coisas e comportamentos novos com base na repetição de padrões ou dados, a partir da percepção de preferências até se tornarem capazes de tomar suas próprias decisões em determinadas situações.

.

CAPÍTULO III – CRIMES CIBERNÉTICOS E OS TRIBUNAIS SUPERIORES

Durante o discorrer de todo o texto monográfico restou abordado às principais características da rede mundial de computadores e ainda sobre os crimes praticados nela, conhecidos como crimes cibernéticos. Essa tratativa central traz à tona a interpretação dos tribunais quanto aos crimes praticados no mundo virtual.

No presente capítulo serão apresentados quatro tópicos distintos, sendo o primeiro destes a criminalização dos cibercrimes, de forma a expor o apanhado histórico da legislação que passou a considerar os atos criminosos praticados no mundo virtual como crimes da esfera penal.

Seguinte a este, ainda abordar-se-á a análise jurídica dos cibercrimes no Brasil, de forma a demonstrar a evolução legislativa do país quanto a repressão dos crimes do mundo virtual. De forma complementar o tópico seguinte exporá os desafios que esta legislação enfrenta para reprimir as referidas condutas, vez que os crimes que permeiam a rede mundial de computadores são praticados com certo cuidado por parte dos criminosos para que se evite a descoberta de quem os pratica e sucessivamente sua punição.

Assim, para a conclusão o tema tratado versará acerca dos termos de uso e a política de privacidade, sendo desenvolvido de modo a explicitar o que são estes termos e qual a sua relação direta com a privacidade do usuário do mundo virtual, definindo de forma clara quais são os limites da internet e sua segurança em geral.

3.1. Criminalização dos cibercrimes

Com a edição da Lei nº 12.737, datada de 30 de novembro de 2012, popularmente conhecida como Lei Carolina Dieckmann, que passou a tratar acerca dos cibercrimes, ou seja, crimes praticados em dispositivos com acesso informático, o código penal brasileiro sofreu uma alteração notável, pois passou a abordar um tema que, até então, não possuía tipo penal específicos para lidar com estes delitos. Desta forma, é possível o destaque de que em outros países, como por exemplo, Portugal já existia, à época, legislações específicas para tratar dos cibercrimes (BRASIL, 2012, *online*).

Anterior a lei suprareferenciada passar a ser dotada de validade legal, boa parte das condutas criminosas praticadas por meio de dispositivos informáticos eram enquadradas em tipos penais comuns. Nesse sentido, para que os criminosos não ficassem impunes, os crimes cometidos por estes eram tratados como atos ilícitos praticados no mundo real. Porém, segundo PEREIRA (2013, *online*), muitas das condutas criminosas praticadas não eram punidas, pois estas eram consideradas como fato atípico.

Neste sentido, mister se faz apontar que o termo criminalizar surge no intuito de, segundo MEU DICIONÁRIO (s.d., *online*) “considerar crime (um ato)”, ou seja, ao tratar sobre determinada conduta desempenhada no ambiente virtual como conduta criminosa é possível extrair-se que houve a criminalização do cibercrime, de forma a tornar comum o surgimento de leis que tipifiquem crimes praticados neste contexto fático.

Deste modo é possível afirmar que a criminalização do cibercrime no mundo teve início na década de 1960, nos Estados Unidos, vez que à época, notou-se o surgimento perante a imprensa e através da literatura científica norte-americana dos primeiros casos de uso da rede de computadores para prática de crimes como sabotagens e espionagem, desta forma tão logo o país buscou desenvolver leis severas para punir estas condutas e repelir novas tentativas de ataque (BARROS, 2006, *online*).

No Brasil os tramites para criminalização dos crimes praticados através da rede mundial de computadores demoraram um pouco mais para acontecer, vez que a legislação brasileira não acompanhou o ritmo do crescimento vertiginoso da internet e dos crimes virtuais. É possível observar este atraso através da penalização da pornografia infantil visto que, esta circulava pelo país desde meados dos anos 90, porém somente no ano de 2008 a Lei nº 11.829/2008 alterou o Estatuo da Criança e do Adolescente, passando a efetivamente penalizar a pornografia infantil virtual. Destaca-se ainda que leis específicas de combate a crimes virtuais, que trouxeram alteração ao Código Penal, só entraram em vigor a partir do ano de 2012 (BRASIL, 2008, *online*).

A Lei nº 11.829 de 2008, referenciada alhures, visou alterar o Estatuto da Criança e do Adolescente, introduzindo artigos para aprimorar o combate à pornografia infantil e "criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet" (BRASIL, 2008, *online*).

A referida lei instituiu, dentre outras, pena de reclusão de 3 a 6 anos para quem:

> Art. 241 – A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (BRASIL, 1990, *online*).

Seguinte a esta lei, surge para o cenário da legislação brasileira a Lei nº. 12.015, de 2009 que, visou alterar a legislação constante no Estatuto da Criança e do Adolescente, com o intuito de punir assediadores virtuais, passando a instituir, dentre outras penas a pena de reclusão de 1 a 4 anos para quem buscasse relações com menores de 18 anos em salas de bate-papo da *Internet* (BRASIL, 2009, *online*).

Inúmeras outras leis foram criadas nos últimos anos buscando punir diferentes práticas criminosas do mundo virtual, como por exemplo, a Lei Carolina Dieckmann que visou repelir e punir de forma ativa a invasão de dispositivos informáticos e a violação de dados. Destaca-se que recentemente a referida lei teve sua pena aumentada através da edição de outra lei, qual seja a lei nº 14.155/2021,

demonstrando o interesse nítido do legislador de além de criminalizar punir também com peso práticas de cibercrimes (BRASIL, 2021, *online*).

Neste sentido é possível notar que o Brasil, de forma alinhada ao pensamento mundial, busca através de sua legislação reprimir e punir crimes praticados através de dispositivos informáticos, ou seja, condutas criminosas praticadas no mundo virtual e que são frutos do trabalho de *hackers*.

3.2. Análise jurídica dos cibercrimes no Brasil

A tecnologia e o seu uso correto proporcionam inúmeras vantagens para a sociedade, dentre elas se destacam a: comunicação, informação, entretenimento, prestação de serviços bancários on-line, pagamento de contas, encontrar um emprego, assistir a filmes, programas de TV, documentários, ouvir músicas, realizar reservas de hotéis, compra e venda de produtos e mercadorias, entre outros. Apesar disso a *internet* disponível para tais funções oferece também aos seus usuários os meios para praticar cibercrimes.

A problemática que se acumula no país acerca dos cibercrimes é a de que, além de o sujeito passivo ter que saber tomar medidas preventivas, estes também devem ser altamente adaptáveis, pois as circunstâncias das invasões podem mudar com o tempo visto que os criminosos são criativos e diariamente buscam novas formas para praticar crimes no mundo virtual (RUTHERFORD, 2015, *online).*

Neste sentido, insta destacar que, os casos de crimes cibernéticos denunciados no Brasil aumentaram significativamente nos últimos anos. No ano de 2017, o Brasil ficou em sétimo lugar no ranking de países com mais ciberataques em relação ao mundo todo. Já no ano de 2019, o país cresceu em números de ataques, alcançando o terceiro lugar no ranking mundial (CUNHA, 2021, *online*).

Esta situação passou a ser encarada com maior seriedade em razão da pandemia, visto que, a população passou a se utilizar de escritórios domésticos, famoso *home Office,* para trabalho o que alimentou e contribuiu fortemente para os ataques virtuais acontecessem, em razão da falta de software de segurança. Além

disso, com o crescente uso de ferramentas tecnológicas, passou a ocorrer também maior compartilhamento de informações via *links*, o que acaba levando ao hackea mento de dispositivos informáticos como computadores e celulares (CUNHA, 2021, *online*).

Em recente pesquisa realizada pelo FortiGuard Labs, laboratório de inteligência em ameaças digitais da Fortinet (2022, *online*), tornou-se público que:

> O Brasil sofreu 31,5 bilhões de tentativas de ataques cibernéticos de janeiro a junho deste ano, o que representa um aumento de 94% em relação aos 16,2 bilhões de tentativas registrados no mesmo período do ano passado. Colocando o país como o segundo mais visado da América Latina, atrás de México, com 85 bilhões, e seguido por Colômbia (com 6,3 bilhões) e Peru (com 5,2 bilhões).

Estes dados se tornaram preocupantes, vez que a população aparentemente está vivenciando um enorme impacto causado pelos *hackers*, estelionatário, criminosos, que se utilizam da internet e dos meios de comunicação para obtenção de vantagem ilícita, seja ela monetária ou não (FORTINET, 2022, *online*).

Deste modo, cabe suscitar a necessidade urgente de melhorias e investimentos em softwares, programas de segurança para os usuários brasileiros da rede mundial de computadores. Dentre essas melhorias há de se destacar também a necessidade de se ampliar e aplicar de forma devida a punição para aqueles que cometem os cibercrimes.

3.3. Tipificação do cibercrime no código penal brasileiro

Atualmente, é possível verificar que a existência de avanços significativos nas questões que permeia o acesso à internet, no entanto, faz-se necessária reflexão acerca de possíveis benefícios e danos causados pelo uso da rede de computadores.

Deste modo, embora haja punições aplicáveis às condutas criminosas praticadas pelos autores de crimes virtuais, há de se destacar que o Código Penal brasileiro foi formulado no ano de 1940, época essa em que não era possível ter

acesso a internet no Brasil, tornando assim o referido código uma lei genérica e não eficaz para combater todas as condutas ilícitas que acompanharam a evolução digital, por ser anterior ao advento da internet (BRASIL, 1940, *online*).

Neste sentido, como previsto perante o texto da Lei nº 2.848/1940 sobre a aplicação da lei penal no art. 1º “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.”, assim, não pode um indivíduo ser punido por um crime que sequer ocupa espaço perante a legislação penal nacional (BRASIL, 1940, *online*).

Diante deste fato, começaram a tramitar perante o legislativo diversos projetos de lei com o intuito de introduzir ao código penal brasileiro dispositivos que, passassem a punir sujeitos ativos das condutas criminosas praticadas através de dispositivos informáticos (FERRARI, 2020*, online*).

Deste modo, além dos supramencionados Projetos de Lei, que tramitaram perante a Câmara, referente à árdua tarefa de combater o cibercrime no país, é possível observar que, como alternativa, o Brasil visou aderir e ratificar a Convenção de Budapeste. (FERRARI, 2020*, online*).

Toda essa evolução ideológica trazida para a legislação brasileira através do estudo da convenção de Budapeste carregou o Código Penal, com a tipificação de crimes que podem e são diariamente praticados através do mundo virtual, condutas estas conhecidas como cibercrimes (FERRARI, 2020*, online*).

Dentre estes cibercrimes há de se destacar a possibilidade da prática de furto qualificado praticado por meio de dispositivo teleinformático, esta prática está descrita perante o art. 155 §4º-B e §4ºC, da seguinte forma:

> Art.155 (...)
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.

> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (BRASIL, 2021, *online*).

Outros dispositivos legais que sofreram bastantes alterações foram os institutos dos crimes contra a honra, elencados perante os artigos 138, 139 e 140 do Código Penal, porém as alterações sofridas por estes não se baseiam e retificação de seu texto e sim na atualização de sua interpretação normativa, vez que esta passou a se estender aos crimes praticados na ordem virtual (BRASIL, 1940, *online*).

Dente tantos outros crimes que passaram a ser interpretados de forma expansiva e até sofreram modificações em seus textos legais merecem destaque o crime de ameaça (art. 147 do CP); extorsão (art. 158 do CP); extorsão Indireta (art. 160 do CP); escárnio por motivo de religião (art. 208 do CP); favorecimento da prostituição (art. 228 do CP); ato obsceno (art.233 do CP); escrito ou objeto obsceno (art. 234 do CP); incitação ao crime (art. 286 do CP); apologia de crime ou criminoso (art. 287 do CP); invasão de dispositivo informático (art. 154-A do CP); apropriação indébita (art. 168 do CP); estelionato (art. 171 do CP); violação de direito autoral (art. 184 do CP) (BRASIL, 1940, *online*).

Assim, a partir da edição de diversas leis que favoreceram a criminalização dos cibercrimes e ainda com a atualização legislativa sofrida pelo código penal há de se destacar que é claro o intuito do legislador a punição dos criminosos que se valem do mundo virtual para ofender, discriminar, mentir, furtar, enganar e violar direitos.

3.4. Termos de uso e política de privacidade

A própria internet possui suas leis, existem termos de uso pré-estabelecidos por aqueles que querem fazer uso da rede mundial de computadores. Os Termos de uso e política de privacidade são considerados como uma espécie de contrato que passa a reger e estruturar a relação entre usuários da Internet e proprietários de sites, para tornar menos perigosa a relação dos usuários com os sites.

Neste liame os termos de uso e políticas de privacidade são imprescindíveis para que um determinado site ou empresa trate os dados dos usuários de forma correta. Esses termos de uso, tidos como contratos, vão permitir que as informações dos titulares sejam utilizadas apenas para a finalidade prevista nestes contratos e para os objetivos da empresa em coletar esses dados (BRASIL, 2021, *online*).

Deste modo é possível perceber que os referidos termos de uso, tratados como contrato entre usuário e administrador de página, pode ser considerado como um contrato de adesão, visto que para se utilizar daquele meio informático o usuário deve concordar com os termos daquela determinada plataforma sem a possibilidade de fornecer qualquer resquício de alteração em suas cláusulas (BONANI, 2020, *online*).

Por esta razão, os Termos de Uso devem ser explícitos e de fácil visualização pelo usuário. De forma que, caso haja algum mau uso da plataforma, a culpa não será da empresa que deixou os termos implícitos e de difícil acesso, mas sim do usuário que não se atentou aos termos de uso contidos na página (BONANI, 2020, *online*).

Porém, merece destaque que, caso algum dos usuários destas páginas se depare com cláusulas abusivas ou até incoerentes com o objetivo da empresa, de forma a causar dano ao usuário, este poderá optar por não utilizar a plataforma e até mesmo recorrer a um órgão de fiscalização para que os termos sejam retificados de forma a se adequarem conforme a lei, com intuito de que o consumidor seja protegido e seu direito não seja violado (BONANI, 2020, *online*).

Por sua vez, a política de privacidade arraigada aos termos de uso descreve a forma de tratamento dos dados do usuário que concordar com os termos, vez que estes podem se tratar de dados sensíveis. Segundo a Lei Geral de Proteção de Dados temos como conceito de “dados sensíveis”, dados que envolvem questões particulares dos usuários, como religião, opinião política, partido e assim por diante. As questões de proteção de dados estão relacionadas com os princípios contidos nesta lei (BRASIL, 2021, *online*).

Percebe-se deste modo que a proteção de dados sensíveis envolve o resguardo dos princípios da liberdade de expressão, da privacidade e do livre desenvolvimento da personalidade e da dignidade. Com isso, fica evidente também a importância da lei para orientar a questão, além do tratamento de dados gerais, aqueles que identificam o usuário: nome, data de nascimento, RG ou CPF etc., com todas essas proteções sobre os dados, os titulares mantêm seus direitos (BONANI, 2020, *online*).

Portanto, a política de privacidade definirá quais dados serão utilizados, a finalidade para a qual os dados são coletados, como serão processados, se serão acessados por terceiros ou se poderão ser compartilhados com interessados. Com isso, o titular pode autorizar ou não o uso de seus dados de acordo com a política de privacidade da plataforma digital (CARNEIRO, 2020, *online*).

Por fim, cabe destacar que antes da Lei Geral de Proteção de Dados, os termos de uso e as políticas de privacidade não exigiam condições mais rígidas, nem o consentimento do usuário precisava necessariamente ser tão claro e autorizado que os usuários não notassem. Porém, atualmente através da LGPD toda essa política de privacidade se tornou mais rígida de forma que o desrespeito a esta poderá culminar em uma ação indenizatória com fim de suscitar a proteção de direitos digitais.

CONCLUSÃO

Deste modo é possível concluir a presente monografia através da análise de que a legislação brasileira vem se tornando intolerante para com os cibercrimes, visto que nos últimos anos tem-se editado mais leis acerca do tema do que em toda década passada.

Por sua vez, a intolerância legislativa tem seu nascimento marcado pelo reconhecimento da Lei nº 12.735/2012, também conhecida como Lei Azeredo, que tinha como objetivo tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, teve alguns artigos de seus artigos vetados.

Seguinte a esta Lei, surgem para o ordenamento jurídico novas leis, porém no início ainda havia certo receio do legislador e de toda a bancada do congresso, pois a tecnologia ainda não era um ambiente completamente explorado no Brasil, então restava para os operadores da lei a dúvida de até que ponto era se caracterizaria crime em uma conduta praticada em meio a internet, tendo em vista toda autonomia com que essa surgiu.

Porém, o ponto alto de todo esse movimento pró-criminalização cibernética ganhou força a partir do Marco Civil da Internet, editado no Brasil através da Lei nº 12.965/2014, que passou a assegurar usuário o direito ao sigilo de suas comunicações via internet (salvo por ordem judicial); informações claras e completas dos contratos de prestação de serviço; não fornecimento a terceiros de seus registros.

A regulamentação de uso da internet trouxe para o brasileiro maior segurança em suas relações *online*, vez que, aos poucos foi se construindo melhor

que “a internet não é terra sem lei” e o que é feito através dela também é passível de responsabilização.

Diante do que restou aqui apresentado tornou-se claro o motivo da escolha do presente tema vez que inúmeras dúvidas e discussões que pudessem vir a surgir acerca dos cibercrimes e a tipificação das condutas perante o ordenamento jurídico brasileiro foram sanadas através deste trabalho monográfico.

Logo é uma problemática que se acumula e que possui constante crescente perante o ordenamento jurídico face às grandes atualizações tecnológicas enfrentadas. Portanto, há motivos suficientes para que este trabalho tenha sua continuidade em diferentes linhas de pesquisa.

REFÊRENCIAS BIBLIOGRÁFICAS

ALECRIM, Emerson. **O que é Internet das Coisas (IoT)?.** 2022, *online.* Disponível em: https://www.infowester.com/iot.php. Acesso em: 22 de ago. 2022.

ALKUDMANI, Fares. **Inteligência Artificial e Blockchain podem se complementar?** 2020, *online*. Disponível em: https://portaldobitcoin.uol.com.br/inteligencia-artificial-e-blockchain-podem-se-complementar/. Acesso em: 25 de ago. 2022.

ALVES, Marcelo de Camilo Tavares. **Direito Digital.** Goiânia, 2009. 9-10 p. em http://aldeia3.computacao.net/greenstone/collect/trabalho/import/Direito%20Digital.pdf. Acesso em: 28 de abr. 2022.

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012.** Disponível em: https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/. Acesso em: 22 de jul. 2022.

BARROS, Antônio. **Conheça a evolução dos crimes cibernéticos.** 2006. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos. Acesso em: 15 de set. 2022.

BONANI, Rafael. **Termos de Uso o que são e para que servem.** 2020. Disponível em: https://www.bonani.adv.br/termos-de-uso-o-que-sao-e-para-que-servem. Acesso em: 15 de set. 2022.

BRASIL. **Constituição Federal.** Brasília: Planalto, 1988.

BRASIL. **Decreto-Lei 2.848, de 1940.** Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 de set. 2022.

BRASIL. **Estatuto da Criança e do Adolescente.** Lei nº 8069/90. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 15 de set. 2022.

BRASIL. Lei n. 12.737 – **Lei Carolina Dieckmann.** Brasília: Planalto, 2012.

BRASIL. Lei n. 12.965 – **Marco Civil da Internet**. Brasília: Planalto, 2014.

BRASIL. **Lei n° 11.829, de 2008.** Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm. Acesso em: 15 de set. 2022.

BRASIL. **Lei n° 12.015, de 2009.** Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12015.htm. Acesso em: 15 de set. 2022.

BRASIL. **Lei nº 12.737, de 2012.** Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 de set. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018.

BRASIL. **Lei nº 14.155, de 2021.** Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 15 de set. 2022.

BRASIL. **Meu Dicionário "criminalizar".** s.d. Disponível em: https://www.meudicionario.org/criminalizar. Acesso em 16 de set. 2022.

BRITO, Luíza. **Inteligência Artificial:** Qual a sua relação com o Bitcoin? 2021, *online*. Disponível em: https://coinext.com.br/blog/o-que-e-inteligencia-artifical. Acesso em: 15 de ago. 2022.

CABRAL JÚNIOR, Florêncio Ponte. **Prevendo o futuro das criptomoedas com inteligência artificial.** 2022, *online*. Disponível em: https://itforum.com.br/noticias/prevendo-o-futuro-das-criptomoedas-com-inteligencia-artificial/. Acesso em: 15 de ago. 2022.

CARNEIRO, Ramon Mariano. **"Li e aceito":** violações a direitos fundamentais nos termos de uso das plataformas digitais. 2020. Disponível em: https://revista.internetlab.org.br/li-e-aceitoviolacoes-a-direitos-fundamentais-nos-termos-de-uso-das-plataformas-digitais/. Acesso em 16 de set. 2022.

CARVALHO, Cristiane. **Internet das coisas**: entenda o que é e como funciona. 2021, *online.* Disponível em: https://www.tecmundo.com.br/internet/230884-internet-coisas-entenda-funciona.htm. Acesso em: 15 de ago. 2022.

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

CUNHA, Lilian. **Porque o Brasil é um dos principais alvos de ataques cibernéticos do mundo.** 2021. Disponível em: https://www.cnnbrasil.com.br/tecnologia/por-que-o-brasil-e-um-dos-principais-alvos-de-ataques-ciberneticos-do-mundo/. Acesso em: 17 de set. 2022.

FACHINI, Tiago.**Direito Digital:** o que é, importância e áreas de atuação. Boletim Jurídico, Uberaba/MG, a. 19, nº 1022. Disponível em https://www.boletimjuridico.com.br/artigos/direito-e-internet/10955/direito-digital-e-importancia-areas-atuacao. Acesso em: 17 abr. 2022.

FERRARI, Daniella. **Convenção de Budapeste e crimes cibernéticos no Brasil.** 2020. Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil. Acesso em: 17 de set. 2022.

FORTINET. **Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina.** 2022. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a. Acesso em: 17 de set. 2022.

GOGONI, Ronaldo. **Hacker compromete dados de cartões de crédito de 20 milhões de sul-coreanos.** Meiobit, 2014, *online*. Disponível em: https://meiobit.com/277267/coreia-do-sul-hacker-dados-cartao-credito-20-milhoes-consumidores-40-por-cento-populacao-pais-comprometidos/. Acesso em: 18 de jul. 2022.

GUERRIERI, Nathan. **Cibercrimes**: Sujeito Ativo. Jusbrasil, *online*. Disponível em: https://nguerrieri.jusbrasil.com.br/artigos/378597019/cibercrimes-sujeito-ativo. Acesso em: 15 de ago. 2022.

HARAN, Juan Manuel. **Malware dos anos 90:** os vírus Michelangelo e Melissa. 2018, *online*. Disponível em: https://www.welivesecurity.com/br/2018/11/12/malware-dos-anos-90-os-virus-michelangelo-e-melissa/. Acesso em: 18 de jul. 2022.

HIGA, Paulo. **2,9 milhões de clientes são afetados em ataque à rede da Adobe; hackers também acessaram código-fonte de aplicativos.** Tecnoblog, 2013, *online*. Disponível em: https://tecnoblog.net/arquivo/141978/ataque-adobe-codigo-fonte/. Acesso em: 19 de jul. 2022.

KIANE, Rayse. **Afinal, o que é IoT?.** 2019, *online*. Disponível em: https://via.ufsc.br/afinal-o-que-e-iot/. Acesso em: 19 de jul. 2022.

LAVAGNOLI, Silvia. **Como surgiu a Inteligência Artificial?** 2019, *online*. Disponível em: https://opencadd.com.br/como-surgiu-a-inteligencia-artificial/?utm_term=&utm_campaign=Ind%C3%BAstria+4.0&utm_source=adwords&utm_medium=ppc&hsa_acc=6954626335&hsa_cam=15553666063&hsa_grp=130968470319&hsa_ad=572474769000&hsa_src=g&hsa_tgt=dsa-. Acesso em: 19 de ago. 2022.

LEAL, Priscila de Oliveira Ribeiro. **A evolução do trabalho humano e o surgimento do Direito do Trabalho.** Revista Jus, 2014. Disponível em: https://jus.com.br/artigos/32198/a-evolucao-do-trabalho-humano-e-o-surgimento-do-direito-do-trabalho. Acesso em: 15 abr. 2022.

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

MOREIRA, Rômulo Diego. **O que é tethering?** Entenda a conexão entre celular e computador. 2022, *online*. Disponível em: https://www.techtudo.com.br/noticias/2022/07/o-que-e-tethering-entenda-a-conexao-entre-celular-e-computador.ghtml. Acesso em: 19 de ago. 2022.

NASCIMENTO, Anderson. **O que é cibercrime?** Canal Tech, 2014, *online.* Disponível em: https://canaltech.com.br/seguranca/O-que-e-cibercrime/. Acesso em: 18 jul. 2022.

NOVO, Benigno Núñez. **Direito Digital.** *Online,* 2019. Disponível em: https://jus.com.br/artigos/74019/direito-digital. Acesso em: 28 de abr. 2022.

PAIVA, Mário Antônio Lobato de. **Os institutos do direito informático.** Maio, 2002. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/30390-31543-1-PB.pdf. Acesso em: 28 de abr. 2022.

PEREIRA, Luiz Fernando. **Classificação das normas penais.** Jusbrasil. 2013. Disponível em: https://drluizfernandopereira.jusbrasil.com.br/artigos/111880022/classificacao-das-normas-penais. Acesso em: 15 de set. 2022.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na *Internet*.** Juruá Editora. Novembro, 2003. 1ª Edição.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais:** Comentários à Lei nº 13.709/2018 (LGPD). Saraiva; 1ª Edição. 2018.

PINHO, Larissa. **Direito Digital:** temas avançados. 2022. TJAM. Disponível em: https://www.tjam.jus.br/index.php/esmam-noticias/5400-atualizacao-para-magistrados-esmam-lanca-curso-direito-digital-temas-avancados. Acesso em 28 de abr. 2022.

POLIDO, Fabrício Bertini Pasquot. **LGPD e ANPD**: saiba o que são e entenda as diferenças entre a lei e o órgão. Jota, 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-anpd-saiba-o-que-sao-e-entenda-as-diferencas-entre-a-lei-e-o-orgao-13042022. Acesso em: 27 jun. 2022.

RUTHERFORD, Mikhail. **Crimes na internet:** falta de normatização, dificuldades na regulamentação e entendimentos sobre o assunto. Jusbrasil. 2015. Disponível em: https://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-internet-falta-de-normatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto. Acesso em: 15 de set. 2022.

SILVA, Kevin Rick Matias. **A dificuldade de aplicabilidade do direito digital à privacidade**: memória coletiva, liberdade de expressão e esquecimento. PUC, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1954/1/KEVIN%20RICK%20MATIAS%20SILVA%20-%20tcc.pdf. Acesso em: 20 mai. 2022.

SILVA, Marcelo Mesquita; BARRETO, Alesandro Gonçalves; KUFA, Karina. **Cibercrimes e seus reflexos no direito brasileiro.** 1ª ed. 2ºtir. Fev/2020 Salvador: Editora JusPODIVM. 2022.

TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. Revista dos Tribunais. 2ª Tiragem. 2019.

WAKEFIELD, Jane. **Entenda o ataque virtual à Sony.** BBC, 2014, *online*. Disponível em: https://www.bbc.com/portuguese/noticias/2014/_entenda_coreia_norte_lgb. Acesso em: 22 de jul. 2022.