CIBERCRIMES: DA PROTEÇÃO À INTIMIDADE AOS DESAFIOS NA RESPONSABILIZAÇÃO CRIMINAL

Fabrício Coelho de Campos[1]
Antônio Leonardo Amorim[2]

RESUMO

Essa pesquisa explora a problemática que envolve a prática dos crimes cibernéticos, em especial as dificuldades encontradas para a devida responsabilização daqueles que praticam os cibercrimes. Importa recordar que em conjunto com os avanços tecnológicos, há também um aumento na criminalidade que exige a atenção da coletividade como um todo. Face à falha jurídica, no que diz respeito aos delitos eletrônicos, mostra-se então a necessidade de verificar se tal falha, preenchida juridicamente por meio das analogias com os delitos já tipificados no código penal, como difamação e injúria, está a ser julgada de forma eficaz, cumprindo o seu propósito. Diante disso, tem-se o seguinte problema de pesquisa: quais os desafios encontrados na responsabilização nos casos de crimes cibernéticos? Para obter resposta a esse problema de pesquisa, se utilizará do método dedutivo, com realização de pesquisa bibliográfica e documental, buscando compreender as dificuldades apontadas pela literatura na responsabilidade de sujeitos autores de cibercrimes. No entanto, por meio de investigações e estudos de casos específicos, constatou-se o quão vulnerável é o sistema jurídico brasileiro na gestão do cibercrime, frequentemente com a impossibilidade de identificar o autor do delito e, por conseguinte, na sua responsabilização. Assim, é fundamental que os utilizadores da internet estejam atentos às orientações de segurança e evitem a divulgação de informações pessoais como forma de combater as infrações.

Palavras-chave: Cibercrimes; Crimes eletrônicos; Direito Digital; Dados pessoais.

INTRODUÇÃO

Devido à intensidade da globalização contemporânea, foi possível desenvolver a Internet e outros meios de comunicação, contribuindo para a modernização da sociedade. Embora haja uma chance de promover a integração da ciência na esfera social, há também a promoção de comportamentos criminosos que afetam a segurança social e estatal.

A internet foi fundada no século XX para organizar servidores e instrumentalizar formas de organização de documentos. O mundo dos computadores consiste em uma série de documentos que lançam navegadores como, por exemplo, Google Chrome, Mozilla Firefox, Internet, dentre outros. Graças a isso, existem inúmeras ferramentas disponíveis para

---

[1] Artigo apresentado ao Curso de Direito, da Universidade Federal de Mato Grosso do Sul - UFMS, campus de Corumbá, como exigência para a obtenção do título de Bacharel em Direito. Acadêmico do Curso de Direito Universidade Federal de Mato Grosso do Sul – UFMS, campus de Corumbá. E-mail: fabricio.coelho@ufms.br

[2] Professor do Curso de Direito da Fundação Universidade Federal de Mato Grosso do Sul - UFMS, Campus do Pantanal - CPAN, Cidade de Corumbá/MS, Doutor em Direito na Universidade Federal de Santa Catarina, bolsista CAPES (2022/2023), Mestre em Direito pela Universidade Federal de Mato Grosso do Sul (2017-2019), bolsista CAPES (2017-2018), Especialista em Direito Penal e Processo Penal (2017-2018), Coordenador do Projeto de Pesquisa Criminologia Crítica do Pantanal. E-mail: antonio.amorim@ufms.br. ORCID: https://orcid.org/0000-0003-1464-0319.

trabalhar, estudar e, também de entretenimento (redes sociais). Com o passar dos anos e com a expansão da internet e suas formas aumentou-se a quantidade de propagação de vírus (malware), sendo essa a principal ferramenta de ingresso em outros computadores e invasões de redes por hackers, para a realização de ataques cibernéticos.

O cibercrime pode ocorrer por mais de um comportamento malicioso ao mesmo tempo, além de estar em vários lugares simultaneamente, mantendo silêncio e discrição. Quanto mais a tecnologia integra o cotidiano das pessoas, o conhecimento dos elementos virtuais se torna a base central da expansão da modernidade.

Esta área tem ganhado grande importância na atualidade, sendo inclusive essencial para os cidadãos. Como resultado, milhares de empresas começaram a investir em criptografia, que seria uma forma de ocultar informações usando linguagem codificada. Os órgãos governamentais também estão adotando o formato digital e substituindo a forma convencional de desenvolvimento de suas atividades administrativas. Um exemplo marcante é o judiciário brasileiro, que passou a poder realizar audiências, atas e consultas por meio de plataforma digital, garantindo a segurança de todos os procedimentos e a participação à distância.

Diante do exposto, tem-se o seguinte problema de pesquisa: Quais os desafios encontrados na responsabilização nos casos de crimes cibernéticos? O objetivo geral deste trabalho é analisar as dificuldades encontradas na responsabilização de crimes cibernéticos, tendo como objetivo específico a descrição do que são dados pessoais, análise dos crimes digitais, bem como de inferir os desafios da responsabilidade dos cibercrimes.

Essa pesquisa se utilizará do método dedutivo, com realização de pesquisa bibliográfica e documental, buscando compreender as dificuldades apontadas pela literatura na responsabilidade de sujeitos autores de cibercrimes.

A justificativa para este trabalho, bem como, a sua importância para o âmbito acadêmico é de que a privacidade virtual ou da Internet é algo que se torna importante ao longo do tempo, e a informatização da cultura é algo que preocupa a sociedade. Ter informações pessoais no âmbito Web ou em redes sociais na Internet não é completamente seguro, pois são dados pessoais que podem ser usados por empresas de publicidade ou que podem ser alvos de crimes virtuais, em especial, no que tange a ofensa a sua honra e a dignidade.

Portanto, diante deste tema, serão abordados abaixo discussões sobre a prática de cibercrimes, desafios encontrados para responsabilização dos crimes cibernéticos, a importância da proteção contra crimes digitais em ênfase dos roubos de dados pessoais, e uma reflexão sobre como a moderna tecnologia afeta a segurança pessoal e estatal.

2 A PROTEÇÃO DOS DADOS PESSOAIS NA LEGISLAÇÃO BRASILEIRA

A privacidade como sendo espécie do Direito à Personalidade, descrito a partir do artigo 11 e seguintes do Código Civil, pode ser definida como o escopo da vida pessoal de um indivíduo que se desenvolve em um espaço reservado e deve ser mantido em sigilo. Privacidade é uma esfera da vida privada que tem o direito de se proteger contra qualquer interferência, sendo um aspecto íntimo e reservado de uma pessoa ou grupo, especialmente do ente despersonalizado intitulado família (Bioni, 2019).

É imperioso destacar que o direito à privacidade faz parte da Declaração Universal dos Direitos Humanos (art. 22). Isso significa que é um direito inerente a todo ser humano, independente de outros fatores (sexo, idade, nacionalidade e etnia), não podendo ser transferido ou renunciado, e, como o restante dos direitos humanos, o direito à privacidade busca garantir a dignidade do indivíduo (Lima, 2016).

Além da Declaração Universal dos Direitos Humanos, a privacidade é protegida pela Carta Magna brasileira de 1988 (art. 5º, X). A Constituição protege o endereço de cada indivíduo, suas comunicações, seus documentos particulares e sua imagem. O segredo da correspondência é um princípio de legislação contido em várias constituições (Bioni, 2019).

Observou-se que, com o avanço da Internet e da tecnologia, o país precisou modificar suas leis para proteger a privacidade nesta nova forma de comunicação, o que deu origem ao Marco Civil da Internet (Lei n° 12.965/2014). Neste liame, as redes sociais tornaram-se bancos de dados nos quais são coletadas informações pessoais e documentos sobre as atividades da vida real das pessoas que os usam.

Informações pessoais como estado civil, cidade de residência e sexo, religião, partido político, família, são comuns nesse ambiente virtual, e isto disponibiliza a todos, dados que há pouco tempo evitava-se fornecer tão facilmente.

A virada do milênio transformou os costumes da sociedade mundial no campo da tecnologia, com esse avanço, surgem novas tendências às quais precisam ser estudadas, regulamentadas, discutidas e analisadas.

No campo do Direito não é diferente, com essas novas tendências acerca da tecnologia, necessário se faz uma regulamentação jurídica do assunto, daí é que se depreende o surgimento do Direito Eletrônico ou Direito Digital. Paiva (2016, p. 4) explica que este novo ramo “constitui o conjunto de normas, aplicações, processos, relações jurídicas que surgem como consequência da aplicação e desenvolvimento da informática, isto é, a informática é geral deste ponto de vista e da forma como é regulado pelo direito”.

Sendo assim, o Direito Digital é uma ciência jurídica de autonomia relativa em relação aos outros ramos do Direito. Em que pese, essa ciência jurídica visa regular as relações das pessoas no ambiente virtual com a finalidade de controle e fiscalização dos mais diversos meios de comunicação, até mesmo da própria informática (Bioni, 2019).

Tratando da classificação do Direito Digital, a corrente majoritária que é cunhada por Frederico de Barros Carvalho, Anderson de Paiva Gabriel, Bruno Ricardo Bioni, Marco Aurélio Greco, Rodrigo Dias de Pinho Gomes dão a entender como de caráter privado, pois existem inúmeras situações que o classificam dessa forma, como por exemplo, os contratos eletrônicos, os contratos informáticos, os documentos eletrônicos.

Entretanto, esse âmbito privado se insere no setor público na mesma lógica do caráter privado. Podemos ressaltar então que, o direito digital é um direito multifacetado e com características próprias, pertencente tanto ao direito privado quanto ao público (Lima, 2016).

Como já visto, a evolução da informática e da cibernética conduziu e vem conduzindo inúmeros benefícios para a população mundial e, é de suma importância preservar direitos fundamentais inerentes à pessoa humana, como a liberdade e a privacidade, além de colocá-las a salvo de qualquer situação que possa ser encarada como criminosa. E nesse sentido o Direito Digital visa proporcionar a cada indivíduo total controle de suas informações pessoais (Bioni, 2019).

O direito fundamental à privacidade e à intimidade é evidentemente uns dos bens mais íntimos do ser humano, pois sem ela o ser humano acaba sofrendo violação no que tange a sua personalidade.

Posto isso, a CF de 1988 em seu Artigo 5° inciso X, postulou a respeito à inviolabilidade à intimidade, à honra, à imagem, e a vida privada, das pessoas, e garantiu em contrapartida a indenização por danos morais ou materiais caso algum desses direitos sejam violados, isso quando a conduta não seja considerada criminosa, que deverá ter repercussão própria no âmbito do Direito Penal.

Zanon (2013, p. 71) aponta que:

> [...] a privacidade tem um estatuto constitucional de inviolabilidade, como termo em que diferem também as garantias individuais fundamentais do direito à vida, à liberdade, à igualdade, à segurança e à propriedade. Nesse sentido, a CF proclama que perante a vida privada e a intimidade de cada um dos indivíduos existe um dever, que atinge a todos os sujeitos, de direitos, de abstenção de atos de intromissão indevida.

Os dados como bem jurídico se inserem pela iniciativa da nossa constituição no que tange à privacidade, à intimidade e a liberdade, pois esses princípios humanos são norteadores para o direito digital e são fundamentais para garantia do uso seguro da rede

mundial de computadores (Lima, 2016).

Toda pessoa natural ou jurídica tem direito à proteção de seus dados pessoais, segundo a Lei nº 13.709/2018, que é responsável pelo tratamento de dados pessoais dentro dos meios digitais. Podemos afirmar que aqui surge para o direito digital em caráter nacional a proteção dos dados pessoais.

Contextualizando as iniciais sobre as vertentes dos dados pessoais, Gomes (2017, p. 54) transcreve em sua obra "Big Data: Desafios à tutela da Pessoa Humana na Sociedade da Informação" que as novas tecnologias são responsáveis também por garantir uma espécie de anonimato para aqueles que praticam condutas online, explicando que:

> Diante das novas tecnologias, da chamada sociedade da informação, percebe-se que a privacidade deixou de se restringir unicamente à garantia do anonimato, do sigilo, do direito de ser deixado só, havendo uma verdadeira modificação do quadro geral do escopo de abrangência da privacidade, para se compreender também o controle dos dados pessoais. A privacidade passa então a ser vista em sua definição funcional de forma mais ampla e abrangente, como o direito conferido à pessoa de controle das informações pessoais que lhe dizem respeito.

Reconhece, neste momento, a necessidade da intervenção do Estado em garantir que se efetive mecanismos de proteção da privacidade por meio de legislação, buscando inclusive a regulamentação do uso da internet. Nesse liame, tem-se como fonte primordial a operação da autonomia individual e da liberdade para o desenvolvimento da dignidade humana e da sua proteção em âmbito criminal (Bioni, 2019).

Salienta-se, portanto, que assim como os direitos da personalidade, a privacidade é irrenunciável, entretanto o titular poderá sofrer limitação voluntária, se assim o permitir. Importante mencionar o Enunciado 4 da I Jornada de Direito Civil da Justiça Federal que assim dispõe, "o exercício dos direitos da personalidade pode sofrer limitações voluntárias, desde que não seja permanente nem geral".

Analisando a proteção de dados e informações do cidadão que é conferida pelo ordenamento jurídico, tem-se que o direito de informação é assegurado pela CF de 1988, no seu artigo 5º, XXXIII, que assim dispõe:

> Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

O inciso mencionado, foi inserido em decorrência da Lei n° 12.527/2011, também conhecida como Lei de Acesso à informação. Essa lei regulamenta o direito constitucional de acesso às informações públicas. Tal norma entrou em vigor em 16 de maio de 2012, criando mecanismos que possibilitam a qualquer pessoa física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades.

Tratando-se do assunto pertinente ao conhecimento de informações ou retificações de dados, a qual o estado é detentor da guarda insta salientar ainda, que a própria CF de 1988 novamente assegura o acesso à informação através do remédio constitucional Habeas Data previsto no mesmo artigo 5º, porém no inciso LXXII, (alíneas a e b) e visa garantir o acesso de uma pessoa (física ou jurídica) a informações sobre ela, que façam parte de arquivos ou bancos de dados de entidades governamentais ou públicas e assim dispõe:

> Conceder-se-á habeas data:
> A. Para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> B. Para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

A garantia do direito de auferir informações pessoais constantes de registros ou bancos de dados de entidades governamentais de natureza pública nunca se confunde com o direito de adquirir certidões (art. 5.º, XXXIV, "b", da CF/88), nem sequer com o direito de obter informações de interesse exclusivo, coletivo ou universal (art. 5.º, XXXIII, da CF/88).

A Lei 8.078/90 em seu artigo 43, dispõe que “o consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes” (Brasil, 1990).

O artigo 43 do Código de Defesa do Consumidor refere-se à questão do acesso por parte do consumidor aos seus dados pessoais que estão em proteção e zelo pelas empresas. Mostra-se, desta maneira, bem sucinta a proteção desses dados na relação de consumo. Porém, é importante que se frise a garantia de obter informações sobre o que está ocorrendo ou onde estão os dados pertinentes ao consumidor.

Analisando essas disposições normativas, é possível concluir que o ordenamento jurídico brasileiro tem um bom aprofundamento sobre os aspectos da tutela dos dados pessoais, visto que existem meios legais e judiciais para obter informações pertinentes aos dados pessoais tanto das pessoas jurídicas quanto das pessoas físicas, bem como as colocando a salvo de qualquer forma de violação dos direitos da personalidade (Bioni, 2019).

A proteção de dados é um bem jurídico que foi reconhecido pelos tribunais como algo que deve ser protegido pelo Estado. É também uma parte importante da lei de privacidade, que governa como os dados dos indivíduos podem ser coletados e usados. Existem muitas teorias filosóficas sobre proteção de dados, mas este artigo se concentra em duas noções pró-epistêmicas: primeiro, que a proteção de dados preservada por si mesma (em benefício do próprio conhecimento) e, segundo que constitui uma forma de autonomia

moral para os indivíduos (Lima, 2016).

A proteção de dados é vista como um bem jurídico que deve ser protegido a todo custo. É um conceito que protege os dados das pessoas e seu direito à privacidade. É importante entender o conceito de proteção de dados para entender como ela está protegendo o público (Bioni, 2019).

O conceito de proteção de dados é baseado na ideia de que as pessoas têm o direito de proteger seus dados. Os dados são de sua propriedade e eles têm o dever de mantê-los privados. O conceito de proteção de dados baseia-se na ideia de que as pessoas têm o direito de serem protegidas contra ameaças e acesso não autorizado aos seus dados. A proteção de dados é importante porque permite que os indivíduos se protejam de danos, além de ser uma forma de proteger os indivíduos do acesso não autorizado aos seus dados.

O sentido de privacidade no direito é baseado na ideia de que as pessoas têm o direito à privacidade, que significa que as pessoas têm o direito de estar livres de vigilância e intrusão. Privacidade na lei significa que as pessoas têm o direito de estar livres da interferência e intromissões do governo em suas informações pessoais. O direito à privacidade é importante porque permite que os indivíduos estejam livres de interferência em suas vidas pessoais. A privacidade na lei é importante porque permite que os indivíduos estejam livres de interferência em suas vidas pessoais (Lima, 2016).

Em continuidade a proteção de dados é um bem jurídico que deve ser protegido a todo custo. A ideia de privacidade no direito é baseada na concepção de que as pessoas têm o direito à privacidade. O direito à privacidade significa que as pessoas têm o direito de estar livres de vigilância e intrusão (Bioni, 2019).

2.1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A BUSCA POR SEGURANÇA NA INTERNET

A Lei nº 13.709, de 14 de agosto de 2018 possui por propósito garantir e salvar, no campo do tratamento de dados pessoais, a dignidade e os direitos essenciais do indivíduo, especialmente com relação à sua liberdade, igualdade e intimidades pessoal e familiar, nos termos do art. 5º, incisos X e XII da CF.

Ao tratar do tema pertinente da proteção dos dados pessoais, no sítio eletrônico do Senado Federal e nos dizeres de Guedes e Oliveira (Senado Federal, 2018), ambos da Agência do Senado Federal introduzem o tema da seguinte forma:

> No dia a dia, o brasileiro é solicitado a fornecer uma série de dados pessoais, que incluem até mesmo contracheques e extratos bancários, para verificação da sua

> capacidade de pagamento. Com o pé em práticas que já expunham a privacidade dos cidadãos no mundo analógico, o país chegou à era do chamado big data e da rastreabilidade agressiva sem uma lei que proteja os dados pessoais de seus habitantes Instados a se relacionar com um gigantesco sistema de armazenamento, classificação, transmissão e mesmo comercialização de dados, as chamadas pessoas naturais estão vulneráveis: seus hábitos, preferências de consumo, características étnicas, posições políticas, condições de saúde, orientação sexual, patrimônio, situação creditícia e muitos outros aspectos são observados, coletados e "tratados" para diversos usos, incluindo estratégias de venda e direcionamento de propaganda eleitoral.

O texto legal defende um maior controle dos cidadãos em relação a suas informações pessoais, necessitando de consentimento expresso para coleta e utilização dos dados, tanto pelo poder público quanto pela iniciativa privada e obriga o oferecimento de opções para o utilizador ver, retificar e apagar estes dados.

Em relação às hipóteses do tratamento de dados, é imprescindível o consentimento do titular. E, só poderão ser utilizados para a proteção do crédito, nos termos do código de Defesa do Consumidor para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento, para a tutela da saúde, com procedimento realizado por profissionais da área ou por entidades sanitárias; para a realização de estudos por órgão de pesquisa, sem a individualização da pessoa; para a proteção da vida ou da integridade física do titular ou terceiro; para pleitos em processos judicial, administrativo ou arbitral; para a execução de contrato ou procedimentos preliminares relacionados a um contrato; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas.

A abrangência da Lei visa quaisquer dados pessoais obtidos em qualquer tipo de suporte (papel, eletrônico, informático, som, imagem, etc.). Classificação dos Dados - LGPD (governo federal, 2021) descrevem ainda exemplos de dados pessoais e dados não pessoais:

> Exemplos de dados pessoais: Nome e apelido; Endereço de residência; Endereço eletrônico; Número de um cartão de identificação; Dados de localização (por exemplo, a função de dados de localização em um celular); Endereço IP (protocolo de internet); Testemunhos de conexão (cookies); identificador de publicidade do telefone; e Dados obtidos por um hospital ou médico que permitam identificar uma pessoa de forma inequívoca.
> Exemplos de dados considerados não pessoais: Número de registro de empresa; Endereço eletrônico de empresa; e Dados anônimos.

Mostrando um parâmetro geral sobre a Lei nº 13.709, pode-se observar que a lei traz preceitos e condições que visam a proteção dos dados pessoais em uma vasta gama, condizente ainda para a coleta e tratamento desses dados diante dos órgãos defendidos pelo presente estudo.

3 NOÇÕES GERAIS SOBRE CIBERCRIMES

Durante o século XIX, as informações e mensagens eram enviadas por meio de carruagens, barcos e navios. Com o meio técnico-científico-informacional, as relações sociais começaram a sofrer alterações visto que é um meio onde pode ser encontrado: tecnologia, ciência e informação. Essas descobertas tiveram grande importância, pois influenciam com inovações os meios de comunicação (Adas, 2002, p. 44).

O desenvolvimento de um país é indissociável do progresso da ciência e da tecnologia. Durante as décadas de 1980 e 1990 o Brasil experimentou uma abertura positiva devido à influência do processo de globalização, a necessidade de uma nova estrutura adequada para o desenvolvimento de uma Nação Tecnológica (Cunha, 2009).

É claro que a integração da tecnologia tem contribuído para a transformação social, conhecendo o ambiente virtual, além do espaço físico para o qual se contribuiu a evolução das tecnologias existentes como o telefone e o surgimento de computadores mais poderosos. Com a expansão e reorganização do capitalismo após 1980, a sociedade caminhava para uma grande transformação influenciada pela globalização e industrialização intensificada. Em meio às mudanças e evolução que se seguiram à integração da rede e suas conexões, o que foi as formas mais importantes de comunicar e divulgar dados e ideias. A sociedade tornou-se mais compreendida ou representada em termos de influência na internet e nos relacionamentos interpessoais (Adas, 2002).

Como muitas empresas começaram a investir em tecnologia, houve um aumento no fornecimento de dados e informações do usuário a partir daí foram arquivados e fáceis de rastrear usando algoritmos. Portanto, em meados da década de 1980 com mudanças nas esferas sociais e econômicas, houve um aumento das atividades criminosas que começaram a se refletir nas manipulações de caixas de banco, pirataria de software e pornografia infantil, telecomunicações e outros abusos fatores que começaram a preocupar os cidadãos (Cunha, 2009).

Como resultado, o judiciário brasileiro, diante dessa evolução, teve que por diversas mudanças que se seguiram à Constituição Federal de 1988. Porém, com o constante surgimento de novos crimes na nova realidade, eles engajaram empresas para investir na segurança dos internautas como novas classificações de crimes no Código Penal Brasileiro, garantindo proteção aos usuários.

Com o advento da Lei nº 12.965 de 2014 (Marco Civil da Internet), possibilitou-se a regulação da utilização dos meios eletrônicos, e, dessa forma, aquele que usufrui deste veículo deverá respeitar garantias, princípios, e passa a ter seus direitos respeitados. Pode-se

também ser processado penalmente quando do seu mau uso, o que inclui a lesividade para com outrem, realizando ações contrárias ao ordenamento jurídico. Entretanto, o país ainda não está desenvolvido ao ponto de possuir delegacias virtuais nos municípios de algumas regiões do país.

No Brasil, os crimes de exposição de internet ou virtuais foram alterados pela Lei Carolina Dieckmann e tipifica-se na Lei nº 12.737/2012, pelo caso envolvendo a atriz com suas fotos íntimas vazadas de seu computador e a época causou muita controvérsia.

Alguns pensam que a internet é um vasto meio de prática de crimes que não gera responsabilidade alguma, mas essa realidade vem mudando com o passar dos anos e o desenvolvimento dessa área criminal em todo o mundo. Antes mesmo da legislação brasileira criar uma lei específica, os tribunais já criavam jurisprudências relacionadas a isso com base no Código Penal (Cunha, 2009).

Dentre os crimes cometidos no ciberespaço podemos citar alguns como lesão corporal (Art. 129 do Código Penal), injúria (Art. 140 do Código Penal), constrangimento ilegal (Art.146 do Código Penal), ameaça (Art. 147 do Código Penal) extorsão (Art. 158 do Código Penal) e estupro (Art. 213 do Código Penal).

Podemos configurar a "pornografia de vingança" em cada um desses crimes através de uma analogia baseada em seus textos puramente ditos. Lesão corporal consiste em ofender a integridade corporal ou a saúde de outrem, que por meio da pornografia de vingança pode comprometer a saúde psicológica, que acaba afetando também a física. A lesão advinda da pornografia de vingança pode ser leve, grave ou gravíssima, conforme sejam os traumas sofridos (Cunha, 2009).

Para Cunha (2009, p. 46-47) a norma do art. 129 do Código Penal, trata da "incolumidade pessoal do indivíduo, protegendo-o a saúde corporal, fisiológica e mental (atividade intelectual, volitiva e sentimental)". Sendo assim, qualquer conduta capaz de afetar alguma das três dimensões é passível de ser enquadrada como lesão corporal.

Injúria consiste em injuriar alguém lhe ofendendo a dignidade ou o decoro, no caso específico o agressor utiliza da exposição do material criminoso com o intuito de menosprezar sua imagem, manchando o conceito que tem de si.

Para Capez (2011, p. 305) "o bem protegido por essa norma penal é a honra subjetiva, que é constituída pelo sentimento próprio de cada pessoa acerca de seus atributos morais (chamados de honra-dignidade), intelectuais e físicos (chamados de honra-decoro)". Constrangimento ilegal consiste em constranger alguém, mediante violência ou grave ameaça, ou depois de lhe haver reduzido, por qualquer outro meio, a capacidade de resistência, a não fazer o que a lei permite, ou fazer o que ela não manda. Por meio do

material criminoso obriga a pessoa a cometer crimes em seu lugar ou exigir que não os abandone (Capez, 2011).

A ameaça consiste em ameaçar alguém, por palavra, escrita ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave. Na posse do material criminoso ameaça divulgá-lo em redes sociais, causando na vítima insegurança quanto a sua privacidade e honra (Capez, 2011).

Extorsão consiste em constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer tolerar que se faça ou deixar de fazer alguma coisa. Esse acaba sendo o pior deles, pois além de todo o pavor causado o criminoso exige dinheiro ou vantagem econômica para não divulgar o material, deixando muitas vezes a vítima nas mãos do mesmo por tempo indeterminado, pedindo assim quantias cada vez mais altas de dinheiro ou bens (Capez, 2011).

Estupro consiste em constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso. Trazendo para o nosso tema, é aqui que se encaixa o termo "estupro virtual", pois a vítima pode ser obrigada a manter relações físicas ou "virtuais" e/ou juntamente com atos libidinosos (Capez, 2011).

4 AS DIFICULDADES NA INVESTIGAÇÃO PARA OBTER OS INDÍCIOS DA AUTORIA NOS CRIMES VIRTUAIS

A internet revolucionou a forma como as pessoas se comunicam e compartilham informações. No entanto, seu uso também abriu novas maneiras para os criminosos cometerem crimes anonimamente e sem detecção pelo Estado. Um dos desafios mais difíceis que os pesquisadores enfrentam na investigação de crimes online é determinar quem cometeu um determinado crime. Isso ocorre porque muitos cibercriminosos adotam métodos sofisticados para ocultar suas identidades e rastros das agências de aplicação da lei. Para superar esse obstáculo, os investigadores desenvolveram várias técnicas que os ajudam a rastrear suspeitos online (Andrade et al., 2017).

Muitas vezes é difícil determinar quem é o responsável por crimes cometidos na internet. Isso ocorre porque o perpetrador muitas vezes pode permanecer anônimo, e a internet permite um nível de anonimato que geralmente não é possível no mundo físico. Além disso, a internet não possui as mesmas medidas de responsabilidade que existem no mundo físico. Isso significa que muitas vezes não há tanta evidência confiável disponível ao investigar crimes cometidos online (Carneiro, 2012).

Para identificar o autor de um crime, os investigadores muitas vezes precisam coletar evidências. Essa evidência pode ser qualquer coisa, desde depoimentos de testemunhas oculares até capturas de tela de conversas online. Muitas vezes, no entanto, é difícil reunir essas evidências, e muitas vezes é difícil encontrar pessoas dispostas a falar sobre crimes cometidos online. Além disso, os crimes na Internet geralmente ocorrem por longos períodos, o que pode dificultar o rastreamento dos perpetradores (Andrade et al., 2017).

Também existem limitações associadas à realização de investigações na Internet. Por exemplo, as investigações podem ser lentas e difíceis de avançar quando os resultados não parecem apontar na direção desejada. Além disso, pode ser difícil provar que um crime realmente ocorreu, porque os crimes online geralmente ocorrem sem um elemento físico (Cavalcante, 2018).

No entanto, mesmo após estabelecer inúmeras regras para limitar atividades maliciosas no mundo virtual, existem algumas lacunas que ainda precisam ser preenchidas pelo legislador, pois em um mundo onde ferramentas imensuráveis e infinitas podem ser obtidas, é importante que essa ordem seja mantido pode lidar com situações em que, por exemplo, o assunto pode desaparecer no ciberespaço, porque então seria muito fácil para o usuário criar uma conta falsa e depois caluniar a imagem da pessoa e, finalmente, repercutir e excluir a conta (Andrade et al., 2017).

No entanto, os avanços tecnológicos dificultam o combate a crimes que se adaptam constantemente às novas tecnologias. Assim, com o uso ilimitado e massivo da Internet, algumas pessoas com conhecimentos de informática começaram a se aperfeiçoar e usar seus conhecimentos para roubar informações criptografadas como faziam há muito tempo, para obter lucro econômico ou até mesmo para seu próprio bem nos jogos (Cavalcante, 2018).

Em alguns casos, ainda é possível identificar o responsável, mas ainda seria necessário apresentar todo o processo para comprovar essa atividade. Primeiro estabeleça a existência da verdade; e a evidência está nos meios pelos quais ela tenta estabelecê-la e mostrar a verdade, o que é dito. Presume-se também que a prova é: ordinária, elementos apresentados pelas partes ou pelo próprio juiz para apurar a existência de determinados fatos neste processo, com a ferramenta de verificação de tema probandum (Andrade et al., 2017).

No Brasil, a Comissão Parlamentar de Inquérito (CPI) de Crimes Cibernéticos em 2015 destacou a grande dificuldade em rastrear, identificar e punir crimes online. A dificuldade decorre do fato de que a velocidade de obtenção de informações das empresas não é a velocidade da Internet. O chefe de Repressão aos Crimes Cibernéticos da PF, Elmer Vicente, explicou que a investigação começa com a identificação do endereço IP em que começou o crime denunciado pela prestadora de serviço. O próximo passo é obter um nome

de usuário IP do seu ISP. De acordo com Elmer, no entanto, existem duas dificuldades principais. Isto primeiramente, curiosamente, algumas empresas não aceitam seu pedido de informações policiais na Internet. Outra dificuldade é que, antes de algumas empresas receberem as informações solicitadas pela polícia na internet civil, as empresas geralmente só divulgam os dados por meios legais (Agência Câmara de Notícias, 2015).

Recorda-se que nem todos os cibercriminosos são especializados ou conhecedores da área de informática. Alguns desses crimes, como pedofilia e crimes contra a honra, podem ser cometidos por usuários comuns que possuem apenas um celular ou qualquer dispositivo tecnológico com acesso à Internet. No entanto, tais situações podem ser mais fáceis de identificar. Assim como as pessoas possuem números de identificação como CPF (Cadastro de Pessoas Físicas), computadores e periféricos conectados à Internet também são um número diferenciado por um endereço IP, um protocolo único que permite que máquinas acessem a rede (Carneiro, 2012).

Além disso, é imprescindível que o público em geral realize uma busca criteriosa na web para conscientizar o usuário sobre a possibilidade de crimes e abusos, o que é uma forma de evitá-los e, ao mesmo tempo, poder combater tais crimes. Como, ao mesmo tempo, o Estado também deve tentar prevenir esses criminosos, treinar seus agentes para que o responsável seja encontrado e a ordem social seja restabelecida (andrade et al., 2017).

Em continuidade, vale ressaltar sobre desafios encontrados em crimes cibernéticos e suas responsabilidades temos que enfatizar que a ineficiência Estatal, onde, destaca uma grande dificuldade do Estado em investigar e processar delitos virtuais, pois há falta de recursos e pessoas com conhecimento especializado.

Logo, também, encontramos desafios na investigação policial, pois ressalta a necessidade de servidores capacitados e equipados com adequados equipamentos tecnológicos para o sucesso das investigações criminais.

Vale destacar também, a importância da colaboração das empresas, pois ressalta a cooperação de empresas, de redes sociais, internet, com o judiciário com o intuito de melhorar as investigações de forma mais rápida, lembrando ainda que temos ainda a falta de legislação específica.

Portanto, destacamos os desafios do judiciário em discutir complicados crimes, pois existe uma ausência de tipificação adequada dos crimes virtuais e a aplicação de analogias legais insuficientes. Nesse parâmetro vislumbramos uma legislação mais robusta e de políticas públicas que conscientizem sobre o uso ético da internet.

4.1 A LIBERDADE DE EXPRESSÃO NA INTERNET E O CONFLITO COM O CIBERCRIME

Atualmente um dos elementos mais fundamentais da sociedade e do governo é a liberdade de expressão, constituindo um estado democrático, englobando manifestações políticas, ideológicas, religiosas e artísticas. E na esfera digital, para garantir que essa lei não seja violada, norteada por princípios como o art. 13, da Convenção Americana de Direitos Humanos:

> Artigo 13 - Liberdade de pensamento e de expressão 1. Toda pessoa tem o direito à liberdade de pensamento e de expressão. Esse direito inclui a liberdade de procurar, receber e difundir informações e idéias de qualquer natureza, sem considerações de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer meio de sua escolha. 2. O exercício do direito previsto no inciso precedente não pode estar sujeito à censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente previstas em lei e que se façam necessárias para assegurar: a) o respeito dos direitos e da reputação das demais pessoas; b) a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas. 3. Não se pode restringir o direito de expressão por vias e meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de frequências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de idéias e opiniões. 4. A lei pode submeter os espetáculos públicos à censura prévia, com o objetivo exclusivo de regular o acesso a eles, para proteção moral da infância e da adolescência, sem prejuízo do disposto no inciso 2. 5. A lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitamento à discriminação, à hostilidade, ao crime ou à violência (BRASIL, 1992, s. p.).

Esses direitos também incluem os princípios de não discriminação e privacidade, onde o acesso universal garante conectividade justa, cabe a se escolher as medidas adequadas para garantir que esses princípios sejam implementados e para garantir que as empresas privadas não imponham barreiras desproporcionais à internet. O pluralismo é tratado com uma variedade e multiplicidade de vozes, o que favorece a deliberação da opinião pública a fim de manter um processo democrático que permita a disseminação de todo tipo de ideologia amparada pelo art. 13, da Convenção Americana de Direitos Humanos.

A CF trata da liberdade de expressão na internet, de acordo com o artigo 220[3]. A liberdade de expressão é importante desde que não entre em conflito com a Constituição Federal. Vale ressaltar, no entanto, que o anonimato é proibido porque, mesmo com

[3] Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição. § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV. § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

pseudônimo, é importante que o autor seja identificado para não violar o direito à veneração, à imagem, à privacidade etc.

Ayres Brito, ADPF 130, aponta que:

> Silenciando a Constituição quanto ao regime da internet (rede mundial de computadores), não há como se lhe recusar a qualificação de território virtual livremente veiculador de ideias e opiniões, debates, notícias e tudo o mais que signifique plenitude de comunicação. 4. Mecanismo constitucional de calibração de princípios. O art. 220 é de instantânea observância quanto ao desfrute das liberdades de pensamento, criação, expressão e informação que, de alguma forma, se veiculem pelos órgãos de comunicação social.

Em outros casos, podem surgir conflitos entre a liberdade de expressão e interesses pessoais, pois por um lado temos o direito de expressar nossos pensamentos, informações, proibição de censura, e por outro está consagrado no art. 5º inciso X da Constituição Federal, inviolabilidade da vida privada, intimidade, honra e imagem humana.

Nesse sentido, a divulgação de fatos sobre qualquer tema ou evento pode prejudicar terceiros, e a necessidade de bloqueio de tal conteúdo deve ser analisada caso a caso.

Em suma, é importante analisar cada caso específico diante de um conflito entre direitos fundamentais. Vale ressaltar que ainda há uma grande necessidade de evolução do direito diante de um mundo virtual com infinitas ferramentas que podem levar a uma revolução social, mas ao mesmo tempo uma sociedade incerta. Portanto, é importante que os usuários conheçam as restrições e regras de uso que previnem a criminalidade e garantem a harmonia da vida no ciberespaço.

CONSIDERAÇÕES FINAIS

É claro que os avanços tecnológicos influenciam diretamente no comportamento social, pois a Internet possui recursos infinitos. Mas ao mesmo tempo abre inúmeras brechas para ataques cibernéticos, ameaçando a segurança digital. Esses atos podem incluir crimes de difamação, divulgação de dados, crimes contra a honra, calúnia, intimidação e outros crimes. Infelizmente, essas violações são cada vez mais frequentes e muitas vezes isso pode ser devido à falta de cuidado e conhecimento por parte do usuário.

As facilidades de acesso à Internet, aliadas à acessibilidade de computadores e smartphones, têm levado a um aumento contínuo da ocorrência de crimes cibernéticos.

O Brasil está cada vez mais entre os 10 (dez) países que mais usam a Internet, mas ainda assim não possui um sistema jurídico que abranja todas as condutas puníveis, o que faz com que o usuário brasileiro não esteja nem perto de estar devidamente protegido, segundo o site do governo federal em 26 de abril de 2021 publicado pelo ministério das comunicações.

Nesse sentido, além da falta de habilidades de muitos internautas em relação aos perigos cibernéticos, os cibercriminosos também se beneficiam do uso inevitável da Internet no dia a dia dos brasileiros.

O Código Penal brasileiro tipifica diversas ações no ambiente de rede, mas suas penalidades são relativamente leves e insuficientes para deter a implementação dessas ações. A Lei Carolina Dieckmann (Lei nº 12.737 / 2012), que altera o Código Penal e insere dispositivos em seu corpo principal. Porém, trouxe interpretações dúbias e penas leves para os criminosos. Portanto, a falta de legislação específica contra o crime cibernético exacerbou a ideia de que a Internet é uma terra sem lei.

Embora o Código Penal Brasileiro tipifique alguns comportamentos que ocorrem em um ambiente cibernético, as penas estabelecidas são um pouco mais leves e insuficientes para combater a recorrência e novas práticas. Portanto, é importante enfatizar que regras específicas devem ser formuladas para lidar com crimes que ocorrem em ambientes virtuais, pois esses comportamentos ocorrem cada vez com mais frequência, e as lesões sofridas pelas vítimas são muito graves tanto física quanto psicologicamente.

Portanto, em sentido educacional e de conscientização é necessário uma ação social para os cidadãos de uso das redes sociais e outros, sobre cibersegurança para prevenir os usuários de sofrerem golpes, ou mesmo para denunciar os crimes cometidos por usuários que infringem as regras e restrições dos espaços das redes sociais ou qualquer outro espaço cibernético, consequentemente tendo uma robusta legislação e, como também, políticas públicas eficazes para que não haja abusos de privacidade, disseminação de desinformação e até mesmo em violações dos direitos humanos.

Por fim, é essencial que os usuários online promovam a transparência e a conscientização sobre os riscos e responsabilidades associados ao uso da Internet. Isso inclui desde a proteção de dados pessoais até o combate ao discurso de ódio e à radicalização online. Somente com medidas concretas e colaboração entre governos, empresas e sociedade civil podemos garantir que a Internet continue sendo uma ferramenta para o progresso e a inclusão, em vez de um campo minado de ameaças e abusos.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil (1988). **Diário Oficial [da] República Federativa do Brasil,** Brasília, DF, 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/. Acesso em: 10 fev. 2020a.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 10 jan. 2002. Disponível em: http://www.planalto.gov.br/. Acesso em: 10 fev. 2020b.

AGÊNCIA DE NOTICIAS - CÂMARA DOS DEPUTADOS. **CPI constata dificuldade em rastrear e punir crimes de internet.** 2015 (Online). Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/22952/1/TCC%20Crimes%20Cibern%C3%A9ticos%20Alicia%20e%20Thuanny.pdf. Acesso em 22 de jun. 2022.

ANDRADE, Mariah Dourado de.; BENTES, Dorinethe dos Santos; GUIMARÃES, David Franklin da Silva. Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais. **Revista Vertentes Do Direito** (2), 191-205. https://doi.org/10.20873/uft.2359-0106.2017.v4n2.p191-205. Acesso em 22 de jun. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Ed. Forense Ltda., 2019.

BRASIL. **Lei nº 13.709, de 14 De agosto de 2018.** Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 18 de jun. 2022.

BRASIL, Lei nº 12.965 de 2014. **Marco Civil da Internet.** Brasília: Senado, 2014. Disponível

em:
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 18 de jun. 2022.

BRASIL, Nações Unidas. **Artigo 12:** Direito à privacidade. Brasil, 2018. Disponível em: https://nacoesunidas.org/artigo-12-direito-a-privacidade/. Acesso em: 18 de jun. 2022.

BRASIL. **Lei n.º 12.737 de 30 de novembro de 2012**, que traz a tipificação criminal de delitos informáticos. Disponível em:
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 18 de jun. 2022.

BRASIL. **Lei n° 12.527, de 18 de novembro de 2011.** Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm Acesso em 19 de jun. 2022.

BRASIL. **Lei n° 9.507, de 12 de novembro de 1997.** Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm Acesso em 19 de jun. 2022.

BRASIL. **Decreto no 678, de 6 de novembro de 1992:** Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em 25 de jun. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 10 de jun. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado, 1998.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**, Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado/. Acesso em 10 de jun. 2022.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico**, Rio Grande, XV, n.99, abr. 2012. Disponível em: http://www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_. Acesso em 10 de jun. 2022.

CAPEZ, Fernando. **Curso de Direito Penal** - Parte Especial. 11. Ed. São Paulo: Saraiva, 2011.

CAVALCANTE, W. F. **Crimes cibernéticos:** noções básicas de investigação e ameaças na internet. 2018 (Online). Disponível em: https://egov.ufsc.br/portal/conteudo/crimes-cibern%C3%A9ticos-no%C3%A7%C3%B5es-b%C3%A1sicas-de-investiga%C3%A7%C3%A3o-e-amea%C3%A7-na-internet. Acesso em 15 de jun. 2022.

CUNHA, Rogério S. **Direito Penal** – Parte Especial. 2.ed. ver. atual. e ampli. São Paulo: Editora Revista dos Tribunais, 2009,

GOMES, Rodrigo. **Big Data:** desafios à tutela da pessoa humana na sociedade da informação. Rio de Janeiro, 2017.P.61.

LIMA, Glaydson Farias de. **Manual de Direito Digital:** Fundamentos, legislação e jurisprudência. São Paulo: Appris, 2016.

OLIVEIRA, J. E. **Acórdão N. 911432, 20150020218878AGI.** 4ª Turma Cível, Data de Julgamento: 25/11/2015, publicado no DJE: 15/12/2015. Pág.: 193. Disponível em: https://bityli.com/EKCCLx. Acesso em: 29 de jun. 2022.

PAIVA, Mário Antônio Lobato de. **Os institutos do Direito Informático.** São Paulo, Âmbito jurídico. 2016. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5487. Acesso em: 19 de jun. 2022.

SENADO FEDERAL. **Projeto de lei geral de proteção de dados pessoais é aprovado no Senado.** Disponível em https://www12.senado.leg.br/noticias/materias/2018/07/10/projeto-de-lei-geral-de-protecao-de-dados-pessoais-e-aprovado-no-senado Acesso em 24 de jun. 2022.

SUPREMO TRIBUNAL FEDERAL – **Tribunal Pleno/ ADPF 130/** Relator: Ministro Carlos Britto/ Julgado em 30.04.2009/ Publicado no DJe em 05.11.2009, p. 2.381.

ZANON, João Carlos. Direito à Proteção dos Dados Pessoais. São Paulo: **Revista dos Tribunais**, 2013.

GOVERNO FEDERAL - **Guia De Boas Práticas - Lei Geral De Proteção De Dados (LGPD)**: Comitê Central de Governança de Dados - Agosto/2020 - Tratamento dos Dados Pessoais. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf

Governo Federal - **Classificação dos Dados – LGPD** - Disponível em: https://www.gov.br/mds/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados

https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/04/brasil-esta-entre-os-cinco-paises-do-mundo-que-mais-usam-internet Acesso em 13 de Jun. 2024.