ANÁLISE CRÍTICA-EVOLUTIVA DOS CIBERCRIMES PERANTE A LEGISLAÇÃO BRASILEIRA

CRITICAL-EVOLUTIONARY ANALYSIS OF CYBERCRIMES UNDER BRAZILIAN LEGISLATION

Marina Della Torre Canheu
http://lattes.cnpq.br/3623864172723312
Lavínia de Carvalho Reis

RESUMO

O presente artigo tem o intuito de construir de modo crítico a relação estabelecida pelo ordenamento jurídico brasileiro acerca de crimes cibernéticos, as falhas em sua composição e a maneira a qual busca tratar a penalização de cibercriminosos, ferindo, especialmente, o princípio da legalidade, protegido pela Constituição Federal e pelo Código Penal. Além disso, serão designados alguns pensamentos quanto a crimes existentes no meio tecnológico, maiores esclarecimentos quanto ao metaverso, e condutas que devem ser previstos e supervisionados por instituto responsável, gerando, assim, regras, uma porção legislativa que busque solucionar a problemática dos cibercrimes sem deixar lacunas tão expressivas na lei, e que principalmente, acompanhe o desenvolvimento absurdo e veloz da tecnologia.

Palavras-chave: Cibercrime, Princípio da Legalidade, Tipicidade, Internet, Metaverso.

ABSTRACT

This article aims to critically construct the relationship established by the Brazilian legal system regarding cybercrimes, the flaws in its composition and the way in which it seeks to treat the penalization of cybercriminals, particularly violating the principle of legality, protected by the Federal Constitution and the Penal Code. In addition, some thoughts will be given regarding existing crimes in the technological environment, further clarifications regarding the metaverse, and conduct that must be foreseen and supervised by a responsible institute, thus generating rules, a legislative portion that seeks to solve the problem of cybercrimes without leave such significant gaps in the law, and that mainly follows the absurd and rapid development of technology.

Keywords: Cybercrime, Principle of legality, Typicality, Internet, Metaverse.

INTRODUÇÃO

Comecemos porquanto à ideia de que o ser humano traz consigo uma necessidade incessante pela comunicação, independente do meio, como forma de evoluir, quebrar fronteiras, desenvolver conhecimento e democratizá-lo, o que o torna acessível ao mundo, que cada vez mais, e com mais rapidez têm se transformado em um mundo tecnológico.

A partir da década de 1980, a tecnologia informática evoluiu de modo drástico, com muita rapidez, criando uma revolução em nossa sociedade, implementando novidades inimagináveis, tanto no ambiente de trabalho, quanto no lazer e nas relações humanas, o que, nos dias de hoje, passou a ser essencial, ou até mesmo, possa-se dizer, uma necessidade na vida em sociedade.

Desse modo, é imprescindível pensar que essa nova modalidade de vida em sociedade provoque e exija alterações e novos conceitos da ordem jurídica, reguladora do nosso inter-relacionamento. Partindo desse ponto, é preocupante a questão da segurança que esse meio digital oferece, até que ponto essa aldeia global é segura, numa rede que facilita acesso à dados privados, e facilita a prospecção de crimes contra a honra, difamação, calúnia, entre muitos outros crimes que serão tratados neste artigo.

Assim, o artigo a seguir, tem o intuito de contribuir para a discussão acerca do cibercrime, relacionando-o a críticas quanto ao posicionamento do Ordenamento Jurídico Brasileiro e o ferimento de um dos maiores princípios carregados pelo Código Penal, se não o maior, o Princípio da Legalidade.

Havendo tal discussão será possível compreender quais os riscos que a utilização Internet traz consigo, como a sociedade deve lidar, e compreender que o mundo virtual não é uma terra sem lei, embora a legislação neste âmbito seja carregada de falhas.

CIBERCRIMES

Para que o presente estudo seja iniciado, é imprescindível citar DAOUN e BLUM[1](2000, p. 118), no que diz “o cidadão do mundo virtual, é antes de tudo, um cidadão do mundo real e da

[1] BLUM, R. M. S. O; DAOUN, A. J. Cybercrimes. Artigo em Direito & internet: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

mesma forma deve ser encarado como um agente criminoso". Essa perspectiva torna possível entender que aquilo que acontece no mundo virtual tem o poder de atingir o mundo real, portanto, uma atitude ilícita é passível de sofrer com condutas previstas e vigentes no ordenamento jurídico.

A priori, faz-se necessário, também, conceituar cibercrime, que nada mais é do que, conduta típica e ilícita, que constitua crime, com o uso da internet, ambiente de rede, aplicativos de relacionamento, redes sociais, entre outros, como meio para a prática delituosa.
Tal conceito foi definido por ROSSINI (2004, p.110)[2], como:

> [...] conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Dessa forma, com o tamanho avanço da tecnologia e do acesso aos meios cibernéticos pela população brasileira, destaco os dados apresentados pela pesquisa TIC Domicílios 2023, do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, sinalizando que, no Brasil, 84% da população brasileira com 10 anos ou mais se conectou à Internet, o que representa 156 milhões de pessoas.

O dado apresentado acima colabora com a ideia de que o elevado número de usuários navegando pela internet contribui para o aumento exponencial da incidência de crimes cometidos, utilizando como meio a internet.

Uma vez em que se constrói a ideia de que o direito existe para regular as relações humanas, e o momento ao qual a internet passou a fazer parte dessas relações, mesmo que de modo indireto, torna-se imprescindível que seja feita uma modificação da legislação acerca desse tema, para assegurar o uso correto do meio e a segurança dos usuários.

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

A LEGISLAÇÃO BRASILEIRA SOBRE CIBERCRIMES

Faz-se necessário conhecer e compreender quais leis foram criadas e implementadas ao ordenamento jurídico quanto aos cibercrimes, podendo, dessa forma, debater os impactos das mesmas, quais melhorias forneceram à segurança dos usuários e, ainda, quais as lacunas existentes e falhas.

A Lei dos Crimes Cibernéticos, Lei 12.737/12, conhecida como "Lei Carolina Dieckmann", popularmente, a elaboração dessa lei se deu de maneira extremamente rápida, no intuito de suprir as necessidades visadas no momento em que a atriz global, Carolina Dieckmann, teve fotos íntimas divulgadas na internet após se recusar a pagar uma quantia determinada pelo hacker responsável pelos compartilhamentos, em forma de ameaça. Entretanto, é importante destacar que as reivindicações de uma base legal para crimes digitais se originam do sistema financeiro, frequentemente vítima de ataques, golpes e roubo de dados.

Essa lei tipifica criminalmente, pela primeira vez em todo o ordenamento, os crimes digitais, como: invasão de computadores e outros dispositivos eletrônicos, violação de dados de usuários e interrupção de sites, governamentais e outros.

Dessa forma, a lei Carolina Dieckmann promoveu alterações no Código Penal de 1940, tais alterações estão localizadas nos artigos 154-A[3] e 154-B[4], 266[5] e 298[6], tendo como objetivo penalizar toda e qualquer conduta que sinalize invasão de dispositivo informático de outrem ou contra a administração pública e demais Poderes da União, todas sancionadas pela presidente da época, Dilma Rousseff.

[3] Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

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

[5] Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

§ 1 Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2 Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

[6] Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro.

Marco Civil da Internet[7], surge com o intuito de regular os direitos e deveres dos usuários da internet, tornando-se essencial para a segurança e proteção dos dados dos internautas, garantindo o acesso a informações e conteúdos privados de sites e redes sociais do usuário somente por meio de ordem judicial.

A Lei também caracteriza a possibilidade de retirar um conteúdo do ar, seja ele ofensivo, violento ou pornográfico, tendo, para esse último caso, uma excessão quanto à ocorrência de "pornografia de vingança", a qual pode ser retirada do ar por pedido direto da vítima ao site que hospeda o conteúdo.

O conteúdo da LGPD - Lei Geral de Proteção de Dados[8], responsável por regular a coleta e tratamento de dados pessoais, a lei também altera o artigo 7º[8] e 16º[9] do Marco Civil da Internet. Ademais, é interessante ressaltar a abordagem de PECK e LOTUFO (2021, p.171)[10], quanto à conceituação dos objetivos dessa nova legislação, ao dizer que:

> Pode-se afirmar que o objetivo dessa legislação pautada em princípios é o de nortear as ações que envolvam o tratamento de dados com base na proteção do titular de dados, a liberdade de expressão, de informática, de opinião/comunicação, a proteção da privacidade e do desenvolvimento tecnológico e econômico.

Desse modo, a Lei Geral de Proteção de Dados busca proteger a captação, armazenamento e compartilhamento de dados pessoais coletados por sites e empresas online, na tentativa de criar um ambiente digital seguro.

---

[7] Lei 12.965/2014.

[8] Lei 13.709/2018.

[8] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

[9] Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º ; ou
II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais.

[10] HACKEROTT, Nadia A. T. Aspectos jurídicos do E-commerce. 1.ed. São Paulo, 2021.

A Lei 14.155/21, texto responsável por alterar o Código Penal no que diz respeito à agravação da pena para crimes de violação de dispositivo informático, furto e estelionato cometidos em meio eletrônico ou pela internet.

Após a alteração, e agravação das penas, o crime de invasão de dispositivo, destruição de dados e instalação de vírus, com o intuito de obter vantagem ilícita, compreenderá punição de reclusão de 1 a 4 anos e multa, sendo passível de aumento de um a dois terços caso a invasão resulte em prejuízo financeiro ou econômico. Diferença significativa quanto à pena, já que a anterior previa detenção de três meses a um ano.

Já nos casos de obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais, industriais, informações sigilosas, ou controle remoto não autorizado do dispositivo invadido, a pena passa a ser de dois a cinco anos e multa, diferença também significativa comparada à passível anteriormente, que previa reclusão de seis meses a dois anos e multa.

Entretanto, mesmo com as modificações feitas na legislação para atender todas as necessidades que a sociedade passou a apresentar com os avanços tecnológicos, muito ainda precisa ser feito quanto a crimes que seguem sem tipificação nas leis vigentes, citadas acima, propostas para combater os cibercrimes, além de mudanças pertinentes à Lei dos Crimes Cibernéticos, para que esteja de acordo com os avanços tecnológicos tidos desde sua criação, e às nomenclaturas que passaram desatentamente erradas quanto ao sistema que se aplica e nomenclatura informática, por ter-se estabelecido de forma rápida e urgente.

Desse modo, não tipificar condutas delituosas no ordenamento jurídico-penal afeta o maior princípio do Código Penal, o Princípio da Legalidade, ou, também conhecido como Reserva Legal, que é o próximo assunto a ser explanado neste presente estudo.

PRINCÍPIO DA LEGALIDADE E ANALOGIA

Exposto como o primeiro artigo do Código Penal, o conteúdo que dá origem ao que chama-se de Princípio da Legalidade, ou da Reserva Legal[11], se estabelece como base para todos os outros

[11] Princípio localizado no Art. 1º do Código Penal (1940).

artigos presentes no Código, uma maneira breve e sucinta de demonstrar sua importância e necessidade.

Dessa forma, é imprescindível citar MELLO (2022, p. 102)[12], que em suas palavras descreve a importância desse princípio:

> Enquanto o princípio da supremacia do interesse público sobre o interesse privado é da essência de qualquer Estado, de qualquer sociedade juridicamente organizada com fins políticos, o da legalidade é específico do Estado de Direito, é justamente aquele que o qualifica e que lhe dá a identidade própria.

O Princípio da Legalidade, disposto no art. 1º do Código Penal[13] (também é possível encontrar o mesmo princípio no art. 5º, XXXIX, da Constituição Federal/88)[14], pondo a salvo que não é passível de aplicação de pena aquela conduta não tipificada anteriormente em forma de lei.

A partir desse pressuposto, cabe compreender que, se a legislação não implementar lei que faça previsão aos cibercrimes, em todas as esferas e utilizando da nomenclatura e especificidade correta para que não se abra brechas à possíveis lacunas, de modo que os regule e imponha sanção, não haverá crime, que leva, certamente, a não imposição e regulamentação específica e prévia de pena.

Por mais que, para o homem médio, haja necessidade de haver previsão de pena, e consideração de crime perante à conduta do agente, não se pode cobrá-la, já que não há lei anterior que o possa definir.

Estabelecer uma legislação ideal, avançada, aos crimes virtuais não tende a suprir apenas uma necessidade jurídica do Estado, mas assegura o sentimento de mínima segurança jurídica do cidadão, que, nos dias atuais utiliza a internet e seus meios para continuar a viver atualizado e inserido em sua própria sociedade, inclinando à dignidade do indivíduo e às garantias

[12] MELLO, Celso Antônio Bandeira de. Curso de direito administrativo, p. 102. 36ª Edição, 2022.
[13] Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.
[14] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;

constitucionais carregadas por ele, relembrando o artigo 5º, *caput* e inciso X, da Constituição Federal/88[15].

Para que haja correta implementação, mudança e renovação do aspecto jurídico-penal, a fim de regularizar a legislação no tocante aos crimes cibernéticos, e estar, portanto, regular ao Princípio da Legalidade, é necessário que a "máquina legislativa" do Estado apresente profissionais que incorporem noções informáticas quanto à elaboração de projetos de leis, instrumentos de investigação, nomenclaturas do meio digital, entre outros mecanismos, para assegurar que a competência legislativa brasileira esteja coerente com a nova realidade, suas mudanças e à mente avançada, meticulosa e engenhosa dos cibercriminosos.

Contornando a ideia de estabelecer nova legislação ao ordenamento jurídico e renovar as leis, existe parte doutrinária em concordância com a aplicação de analogia da lei penal, uma vez sendo utilizada pelos juristas como fonte interpretativa à aplicação aos crimes cometidos no ciberespaço.

Outrora, a outra parte da doutrina defenda que a aplicação de analogia[16], integração do ordenamento jurídico com a intenção de cobrir lacunas existentes na lei, a esses casos possa atribuir uma conduta maléfica ao réu, *in malam partem*, o que diverge de um princípio penal, ao qual age, sempre que possível, em benefício do réu, por não haver legislação específica que normatize condutas ilícitas na internet.

Sobre a ideia de utilizar-se de analogia, pensando acerca de ajuizar-se *in malam partem*, far-se-á indispensável citar alguns doutrinadores que são favoráveis a aplicação da analogia, sem que esta seja utilizada *in malam partem*, como NUCCI (2022)[17], que diz:

> [...] se noutros campos do Direito a analogia é perfeitamente aplicável, no cenário do Direito Penal ela precisa ser cuidadosamente avaliada, sob pena de ferir o princípio constitucional da legalidade (não há crime sem lei que o defina; não há pena sem lei

[15] Art. 5º, V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;

[16] (CUNHA, 2015, p.64) [...] a analogia consiste no complexo de meios dos quais se vale o intérprete para suprir a lacuna (o vazio) do direito positivo e integrá-lo com elementos buscados no próprio direito. Nesta ótica, seu fundamento é sempre a inexistência de uma disposição precisa de lei que alcance o caso concreto.

[17] NUCCI, Guilherme de Souza. Código penal comentado. 22. ed. Rio de Janeiro: Forense, 2022.

> que a comine). Nesse caso, não se admite a analogia in malam partem, isto é, para prejudicar o réu.

CUNHA (2020, p. 74-75)[18], ao dizer que:

> Em síntese, com espeque no princípio da legalidade, o emprego da analogia no Direito Penal somente é permitido a favor do réu, jamais em seu prejuízo, seja criando tipos incriminadores, seja agravando as penas dos que já existem.

MASSON (2015)[19], no que diz:

> Não se pode pretender a aplicação da analogia para abarcar hipótese não mencionada no dispositivo legal (analogia in malam partem). Deve-se adotar o fundamento constitucional do princípio da estrita legalidade na esfera penal.

A partir dessas fundamentações, é inevitável concluir que ainda que haja vasta possibilidade de utilizar analogia a certos casos de delitos cibernéticos, muitas outras condutas são atípicas do ordenamento jurídico penal, ações inimagináveis de acontecer em 1940, ano que se deu o Código Penal utilizado no Brasil.

Condutas que apenas foram surgir após o vasto aumento da utilização, informação e acesso que a internet e tecnologia proporcionaram, não apenas para o Brasil, mas para o mundo, corroborando para que o ordenamento jurídico rapidamente ficasse para trás em relação à velocidade com que tudo se modificou.

PROBLEMATIZAÇÃO ACERCA DA EVOLUÇÃO DO METAVERSO E A FALTA DE REGULAMENTAÇÃO.

Retomando a ideia do último parágrafo do tema anterior, a rápida evolução tecnológica faz com que o ordenamento jurídico, não apenas o brasileiro, fique defasado em relação à sua veloz adaptação ao meio social, às novidades, e também, à rápida maquinação de práticas delitivas que podem ser conduzidas através desse meio por cibercriminosos.

[18] CUNHA, Rogério Sanches. *Manual de Direito Penal – Parte Geral*. Vol. Único. 8. ed. Salvador: Editora Juspodivm, 2020.
[19] MASSON, Cleber. Direito penal esquematizado – Parte geral – vol. 1. 9.ª ed. Rio de Janeiro: Forense; São Paulo: Método, 2015.

Dessa forma, ao pensar em um ambiente coletivo, é fato que se possa imaginar que as relações humanas, por mais que virtuais, são passíveis de condutas ilícitas, ainda mais em um ambiente tão propício, onde muitos a tratam como uma terra sem lei.

Nos tempos atuais, o assunto que mais tem circulado no Brasil e no mundo, em relação ao desenvolvimento digital, é o metaverso[20], isto é: um mundo virtual que tenta simular a realidade através de realidade virtual, realidade aumentada, dispositivos eletrônicos e internet.

Segundo o advogado BATICH (2023)[22], quanto ao desenvolvimento do metaverso:

> propiciar um ambiente para criminosos entrarem em contato e organizarem ações como tráfico de drogas, devido à falta de monitoramento pelas autoridades. É um ambiente propício à negociação, lícita ou ilícita.

Muitas realidades virtuais já foram recepcionadas pelos brasileiros, e são elas: *Second Life, Minecraft, Fortnite, Decentraland, VRChat, Roblox, Entropia Universe*.

Diversas plataformas do metaverso, como é o caso da plataforma *Discord*, simulam a realidade, e buscam por gerar interações entre seus usuários, possibilitando a criação de salas de bate-papo que proporcionem conversas em tempo real, sendo elas, por voz, texto e compartilhamento de arquivos.

Porém, um dos primeiros escândalos envolvendo essa plataforma, *Discord*, aconteceu em 2017, ao ser revelado que a plataforma havia sido alvo de *hackers*, que conseguiram acessar informações pessoais de milhões de usuários, incluindo nomes, endereços de e-mail e senhas, ao obterem essas informações, os mesmos enviaram e-mails de spam e phishing aos usuários da plataforma.

[20] Segundo Mahajan e Gupta (2021), o metaverso é uma evolução da internet, uma nova forma de comunicação, que permite maior interação entre as pessoas através de maior nível de imersão, transformando a forma de relacionamento e comunicação. [22] Disponível em:<https://exame.com/future-of-money/crimes-no-metaverso-conheca-os-principais-tipos-e-as-punicoes-legais/> Acesso em: 15 de agosto de 2023.

No ano seguinte, em 2018, a plataforma recebeu mais críticas ao lidar com mais um escândalo, dessa vez por veicular conteúdo de abuso sexual infantil (CSAM[21]). Na época, foi revelado que a plataforma estaria hospedando servidores que eram utilizados para compartilhar conteúdos de abuso sexual infantil. Embora esses servidores tenham sido removidos, a plataforma se manteve irreverente quanto a criar soluções para que o mesmo caso não se repetisse, e que esse tipo de compartilhamento, de CSAM, fosse cessado de uma vez por todas na plataforma.

Em 2020, surgiram novas críticas à plataforma *Discord*, por ser envolvida em mais um escândalo, ao qual estaria envolvida com a disseminação de discursos de ódio, tendo sido revelado que a plataforma estaria, mais uma vez, hospedando servidores utilizados para esse tipo de disseminação. A plataforma removeu os usuários envolvidos, mas não tomou medidas eficientes para que esse tipo de ocorrência fosse extinguido de vez do *Discord*.

É possível observar que alguns crimes praticados no metaverso são bem semelhantes com os crimes reais, seguindo um certo padrão, como: roubo/furto de patrimônio através de golpes ou roubo de dados, racismo, assédio, pedofilia, pirataria, crimes contra a honra, entre outros, além de crimes que foram apropriados ao meio digital, como o roubo de dados pessoais ou de empresa, e exposição sem autorização.

Aprofundando melhor nos crimes apropriados do meio digital, mais especificamente no metaverso, existe certa discussão sobre consequências no mundo externo sobre atos delituosos cometidos virtualmente, e é o caso do que se diz sobre "homicídio no metaverso". Ainda não foi possível concluir se há chances de matar alguém, um avatar, na realidade virtual, mas há ocorrência de crimes que tem o poder de devastar uma vida, como difamação, roubo de bens e dados, entre outros, acarretando efeitos na vida real, e até mesmo induzir ao suicídio.

Sobre isso, BORNELI (2023)[24] faz questão de ressaltar algo muito importante:

> [...] as pessoas que estão no metaverso são as mesmas pessoas que estão no mundo físico, por mais que estejam travestidas de um avatar, boneco. Elas continuam tendo

[21] CSAM, em inglês, significa material de abuso sexual infantil. Esse material consiste em qualquer representação visual, incluindo, mas não se limitando a, fotos, vídeos e imagens geradas por computador que contenham um menor envolvido em conduta sexualmente explícita. [24] Disponível em:<https://exame.com/future-of-money/crimes-no-metaverso-conheca-os-principais-tipos-e-as-punicoes-legais/> Acesso em: 15 de agosto de 2023.

> deveres e são passíveis de qualquer tipo de punição pelos crimes que cometam em um mundo virtual. O mundo virtual, um metaverso, é um espelho do que acontece no mundo real. Os comportamentos são muito parecidos.

Com tantas problemáticas geradas através desses novos meios e modelos tecnológicos, foi desenvolvida uma ferramenta para combater esses crimes cibernéticos, principalmente no metaverso, chamado OSINT, que significa *Open-Source Intelligence*, ao qual foi descrito pelo Congresso dos Estados Unidos da América, na publicação da Lei de Autorização de Defesa, o seguinte:

> A OSINT é uma inteligência produzida a partir de informações publicamente disponíveis que são coletadas, exploradas e divulgadas em tempo hábil para uma audiência própria, objetivando atender a um requisito de inteligência específico[22].

Como é sabido, os criminosos possuem variadas práticas de condutas delituosas, indo além através de dispositivos eletrônicos que funcionam como mecanismos para essas práticas, diante dessas práticas é possível se deparar com a ocorrência de: fraudes, ao criar perfis e identidades falsas para enganar pessoas, assédio, abuso sexual infantil no tocante ao compartilhamento desse tipo de conteúdo, disseminação de ódio e incitação à violência, entre outros.

A utilização da OSINT como ferramenta que auxilia no combate a crimes originários no metaverso consiste no processo de coleta de informações de fontes publicamente disponíveis, sendo possível identificar criminosos através do rastreio de endereços de IP, rastreio de atividades criminosas ao monitorar contas de mídias sociais e demais atividades *online* e interromper operações criminosas ao derrubar sites e plataformas.

No entanto, é extremamente necessário que esse poderoso mecanismo seja utilizado em conjunto de técnicas investigativas e métodos tradicionais de aplicação da lei, no Brasil ainda não é possível utilizar esse meio e não há iniciativas, mas é possível observar alguns casos práticos em que esse método já foi utilizado em outros países. O FBI, em 2021, utilizou OSINT para identificar e prender um homem que solicitava conteúdos sexuais para menores no metaverso. Em outro caso, a Polícia Federal Australiana usou o OSINT para rastrear um grupo

[22] Tradução livre do original: "OSINT is intelligence that is produced from publicly available information collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement".

de criminosos que utilizavam o *Discord* para realizar a venda de drogas. Já em 2023, a Agência Nacional do Crime do Reino Unido utilizou o OSINT para identificar e prender um homem que propagava discursos de ódio através do metaverso.

Desse modo, é possível visualizar que à medida em que os meios eletrônicos, os avanços e desenvolvimento de realidades virtuais, como é o caso do metaverso, possibilitam e facilitam a prática de cibercrimes, passando a ser ainda mais necessário que o ordenamento jurídico esteja apto a realizar as mudanças e criações necessárias em leis e suas práticas, possibilitando a punição ideal e correta aos casos, além de iniciar a utilização do OSINT como ferramenta importante e necessárias para contribuir na aplicação das leis aos casos.

Criminalizar uma conduta na realidade virtual é de extrema importância, além de que, deve haver especificação sobre quem é passível de proteção e punição, fazendo-se necessário enfatizar que a proteção de um avatar, no campo virtual, apenas se dá quando constitui propriedade de uma pessoa física ou empresa.

É um fato que o sistema investigativo carece de agentes especializados em sistemas informáticos que evoluam junto às estratégias de criminosos, fiscalizando suas condutas de modo preventivo.

IGREJA (2022)[23], especialista em tecnologia, inovação e tendências, enfatiza esse pensamento, e diz:

> Acredito que a Justiça terá que se adaptar. A preocupação é que as instituições e organismos sempre estão um passo atrás da evolução tecnológica. O primeiro ponto é saber se os magistrados e todos os envolvidos têm algum grau de conhecimento do que está acontecendo.

Ademais, o sistema legislativo precisa identificar tais condutas e tipificá-las, não apenas em leis, mas deve haver concordância entre o Estado e empresas do mercado de tecnologia para implementar medidas protetivas aos seus usuários, termos de consentimento e convivência, que estabeleçam regras, fazendo com que o conceito de “terra sem lei” deixe de existir.

[23] Disponível em: <https://www.bitmag.com.br/o-que-diz-a-justica-em-caso-de-assassinato-no-metaverso/> Acesso em: 22 de agosto de 2023.

Sinalizar medidas de segurança no meio tecnológico ajuda no combate à criminalização do espaço e transmite maior segurança aos seus usuários.

Porquanto, e de modo infeliz - já que, sem regras específicas, a incidência de brechas pode colaborar para que a lei aplicada não seja válida e o crime praticado não seja punido aos crimes praticados em ambiente virtual - sem as medidas protetivas necessárias e específicas que devem ser oferecidas pelo Estado, os crimes cometidos em ambiente virtual deverão ser respondidos através de leis já existentes do ordenamento legislativo brasileiro.

É estritamente necessário que a população e toda a sociedade jurídica cobre um posicionamento ideal dos representantes do sistema legislativo e do Estado, para que sejam implementadas regras e tipificação de quaisquer conduta frágil e delitiva nos meios digitais, a implementação de nova legislação mais abrangente e específica aos casos dos cibercrimes é uma carência existente há anos no sistema jurídico brasileiro e está longe de ser efetivamente solucionado.

CONSIDERAÇÕES FINAIS

O mundo da internet surgiu como uma facilitadora para as relações humanas e, também, surge como a extensão das informações, que podem ser levadas a qualquer lugar e estão disponíveis ao acesso a todo momento. No entanto, em meio a tantas vantagens existe certa complexidade quanto a profundidade da tecnologia, até que ponto não existem fronteiras, e surge a necessidade de regular e proteger as relações, e todas as movimentações que existem no mundo cibernético para que a ideia de que a internet é uma “terra sem lei” não exista mais.

A partir do conhecimento acerca dos cibercrimes foi possível adentrar no tema de extrema importância a respeito da falta de legislação específica e correspondente aos crimes cometidos em meio virtual, dessa forma, retornamos ao princípio do Código Penal de 1940, em seu artigo 1º, ao qual diz respeito ao Princípio da Legalidade, que faz inexistir crime se a conduta não for tipificada.

Tal descrição foi fundamental para que fosse possível realizar uma análise das leis vigentes a tipificar as condutas típicas e antijurídicas e culpáveis. A análise dessas leis mostra que ainda existem diversas lacunas, por falta de tipificação adequada, falha nos termos e nomenclatura

informática, e por não ser possível que o sistema legislativo acompanhe todo o avanço que a internet traz para as relações humanas. Exemplo disso é a falta de conhecimento necessário quanto ao mundo do metaverso, um universo à parte e desconhecido por muitos que é passível de ser um meio que facilita a prática de conduta ilícita, um dos motivos é por ainda não oferecer proteção devida aos usuários de suas plataformas.

Nesses casos, a proteção de dados no metaverso deve ser abordada de forma distinta da proteção de dados na internet, havendo necessidade de especificidade, isso se dá pelo fato de que as interações no metaverso são mais imersivas e interativas, havendo necessidade de garantir que as informações dos usuários sejam controladas e não sejam utilizadas sem real consentimento, pensando ainda que diversas transações realizadas nesse meio são financeiras.

Para colaborar com a ideia de transformar efetivamente o universo digital em um espaço seguro e transparente é preciso que as empresas criadoras desses ambientes adotem políticas claras quanto à privacidade e segurança dos usuários.

Dessa forma, é imprescindível que os usuários estejam cientes dos riscos e vulnerabilidades que se encontram nesses meios virtuais, e sejam conscientizados sobre a maneira correta de se portar e a quem acionar no caso de possíveis violações, sendo informado quais são os mecanismos de proteção e canais de denúncia. Tornando ainda mais necessário que o sistema jurídico brasileiro se posicione no que diz respeito às novidades que a internet propicia, adequando e desenvolvendo leis específicas, e dispondo de um mecanismo determinado de analogia quanto a esse tipo de crime.

REFERÊNCIAS BIBLIOGRÁFICAS

BLUM, R. M. S.; DAOUN, A. J. **Direito & Internet**. São Paulo: Editora Edipro, 2000.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Portal da Legislação do Governo Federal. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 12 Jun. 2023.

BRASIL. **Código Penal, decreto lei nº 2.848**, de 07 de Dezembro de 1940. Disponível em : <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 20 Jul.2023.

BRASIL. **As modificações promovidas pela Lei Carolina Dieckmann no Código Penal**. Disponível em: <http: www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pelalei-carolina-dieckmann-no-codigo-penal/9986>. Acesso em: 20 Jul. 2023.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 20 Jul. 2023.

BRASIL. **Lei Nº 14.132**, de 31 de Março de 2021. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm>. Acesso em: 20 Jul. 2023.

BRASIL. **Lei n. 12.965** de 23 de Abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 Jul. 2023.

CAPEZ, **Curso de Direito Penal: parte geral**. 15. ed. São Paulo: Saraiva, 2012.

CASA CIVIL. **90% dos lares brasileiros já têm acesso à internet no Brasil, aponta pesquisa.** Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileirosja-tem-acesso-a-internet-no-brasil-aponta-pesquisa>. Acesso em: 20 Jul. 2023.

CUNHA, Rogério Sanches. **Manual de Direito Penal** – Parte Geral. Vol. Único. 8. ed. Salvador: Editora Juspodivm, 2020.

Crimes no metaverso? Conheça os principais tipos e as punições legais. Revista Exame, 2023. Disponível em: <https://exame.com/future-of-money/crimes-no-metaverso-conheca-os-principais-tipos-e-as-punicoes-legais/>. Acesso em: 14 Set. 2023.

Crimes Cibernéticos: o que são, leis aplicáveis e mais. Posesa, 2022. Disponível em: <https://posesa.com.br/crimes-digitais-leis-aplicaveis/>. Acesso em: 14 Set. 2023.

FERNANDES, David Augusto. **Crimes cibernéticos: o descompasso do estado e a realidade**. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

HACKEROTT, Nadia A. T. **Aspectos jurídicos do E-commerce**. 1.ed. São Paulo, 2021.

MASSON, Cleber. **Direito penal esquematizado – Parte geral** – vol. 1. 9.ª ed. Rio de Janeiro: Forense; São Paulo: Método, 2015.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo**, p. 102. 36ª Edição, 2022.

NUCCI, Guilherme de Souza. **Código penal comentado**. 22. ed. Rio de Janeiro: Forense, 2022.

PALAZZI, Pablo Andrés. **Delitos informáticos**. Buenos Aires: Ad Hoc, 2014.

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