PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

CRIMES DIGITAIS NA ERA DO METAVERSO NO BRASIL

DISCENTE: MARQUÉSIA PEREIRA FERNANDES

ORIENTADOR: PROF Ms MARCELO DI REZENDE

GOIÂNIA-GO
2022

MARQUÉSIA PEREIRA FERNANDES

CRIMES DIGITAIS NA ERA DO METAVERSO NO BRASIL

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS)

Prof. Ms. Marcelo Di Rezende

GOIÂNIA-GO

2022

MARQUÉSIA PEREIRA FERNANDES

CRIMES DIGITAIS NA ERA DO METAVERSO NO BRASIL

Data da Defesa: 30 de novembro de 2022

BANCA EXAMINADORA

Orientador: Prof. Ms. Marcelo Di Rezende Nota:

Examinador Convidado: Dra. Marina Rubia Mendonça Leão Carvalho Nota:

CRIMES DIGITAIS NA ERA DO METAVERSO NO BRASIL

Marquésia Pereira Fernandes [1]

Nos últimos meses, a criação de um universo virtual, compartilhado e hiper-realista se tornou o destaque tecnológico, serão necessários alguns equipamentos específicos para acessar o metaverso, o termo não se refere a nenhum tipo específico de tecnologia, mas sim a uma ampla mudança na forma como interagimos com o mundo digital que conhecemos isso porque, na prática, a sensação seria de estar totalmente imerso nesse universo virtual, em uma união da realidade aumentada com a realidade virtual. Ou seja, as telas planas de celulares, computadores e tablets seriam substituídas por uma experiência tridimensional, em que seria possível interagir com objetos e informações variadas. Entender as mudanças relacionadas a esse novo conceito de interação digital antes visto apenas na ficção agora é uma realidade e vem inovando o mundo virtual que conhecíamos, qual importância desse mundo digital ofertado e seus avanços. A pesquisa inicia esclarecendo o conceito de crime no ambiente virtual e explicando a multiplicidade de ferramentas virtuais a importância do uso consciente dessa ferramenta ora tão dinâmica e transformadora quanto desconhecida. A pesquisa traz o debate de o que são os crime digital e tipificação desses crimes como a legislação brasileira dispõe sobre esse assunto, por fim trazer ao debate também que grande parte dessa segurança é atribuída ao próprio usuário, é necessário ter conhecimento que se dará através de uma educação digital adequada vez que a evolução virtual é contínua e o cidadão brasileiro precisa se resguardar esse será o caminho para se chegar a prevenção e proteção de eventuais “GOLPES” e fraudes pois o criminoso tem se aprimorado cada vez mais em suas práticas delituosas

Palavras-chave: Mestaverso, Crime; digital; educação; lei; internet; cibercrime; redes sociais.

[1] Acadêmica do Curso de Direito pela Pontifícia Católica de Goiás.

SUMÁRIO

INTRODUÇÃO

A popularização da internet juntamente com o crescimento do número de usuários, são inúmeros benefícios encurtaram fronteiras, com maior avanço em todos os setores de produção, a informação que circula de forma instantânea, no entanto, cresceu também as ocorrências de crimes digitais essa nova modalidade de crime que surgiu a partir do meio virtual.

A preocupação em torno do assunto só cresce o que faz com que o usuário se pergunte até onde é possível navegar seguro, como se proteger desses piratas digitais que ao menor sinal de oportunidade já saem fazendo vítimas.

Nessa pesquisa discutiremos sobre o METAVERSO, buscando interpretar os elementos relacionados ao tema buscando respostas para os questionamentos levantados e esclarecer seu conceito, pois o que é exatamente o METAVERSO? Como funciona? Quando teremos acesso a essa tecnologia? Como esse é um tema que gera muitas dúvidas, para você entender os principais pontos do METAVERSO, e como ele deve influenciar a sua vida e suas relações.

Portanto, nos capítulos seguintes, faremos uma análise desse novo universo digital, da necessidade de criar formas de proteção ao usuário da internet e de imprescindibilidade de o Estado Brasileiro estabeleça diretrizes, acordos para que as próprias plataformas digitais invistam na proteção de seus usuários, crie instrumentos de segurança que identifique, evite ou interrompa comportamento delituoso.

I INTERNET

A internet é um meio de comunicação cada vez mais utilizada no dia a dia. Dentro da rotina das pessoas, ela é considerada por muitos indispensáveis para realizar diversos serviços, como por exemplo trabalhar, assistir aula, participar de congressos, fazer compras e conhecer novas pessoas. Logo, estar on-line promove relações sociais sem ter que sair de casa.

Esta ferramenta imprescindível se comunica com um banco de dados, que pode até ser considerada como uma fonte de ouro na visão daqueles que possuem a intenção de praticar crime a partir desses dados, possibilitando, portanto, em muitos casos um grande prejuízo financeiro e pessoal ao usuário de boa-fé da internet.

A internet é o “Eldorado” da informação, por ela circulam diversos dados, de tudo quanto é tipo, de bilhões de pessoas. Esses dados, após serem identificados, catalogados, tratados e organizados, geram informações valiosas.

Quanto mais navegamos pela internet, mais obtemos acesso à informação e mais ainda nos é oferecido novas informações. A impressão que deixa ao usuário é a de que ele consegue acessar qualquer parte do mundo e fazer o que ele bem entender através da internet.

Por detrás da parte mais acessível da internet, habita um submundo peculiar e multifacetado. A chamada Deep Web, possui em suas características uma menor transparência e um maior anonimato.

Mas engana-se aquele que pensa que a grande maioria dos crimes acontece na Deepweb. Primeiramente, é importante fazer um breve apanhado das camadas que possui a internet, para que se possa vislumbrar melhor o assunto trabalhado. Vejamos a imagem abaixo:

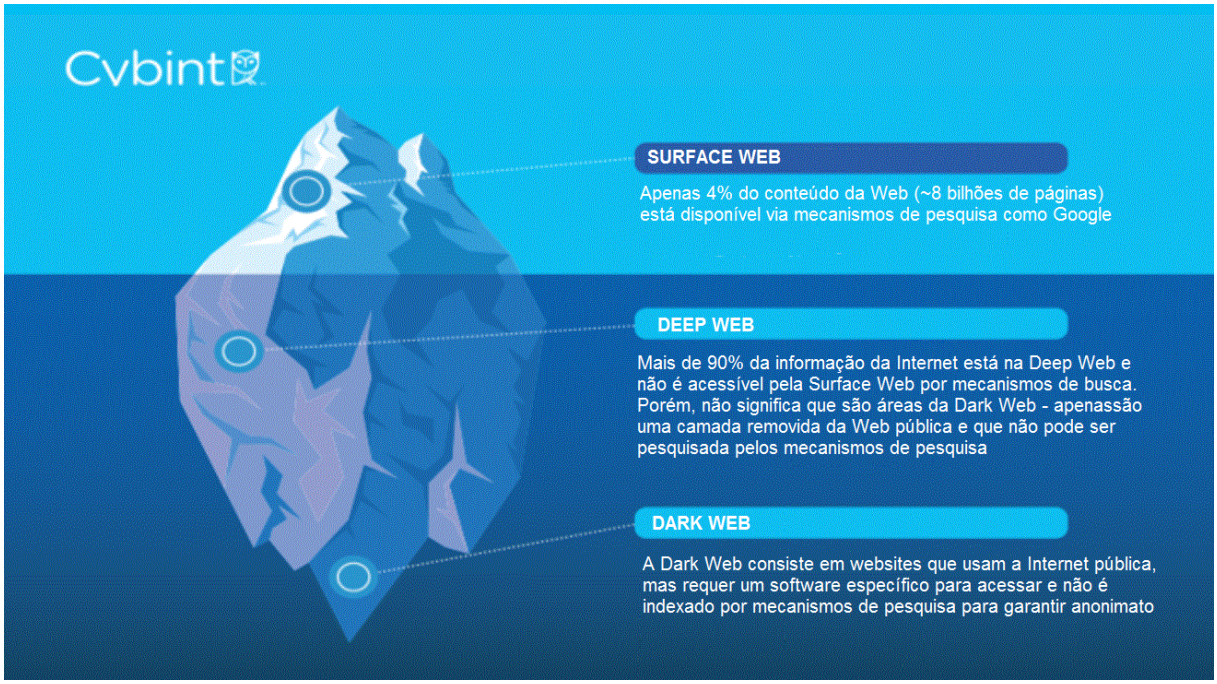

Figura 1: Tamanho da Deep Web

Fonte: secureworldexpo.com

A partir da imagem, percebemos a internet em 3 camadas. A Surface Web é a camada que contém os mecanismos de busca fornecendo um conteúdo aberto aos usuários, é onde acessamos sites como Amazon, Google, Bing, Pinterest, Facebook e Jornais como o BBC News. Em resumo, é onde as atividades diárias acontecem, é também o que a maioria das pessoas conhecem como Internet. A Surface Web é a parte indexada.

A Deep Web é a camada seguinte, que se encontra abaixo da “internet comum”, essa é a parte não indexada da internet, ela não pode ser encontrada por navegadores comuns. Ocorre que ela é formada por dados feitos para serem ocultos do público, nela guarda-se todos os tipos de informações.

Nas palavras de Sydow:

> *UMA PARTE DA DEEPWEB, ASSIM COMO UMA PARTE DA SOCIEDADE, É UTILIZADA ESPECIALMENTE PARA A DELINQUÊNCIA OU PARA DESVIOS SOCIAIS. TAL PARTE NORMALMENTE SÓ NÃO ESTÁ INDEXADA, MAS TAMBÉM NÃO RARO POSSUI FORMA ESPECIAL DE ACESSO, A PARTIR DE MECANISMOS DE ANONIMIDADE MAIS COMPLEXOS COMO O USO SOFTWARES DEDICADOS, USO DE CONFIGURAÇÕES ESPECIAIS OU AUTORIZAÇÕES ESPECÍFICAS. (SYDOW.2021. P.58)*

Nessa perspectiva, chegamos à conclusão de que ao contrário da imaginação da maioria das pessoas, a DeepWeb não é um lugar terrível contendo apenas conteúdo estranho e criminoso. Parte dela é utilizada para a confidencialidade, anonimidade, armazenamento de informações financeiras e bancárias, direitos autorais, e-mails e armazenamento na nuvem.

E por último, temos a camada mais profunda da internet, a chamada Dark Web, nela utiliza-se o anonimato proveniente do TOR, um navegador específico que utiliza um protocolo de funcionamento conhecido como cebola (do inglês onion, formando a sigla do navegador de nome The Onion Router- TOR).

Esse navegador camufla a localização do servidor, permitindo que apenas usuários TOR ou outra aplicação que utilize o sufixo "onion" visualiza as páginas e sites registrados na Dark Web.

Os sites que habitam a Dark Web utilizam servidores fora do convencional compostos por umas redes voluntárias ao redor do mundo, criando uma comunicação fortemente criptografada em camadas, é daí que surge a comparação com uma cebola, pois contém camadas e camadas de criptografia.

O nome de Dark Web vem do conceito de darknet. A darknet é uma rede sobreposta que só pode ser acessada sob requisitos específicos e usa protocolos que excedem completamente a superfície da web e outros padrões da Deep Web. Isso leva ao uso da dark web para distribuição de conteúdo e transações ilegais. Por exemplo, o site do Silk Road foi fechado pelo FBI em 2013 porque era uma plataforma para transações ilegais de drogas e um serviço oculto que usa a rede TOR para garantir o anonimato de compradores e vendedores.

Portanto, devido ao seu anonimato, a Dark Web está realmente inundada com atividades ilegais que vão desde a compra de drogas até a compra e venda de órgãos humanos. Nela ainda pode-se encontrar material sobre pedofilia e zoofilia, contratos com assassinos e tráfico de pessoas, fóruns de terrorismo, nazismo e sites com uma variedade de conteúdos e tópicos inimagináveis.

Para uma melhor compreensão das camadas da internet explicadas acima, se faz necessário a explicação do conceito de indexação. A indexação ou indexar uma informação é o processo de identificação dos sites que existem e o armazenamento da URL[2], nome e o assunto do que se trata o site.

[2] A URL, Uniform Resource Locator, na sua tradução literal é um localizador uniforme de recursos, é o endereço onde se encontra um recurso informático (documento, serviços, mídia) na internet.

Logo, todas as informações que encontramos quando pesquisamos algo no Google, por exemplo, só é possível pois aquele conteúdo foi indexado, permitindo em consequência a identificação do site.

1.1 ANONIMATO

O anonimato no ambiente virtual é um assunto polêmico, pois normalmente não temos informações se é uma pessoa agindo ou um computador de forma automatizada. Nos últimos tempos, nota-se uma crescente atuação de bots[3] comandados por pessoas para disseminar informações em massa.

O significado de anonimato conforme o dicionário Priberam de língua portuguesa é a qualidade do que é anônimo; sistema de escrever anonimamente. Na internet, o anonimato é uma posição de bloqueio ou impedimento no que diz respeito a identificação da autoria de uma postagem.

O anonimato na Internet pode ser empregado através de VPNs, serviço que criptografa o tráfego de internet e disfarça sua identidade online por meio de redirecionamentos entre servidores, mascarando a real localização do usuário.

Antes de adentrarmos a fundo no assunto, é interessante discutir a relevância do anonimato na rede ou quando pode ser usado para fins bons ou ruins. Portanto, é importante fazer uma pergunta: o anonimato é bom? Se é bom, em que cenário se aplica? Por quê? As respostas a essas perguntas dependem da finalidade do serviço anônimo.

Por exemplo, o anonimato pode ser visto em um cenário positivo quando pensamos na conservação da privacidade e segurança na internet, visto que, por um lado auxilia na prática da liberdade de expressão. De outro lado, o anonimato pode ser algo ruim quando um indivíduo sequestra os dados de uma empresa e exige um resgate de alto valor financeiro, deixando a empresa em um cenário totalmente vulnerável e à mercê da pessoa que está do outro lado da tela.

A vida moderna, nos permite compartilhar muitas informações pessoais online. Nesse sentido as redes sociais são catalisadoras dessa prática, visto que, nela as pessoas compartilham os hábitos de consumo, a rotina pessoal, a rotina profissional, estilos de vida, e as opiniões manifestas sobre os diversos assuntos que percorrem na rede.

---

[3] Bot- abreviação de robô- é um programa que executa tarefas automatizadas, repetitivas e pré-definidas.

Importante distinguir os conceitos de anonimato e privacidade. A privacidade é um direito constitucional defendido no artigo 5°, inciso X da Constituição federal de 1988, nela tutela-se o direito de controlar a divulgação de dados e imagem pessoal. O anonimato é a ação de ocultar, não divulgar, a identidade.

Túlio Vianna demonstra que o direito à privacidade corresponde a um conjunto de direitos, vejamos:

> *DIREITO DE NÃO SER MONITORADO, OU SEJA, DE MANTER O QUE DIZ E SUA IMAGEM PRIVADAS*
>
> *DIREITO DE NÃO SER REGISTRADO, QUE DISCORRE SOBRE A PRESERVAÇÃO QUANTO A GRAVAÇÕES SEM CONSENTIMENTO*
>
> *DIREITO DE NÃO SER RECONHECIDO, SE REFERINDO A NÃO TER CONTEÚDOS SOBRE SI PUBLICADOS EM QUALQUER CANAL, INCLUINDO A INTERNET.*
>
> *(APUD SABINO, MARCO ANTÔNIO DA COSTA. 2020).*

Assim, resta clara a diferença que há entre a privacidade e o anonimato, sendo errôneo confundir os dois conceitos que denotam circunstâncias diferentes.

Ao refletirmos sobre a facilidade de se encontrar informações na Internet, e analisando também a facilidade de se espalhar, copiar e reproduzir arquivos, percebemos que, distanciando o pensamento da atividade criminosa, para o usuário comum é difícil estar ou ser totalmente anônimo.

Ora, tudo que se faz no meio virtual deixa um rastro e é impossível apagar todos os rastros digitais visto que alguns sistemas podem manter seus dados mesmo após a solicitação de exclusão. Logo tempos uma falsa sensação de controle sobre as nossas próprias informações.

Em se tratando das atividades delitivas no meio virtual, o anonimato por um lado permite uma segurança para denunciar abusos, violências e transgressões, sendo possível preservar a imagem da vítima, ou seja, o anonimato contribui para dar voz aqueles que de alguma forma são coibidos. Em contrapartida, se torna possível, em função do anonimato, a promoção de discurso de ódio, fake News, fraudes, chantagem, assédio sexual, estelionatos, sequestro de dados, cyber terrorismos e vários outros delitos que têm sua prática mais “acessível” por se utilizar da proteção que o anonimato oferece.

Assim sendo, a internet proporciona a todos os usuários a sensação da total anonimidade. Essa sensação impulsiona alguns indivíduos a ir de encontro a lei, na ilusória sensação de que não serão descobertos, de que agirão sem serem percebidos ou julgados.

A legislação brasileira proíbe o anonimato expressamente, tanto no mundo real quanto no virtual, traz o artigo 5° inciso IV da Constituição:

> *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:*
>
> *IV - É LIVRE A MANIFESTAÇÃO DO PENSAMENTO, SENDO VEDADO O ANONIMATO;*

A intenção do artigo ao vedar o anonimato é identificar e, nos casos em que couber, responsabilizar o autor por conteúdo ilegal ou criminoso que tenha sido reproduzido.

No mesmo sentido, o Marco Civil da Internet, Lei nº 12.965/14, no seu artigo 3° reafirma a livre manifestação do pensamento, nos termos da Constituição Federal, desde que haja também a responsabilização dos usuários de acordo com suas atividades.

A Lei Geral de Proteção de Dados, Lei n° 13.709 de 2017, foi promulgada objetivando complementar a literatura do Marco Civil da internet, também tutela sobre o anonimato, garantindo o direito ao mesmo desde que esteja manifestamente expresso pelo titular das informações. Como por exemplo, traz o artigo 18, inciso IV da lei:

> *ART. 18. O TITULAR DOS DADOS PESSOAIS TEM DIREITO A OBTER DO CONTROLADOR, EM RELAÇÃO AOS DADOS DO TITULAR POR ELE TRATADOS, A QUALQUER MOMENTO E MEDIANTE REQUISIÇÃO:*
> *[...] IV - ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS DESNECESSÁRIOS, EXCESSIVOS OU TRATADOS EM DESCONFORMIDADE COM O DISPOSTO NESTA LEI;*

Ou seja, o documento confirma o direito de anonimato no uso, bloqueio ou eliminação de dados que estejam sendo tratados em desconformidade com a lei. Logo, percebe-se que é

protegido pelo ordenamento brasileiro o direito ao anonimato no tocante ao zelo e a privacidade de dados e informações, não se permite, portanto, o uso desse direito para práticas ilegais e criminosas além de coibir a expressão de pensamento de forma anônima.

1.2 HACKER

No universo virtual, há alguns termos que definem alguns usuários com habilidades e conhecimentos avançados em relação ao universo das tecnologias, administração de banco de dados e servidores, e principalmente segurança da informação.

No geral, ambas as classificações demonstram que os agentes são experts em encontrar vulnerabilidades em sistemas operacionais e softwares. Contudo, os objetivos que os levam a encontrar essas falhas nos sistemas são contrários. Enquanto um utiliza de forma legal e construtiva os seus conhecimentos, que é o Hacker, o outro utiliza para cometer delitos por meio de quebras de segurança e invasões de programas ou sistemas operacionais, que é o Cracker.

Contudo, parte da comunidade tecnológica não se agrada em apenas definir um como bom e o outro como ruim. Assim, dentro da Ética Hacker os termos mais corretos, para essas pessoas, seriam: “White Hat” (chapéu branco), “Black Hat”(chapéu preto) e “Gray Hat”(Chapéu Cinza).

White Hat, é o hacker defensivo, ele é o especialista em utilizar suas habilidades para o bem e identificar as fragilidades de um sistema. O White Hat, age com ética e propósito legal.

O Black Hat, é o tipo de hacker mais conhecido, é aquele que viola a segurança de um sistema visando benefício próprio, como por exemplo, roubar dados de cartão de crédito, sequestrar dados de empresas e pedir um resgate com alto valor econômico. Ele pode identificar a vulnerabilidade de um sistema e vender para uma organização criminosa (os Crackers).

Já os Grey Hat, são os Hackers que ficam “em cima do muro”, eles agem de forma legal, mas em certos casos eles se utilizam de ideais pessoais e tomam ações que prejudicam os sites contudo não cometem crimes utilizando essas informações. Eles são bem-intencionados, contudo, se perdem na sua vontade de ajudar e cometem comportamentos que são eticamente questionáveis.

1.3 CRIMES

A nova modalidade de crime que surge a partir do meio digital deixa exposta a nossa integridade física, moral e financeira. Segundo Jonathan Clough, existem três fatores necessários para a prática de crime: a existência de criminosos motivados, disponibilidade de oportunidades adequadas e a ausência de vigilância eficaz. Ou seja, esses elementos são facilmente encontrados no meio digital. Portando, com uma conexão e um dispositivo com acesso à internet, qualquer pessoa mal-intencionada, pode cometer delitos no ciberespaço.

Inicialmente vale entender o que seria o bem jurídico informático e por que protegê-lo. Pois bem, a fundamentação dessa pesquisa é de que a passos largos surge para o direito uma nova preocupação e uma nova necessidade de se proteger a sociedade e o cidadão decorrente dos avanços tecnológicos. Para defendermos que é necessário criar essa proteção, é necessário que haja um bem jurídico a ser tutelado.

Entendemos o bem jurídico como circunstâncias dadas ou finalidades que são úteis para o indivíduo e seu livre desenvolvimento no marco de um sistema global estruturado(...) (*Apud* SYDOW, p 178. 2022) A vista disso, podemos partir do ponto que o avanço tecnológico gerou a imprescindibilidade de se criar um novo bem jurídico. Doutrinariamente, o bem jurídico informático é denominado “segurança informática”, conceito que reúne 3 elementos compreendidos como ativos informáticos: disponibilidade, confidencialidade e integridade telemática.

A disponibilidade refere-se à necessidade de os dados de um usuário estarem sempre ao seu alcance para que ele utilize sempre que desejar. A confidencialidade diz respeito ao sigilo acerca dos dados, tal como o sigilo bancário, se um usuário decide por não publicar determinada informação, ela deve ser protegida até que o portador do dado permita a utilização do dado. Podemos exemplificar isso usando como modelo o aviso de permissão que alguns aplicativos de celular solicitam, para que aquele determinado aplicativo colete ou não informações acerca do usuário. Já a integridade nos remonta a ideia de que os dados produzidos por usuários e inseridos em um sistema configuram um patrimônio individual que merece ser protegido, visto que cabe somente ao usuário titular do dado dispor sobre alterações no mesmo, os ataques a essas informações colocam-nas em risco deixando-as expostas a perca de características originais.

Pois bem, esclarecido o bem jurídico informático e os elementos que o compõem, passamos a analisar os delitos informáticos. Entendemos que o surgimento do Direito Digital e do Direito Penal informático é uma nova especialidade das Ciências Jurídicas. Quanto ao Direito Penal informático, tal como o Direito Penal, faz-se necessário analisar diversas características e princípios que compõe logicamente o estudo dessa nova área.

Ainda há uma divergência quanto à nomenclatura da ciência jurídica que acompanha e estuda os impactos tecnológicos. Nesse sentido, também há discordância na terminologia que trata da criminalidade da área em estudo. Nos ensinamentos de SYDOW:

> *O TERMO MAIS ADEQUADO SERIA "DELITO INFORMÁTICO" E NÃO "CRIME INFORMÁTICO" PORQUE HÁ CRIMES QUE PODEM SER REALIZADOS A PARTIR DE TECNOLOGIAS, MAS TAMBÉM HÁ CONTRAVENÇÕES PENAIS QUE O PODEM. DESTARTE, A EXPRESSÃO GENÉRICA "DELITOS" ENGLOBA TANTO "CRIMES" QUANTO "CONTRAVENÇÕES PENAIS". QUIÇÁ, TAMBÉM, PODERSE-IA UTILIZA DO TERMO "INFRAÇÕES". NESSE SENTIDO, A RUBRICA DA LEI 12.737/12 AO APRESENTAR QUE A LEI "DISPÕE SOBRE A TIPIFICAÇÃO CRIMINAL DE DELITOS INFORMÁTICOS". (SYDOW.2022. P.266)*

Portanto, para analisarmos o delito informático deve-se partir de diferentes perspectivas em decorrência das suas particularidades. O crime virtual é aquele que não utiliza contato físico entre vítima e ofensor, não possui a necessidade de vistoriar e mapear o local do fato, não apresenta alto risco físico e nem grande violência. Contudo essa categoria delitiva apresenta sempre um padrão que age de forma silenciosa, rápida e sem muito esforço, apresentando por vezes uma simultaneidade de lugares e contando principalmente com o desconhecimento de agentes públicos para falharem na investigação e assim não conseguirem analisar os indícios do crime.

A vista disso, podemos considerar crimes virtuais aqueles que se utilizam de alguma maneira de um sistema de processamento de dados para atentar contrainformações armazenadas e assim se concretizarem. SYDOW, define delito informático da seguinte maneira:

> *DELITO INFORMÁTICO É A CONDUTA TÍPICA, ANTIJURÍDICA E CULPÁVEL COMETIDA ATRAVÉS DE RECURSOS INFORMÁTICOS CONTRA BENS JURÍDICOS COMUNS E/OU COMETIDA EM FAZE DE BEM JURÍDICO*

> *INFORMÁTICO, ATINGINDO OU BUSCANDO ATINGIR A ESFERA DA SEGURANÇA INFORMÁTICA EM SEUS ELEMENTOS CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE. (SYDOW.2022. P.272)*

Atualmente ainda não há uma uniformização da classificação dos crimes informáticos, mas para que seja executado um delito, podemos partir de 3 formas: 1- violando-se o bem jurídico informático em si, em seus elementos, fazendo uso de ferramentas comuns; 2- Utilizando-se do meio informático como instrumento para atacar bem jurídico diverso do informático; 3- Violando-se o bem jurídico informático entre si, em seus elementos, e utilizando-se para isso de meios exclusivamente informáticos.

Em conseguinte, podemos classificar o delito a partir da sua natureza que pode ser quanto ao bem jurídico atingido ou quanto a necessidade do meio. Considerando a primeira natureza, o bem jurídico atingido, o delito poderá ser puro, que é aquele em que o objetivo da conduta do agente é de atingir necessariamente o bem jurídico informático, ou impuro, que é aquele em que pretende atingir um bem jurídico diferente do informático, como por exemplo a honra, patrimônio, dignidade.

Partindo da análise da prescindibilidade do meio, podemos entender o delito por próprios, onde o meio informático é obrigatório para cometer o crime; ou impróprios, que ocorrem quando o agente voluntariamente utiliza o meio informático para cometer o crime, mas ele poderia ter sido praticado por qualquer outro meio.

Com a atualização das tecnologias, novas classificações e modalidades de delito vão surgindo, por conseguinte é atual pensarmos em um mundo virtual que se prepara para emergir globalmente, o Metaverso, que promete ser um mundo virtual onde as pessoas poderão interagir entre si e realizar diversas atividades como fazer compras.

Dessa maneira, o doutrinador Sydow nos convida a refletir sobre a necessidade de se pensar nas possíveis condutas delitivas que poderão ser praticadas no Metaverso[4] e atacarão as NFT's e as criptomoedas[5]. Assim sendo, quando estivermos diante desse cenário, presenciaremos um delito informático que, conforme as classificações aqui explicadas, podem

[4] Metaverso é uma junção do prefixo "meta" e "universo" que descreve o conceito de uma interação futura da internet, composta por espaços virtuais.
[5] NFT (Non Fungible Token) é um tipo especial de token criptográfico que representa algo único; Criptomoedas ou Criptocurrency é um meio de troca financeiro artificial, criado pelo homem.

ser entendidos como delitos próprios por necessitarem do meio informático para se concretizarem. Para concluirmos o assunto, mister citar que o uso do meio informático gera, necessariamente, um rastro dos sites frequentados, dos registros dos comandos utilizados e da máquina por onde saiu o comando.

1.4 LEGISLAÇÃO PENAL

O ciberespaço teve sua popularização no final da década de 1990, é a partir desse fenômeno que surgiu a necessidade de compreender esse espaço sob todas as suas vertentes, social, cultural, científica e demais. A internet se mostrou uma poderosa arma para ampliar conhecimentos e socializar com o outro, assim tornou-se possível uma troca cultural maior.

A tecnologia proporcionou e ainda proporciona um crescimento exponencial de sistemas, programas e aplicativos que foram desenvolvidos para facilitar a adoção do meio virtual. Além disso, no início dessa nova cultura, não havia um limitador do espaço virtual, logo foi inserido na sociedade a expansão de um meio não controlado pelas autoridades e aparentemente totalmente livre, para se fazer, ser (enquanto "personagem virtual") e falar o que quiser.

Essa aparente liberdade juntamente com a facilidade de esconder quem realmente é no espaço virtual, possibilitou abertura para o cometimento de crimes. No Brasil, os primeiros casos de crimes cibernéticos surgem em 1996, foram descobertos casos de pornografia infantil pela internet. A partir daí temos o seguinte histórico: 1998- primeiros casos de clonagem de cartão; 2000 – primeiros casos de fraude bancária pela Internet; 2002 – Phishing: cavalo de tróia; 2009- Grande explosão de fraudes bancária através de clonagem de cartão de crédito e intetnet banking, desse último evento foi apurado pela Federação Brasileira de bancos um prejuízo estimado em um bilhão de dólares; 2011- ataques a páginas eletrônicas do governo brasileiro como por exemplo IBGE e Receita Federal.

Vejamos, segundo o entendimento da Patrícia Peck, a Ciência Jurídica é a responsável por equilibrar a relação comportamento-poder, o que só pode ser feito com a interpretação adequada das realidades sociais, criando normas que garantam a segurança esperada por meio da eficácia e aceitação, dessa forma é possível compreender e abarcar a mudança através de uma estrutura flexível que poderá ser sustentada no correr do tempo.

É a partir desse entendimento que caminhamos para o ramo que hoje é conhecido por Direito Digital. Contudo, a Ciência Jurídica não consegue acompanhar a tecnologia pelo fato de que, esta, por constante evolução, sempre estará a sua frente. Sendo assim, sempre haverá uma lacuna na regulamentação jurídica, visto que esta última é impossibilitada de dar uma resposta rápida por depender de uma adequada interpretação da realidade social, que hoje é modificada a passos largos.

É no desencontro da evolução tecnológica que surge o espaço para os crimes e delitos virtuais, assim urge a necessidade de nos protegermos com medidas legais para combater este tipo de delito. Prescinde ressaltar que o crime virtual possui característica de auto renovação e desenvolvimento, já que evolui juntamente com as tecnologias.

Para termos uma breve noção, a nível mundial, o primeiro registro de tutela jurídica do meio virtual surgiu com a Convenção de Budapeste, firmada pelo Conselho da Europa em 23 de novembro de 2001, entrando em vigor no ano de 2004. A convenção trazia nos seus quarenta e oito artigos a tentativa de uniformizar uma legislação que combatesse o cibercrime, uniformizasse terminologias e estabelecesse uma cooperação internacional.

Portanto, neste capítulo, o objetivo é entender como foi percebido pelo ordenamento jurídico brasileiro os crimes virtuais e delitos informáticos, e como foi desenvolvida a legislação penal informática. É necessário ressaltar que a pobreza de regulamentações do cenário virtual e as questões decorrentes requer do poder judiciário brasileiro a regulamentação através de decisões judiciais. Logo ficamos dependentes do caso concreto para passar a analisar a realidade virtual e suas modificações, esse cenário gera incertezas ao usuário pelo simples fato de que é perigoso e pouco prático visto que a velocidade com que a tecnologia e os delitos decorrentes do meio se modificam é muito maior que o tempo de resposta de uma decisão jurídica.

A primeira preocupação do legislador brasileiro com a interferência do mundo virtual no mundo real foi em 1990 com a criação do Código de Defesa do Consumidor e em 1995 foi publicada a norma 001 que tratava do uso dos meios da rede de telecomunicações para provimento e utilização de serviços de conexão à internet, esse foi o marco comercial da tecnologia no país.

A OAB em 1999 manifestou a primeira tentativa de regulamentação sobre os assuntos virtuais, onde criou uma comissão para apresentar um projeto de lei a ser proposto para o Congresso Nacional que versava sobre a regulamentação de comércio eletrônico, de forma mais específica sobre a validade do documento eletrônico e da assinatura digital.

Mundialmente, a preocupação em regulamentar o ciberespaço foi concretizada a partir da chamada Convenção de Budapeste, publicada em novembro de 2001 e que só foi aderida pelo Brasil em dezembro 2021. O objetivo da Convenção é facilitar a cooperação internacional para combater o cibercrime, a prioridade do tratado conforme o seu Preâmbulo é formar uma política criminal comum para que seja possível proteger a sociedade contra a criminalidade no ciberespaço através de uma legislação adequada e de uma melhoria da cooperação internacional.

Pois bem, voltando ao ordenamento jurídico brasileiro, é a partir do ano de 2012 que o legislador inicia os debates sobre leis específicas do meio digital, assim tivemos a primeira publicação que é a Lei 12.735/2012. A referida lei tramitou no Congresso por mais de dez anos e ao ser publicada foi alvo de várias críticas no quesito sobre sua constitucionalidade.

Originalmente o projeto inicial dessa lei procurava dispor princípios, definições e criminalizar condutas de dano informáticos que alterariam o Código Penal, contudo, dentro do conteúdo aprovado tivemos somente um artigo que alterou o Código Penal, no que diz respeito aos crimes de preconceito de raça ou cor, e outro que alterou Código Penal Militar. Restou nítido que houve grande desvirtuamento do objetivo inicial do projeto, que trazia uma visão necessária ao ordenamento jurídico brasileiro e concentrou-se os esforços nas mudanças do Código Penal Militar quanto aos delitos em tempo de guerra.

A Lei 12.737/ 2012, conhecida como Lei Carolina Dieckmann, que diz respeito aos crimes contra a intimidade e os dados alheios, foi um produto da pressão sobre o legislador para que este criasse um tipo penal capaz de tutelar os dados informáticos. Assim sendo, a referida lei criou o delito de invasão de dispositivo informático simples, alterando o art. 154/CP e criando o art. 154-A com duas figuras. Alterou o art. 266/CP para “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, de informação de utilidade pública ou telemático”. E acrescentou ao art. 298/CP a expressão “falsidade de cartão”, equiparando o cartão de crédito ou débito a documento particular.

Em seguida, tivemos a promulgação da Lei 12.965/ 2014, conhecida como Marco Civil da Internet. Essa lei trouxe ao ordenamento pátrio as definições e expressões específicas que fazem parte do direito Informático, além disso, regrou circunstâncias de atuação do provedor e dos usuários, limitando ainda eventuais abusos que podem derivar do poder público, por fim, assegurou formalidades significativas para o Estado de Direito no contexto do Digital.

Já em 2020, temos a validade da lei 13.709/ 2018, a Lei Geral de Proteção de Dados que foi aprovada e promulgada no ano de 2018, mas só passou a valer em 2020. Esse dispositivo nasceu da inspiração do Regulamento Geral sobre a Proteção de Dados (RGPD), que é um pacote de medidas sobre proteção de dados regulado na União Europeia. Tal como a RGPD, o dispositivo brasileiro é uma medida para tutelar especificamente a proteção de dados dos usuários e estabelecer algumas definições necessárias como a definição de dados sensíveis, constantes no art. 5°, II da lei 13.709/218. A vista disso, a LGPD trouxe obrigatoriedade de tratamento de dados somente para fins legítimos específicos explícitos, sem possibilidade de tratamento posterior de forma incompatível com o estabelecido no dispositivo legal.

E por último, no ano de 2021, tivemos as maiores alterações na legislação brasileira digital que foram:

1- A aderência do brasil a Convenção de Budapeste, que demorou 20 anos para acontecer e agora o Estado brasileiro tem uma grande oportunidade para gerar discussões sobre a melhoria da legislação quanto a regulamentação do ciberespaço e da legislação das matérias afins ao assunto.

2- A promulgação da Lei 14.155/2021- que trata sobre os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, e trouxe alterações para: o artigo 154-A do CP, promovendo um progresso relativo para o Direito Penal Informático ao expandir as possibilidades da invasão informática, mas ainda apresenta certa insuficiência legislativa na sua compreensão do delito informático ao se preocupar somente com a conduta de "ingressar sem autorização dispositivo informático alheio"; o artigo 171 do CP que teve acrescentado ao tipo penal o parágrafo 2°-A inserindo a fraude eletrônica; o parágrafo 2°-B inserindo causas de aumento para quem utilizar servidores fora do país sem analisar os riscos da virtualidade e por último ainda nesse dispositivo modificou o parágrafo 4° criando uma causa de aumento nas situações em que a vítima for idosa ou pessoa vulnerável; o artigo 70 do CPP incluindo o parágrafo 4° e por último acrescentou ao artigo 155, também do CPP, o parágrafo 4°-B e 4°-C.

3- A promulgação da Lei 14.197/2021- que trata sobre os crimes contra o Estado Democrático de Direito e modificou o artigo 359 do CP inserindo no ordenamento jurídico os seguintes tipos penais: Atentado a soberania; Atentado à integridade nacional; Espionagem; Abolição violenta do Estado Democrático de Direito; Golpe de Estado; Interrupção do processo eleitoral; Violência política; e Sabotagem.

É imprescindível citar a Resolução 423/2021 do CNJ que incluiu a disciplina de Direito Digital nos concursos públicos para ingresso na magistratura. Essa resolução traz para o Direito Digital maior peso e importância aos juristas brasileiros, visto que apesar de “novo” entender e estudar o meio Digital é extremamente importante vislumbrando que caminhamos para um futuro cada vez mais tecnológico.

Assim sendo, mesmo que a passos lentos para aprovar leis brasileiras sobre as implicações cibernéticas na sociedade, cabe relembrar que apesar de termos alguns tipos legais, é necessário sempre melhorá-los e modernizar cada vez mais todo o aparato legislativo, jurídico, policial e de colaboração para com outros países a fim de alcançarmos soluções cada vez mais atuais.

II - METAVERSO

Hoje entendemos a internet como um bem que possui valor central e que está em constante evolução. Não há o que se falar em um mundo desconectado, sem a internet e a virtualidade. É uma interação de diversas plataformas imersivas a expressão é usada para denominar um espaço virtual compartilhado, em que as pessoas poderão acessar usando óculos de realidade virtual, óculos de realidade aumentada e outros equipamentos. É um fato bem conhecido que a evolução da tecnologia atingiu sua velocidade de trem-bala nos anos 1900, quando a World Wide Web surgiu. Tecnologias como 3D e Realidade Virtual (VR) ganharam popularidade no mercado.

Apesar de todos os desenvolvimentos, o Metaverso fez sua primeira aparição apenas em 1992, quando Neil Stevenson destacou o conceito de realidade virtual através dos personagens de seu romance 'Snow Crash'. Ainda no início dos anos 90, uma empresa chamada Sega lançou soluções de jogos de realidade virtual, como o SEGA VR-1, para oferecer uma experiência de jogo envolvente aos jogadores de fliperamas. Todas essas invenções podem ser vistas como o impulso inicial para a próspera indústria do Metaverso que vemos hoje.

Metaverso estava crescendo lenta e constantemente, mas então 'algo' aconteceu que trouxe a tecnologia para o campo mainstream. Isso foi o Facebook mudando seu nome para 'Meta' em uma tentativa de mostrar seu foco recém-desenvolvido no setor. No ano passado, quando a gigante da mídia social se renomeou como Meta, o CEO Mark Zuckerberg confirmou seus planos de expandir a marca para tecnologias da nova era, como Metaverso, NFTs.

Para reuniões, jogos que já usado a mais tempo por exemplo, como o popular The Sims, onde a pessoa pode criar uma vida inteira para seu avatar(personagem). O mundo passou por grandes mudanças e todo o universo online da informação contribuiu para disseminar informações globais resultando em questões jurídicas que nunca foram encontradas até agora. Nunca, na história, a vida privada ou empresarial, teve uma exposição tão grande.

Traz a reflexão:

> *"[...]MUITO AINDA SE FALA EM GERAÇÃO X, GERAÇÃO MILLENIALS (OU GERAÇÃO Y) E GERAÇÃO Z. MAS HOJE JÁ EXPERIMENTAMOS EM NOSSA SOCIEDADE UMA NOVA GERAÇÃO: A GERAÇÃO C², DE "CONECTADA". SÃO AS PESSOAS QUE NUNCA VIVERAM SEM QUE ESTIVESSE CONSTANTEMENTE CONECTADAS NA VIRTUALIDADE. PESSOAS PARA AS QUAIS O NORMAL É CONVIVER COM UMA PARTE MATERIAL E UMA PARTE IMATERIAL DE SUAS VIDAS. [...]" (SYDOW, 2021, P. 21 - 22).*

2.1 REALIDADE VIRTUAL E REALIDADE AUMENTADA E IA

Metaverso é um termo usado para descrever um ecossistema que combina realidade virtual e realidade mista para oferecer interações em tempo real entre pessoas. Ele compreende conceitos de realidade virtual, realidade aumentada e IA para ajudar os usuários a se envolverem em experiências imersivas. A tecnologia libera o potencial de um ambiente simulado da vida real, onde as pessoas podem conversar, trabalhar e se divertir usando óculos, fones de ouvido, controladores e recursos relacionados especializados, os participantes usam avatares digitais como seus representantes para construir uma comunidade no espaço virtual. Os usuários navegam pelo Metaverso usando comandos de voz, movimentos oculares ou controladores.

O headset RV ou RA faz com que o usuário mergulhe no mundo virtual por meio da simulação de sensações físicas. Isso faz com que os usuários sintam que tudo o que estão vendo ou experimentando na configuração virtual é real e estão gostando de estar lá. Jogos como Horion Worlds, Rec Room são alguns dos exemplos populares de aplicativos Metaverso. Metaverso se esforça para criar um espaço virtual independente dos elementos físicos do mundo real usando tecnologias modernas. O ecossistema permite que as pessoas se socializem e interajam em uma infinidade de experiências virtuais. Usando a economia digital integrada do Metaverso, os usuários podem se entregar a um mundo de entretenimento, experiência e

ganhos. Os usuários podem armazenar seus ativos virtuais em uma carteira metaverso e ter a certeza da segurança de seus fundos.

O debate em torno do metaverso ter crescido recentemente e uma preocupação com sua segurança, o conceito não é exatamente novo o nome metaverso foi usado pela primeira vez no livro “Snow Crash”, do escritor Neal Stephenson, publicado em 1992. O metaverso é um universo virtual, onde cada pessoa possa ser, fazer e construir o que quiser através de um avatar com características físicas, circunferência, peso e altura. Essa é uma definição que se encaixa perfeitamente no metaverso, termo que, desde o fim de 2021, se tornou cada vez mais popular. O metaverso ganhou status de revolução tecnológica em outubro de 2021, logo depois que Mark Zuckerberg criador do Facebook anunciou que a empresa mudaria seu nome para META. Declarou também que o foco da companhia passaria a estar no mercado de realidade virtual (VR) e de realidade aumentada (VA).

Não é possível descrever com exatidão como o metaverso vai funcionar na prática, já que ele ainda não existe na forma que o fundador do Facebook (agora Meta) o descreveu. O que se sabe é que todos os usuários teriam os seus próprios avatares e poderiam trabalhar, manter contato com amigos, construir e decorar uma casa, comprar roupas e acessórios, ir a shows e até fazer viagens. Tudo de maneira virtual. A realidade virtual (VR, na sigla em inglês) é um ambiente em 3D, criado por computadores, que simula o mundo real e permite a total interação dos participantes. Para acessar essa tecnologia atualmente é preciso usar óculos especiais equipados com fones de ouvido e controladores.

A realidade aumentada (RA) combina aspectos dos mundos virtual e físico. Diferentemente do RV, a realidade aumentada insere elementos virtuais no mundo real. Um dos maiores exemplos de VA (sigla em inglês para realidade aumentada) é o jogo Pokémon Go, em que as pessoas podem jogar usando as câmeras dos smartphones para capturar as criaturas virtuais em um mapa baseado no mundo real. Existem ainda óculos especiais que mostram informações nas lentes.

> *“METAVERSO é O NOME USADO PARA DENOMINAR UM AMBIENTE VIRTUAL IMERSIVO, COLETIVO E HIPER-REALISTA, ONDE AS PESSOAS PODERÃO CONVIVER USANDO AVATARES CUSTOMIZADOS EM 3D. EM OUTRAS PALAVRAS, ELE É UMA EVOLUÇÃO DA NOSSA INTERNET ATUAL.”*

Para entender melhor o conceito de metaverso, compare com a internet de hoje. Atualmente, as redes sociais são as principais mediadoras do ambiente virtual. E a "vida digital" é acessada com celulares e computadores. Com o metaverso, a experiência será muito mais imersiva. Mais do que navegar na internet, será possível vivenciá-la por dentro. Na prática, ao colocar os óculos de realidade virtual, equipados com fones de ouvido e sensores, será possível entrar um mundo virtual online que também incorpora realidade aumentada, avatares holográficos 3D, vídeos e outros meios de comunicação. Ou seja, como se trata de espaços fictícios, o céu é o limite e tudo é possível de ser inventado.

2.2 SETOR EMPRESARIAL

As empresas que estão investindo nesse tipo de tecnologia afirmam que todas as pessoas poderiam interagir, aprender, colaborar e jogar nos espaços do metaverso. Tudo isso de uma maneira muito mais completa do que se pode imaginar hoje. Imagine que as reuniões virtuais de trabalho e lives de artistas que se popularizaram na pandemia poderiam acontecer em um espaço virtual, com muito mais interação, e sem sair de casa. Poder fazer reuniões de trabalho dentro do metaverso é uma das principais apostas de empresas de tecnologia como o Facebook e a Microsoft. Nesse universo virtual, seria possível simular reuniões presenciais, manter contato visual com avatares e interagir de maneira mais intensa com os colegas. Aprender de maneira mais imersiva é outro objetivo do metaverso. Seria possível promover aulas dentro do mundo virtual, com uma experiência mais engajadora para os alunos. Para cursos como medicina, daria para estudar o corpo humano com hologramas tridimensionais. Até mesmo cirurgias e tratamentos de doenças à distância poderiam ser feitos no metaverso, como afirmou a CEO da Microsoft no Brasil, Tânia Cosentino, em uma entrevista recente. Muitos negócios poderiam ser concretizados dentro do metaverso. Especialistas acreditam que uma economia completa poderia existir dentro do mundo virtual, com transações de terras, imóveis, serviços, transporte, arte digital e muito mais.

> *AS OPORTUNIDADES DO METAVERSO SÃO INFINITAS, NA OPINIÃO DE TÂNIA COSENTINO "METAVERSO É O FUTURO, É UMA TRANSFORMAÇÃO BRUTAL QUE VAI TRAZER DEZENVOLVIMENTO TECNOLÓGICO. É UM MUNDO QUE ESTÁ SÓ COMEÇANDO. VAI*

> *TRANSFORMAR A ÁRE DA MEDICINA, PROGRAMAÇÃO(TENOLOGIA), EDUCAÇÃO (EXPERIÊNCIA MAIS ENGAJADORA DO ALUNO). ESTAMOS NO INICIO DA JORNADA" CEO DA MICROSOFT (Agência EY, 13 de dezembro de 2021)*

Além do Facebook, que mudou o nome para Meta como forma de confirmar seu foco nesse mercado, a Microsoft é outra gigante dedicada aos universos virtuais. A criadora do Windows pretende construir um "metaverso empresarial". Outra iniciativa da empresa envolve o console de videogame Xbox, que estaria em um planejamento para criar uma "realidade mista", segundo Phil Spencer, responsável pelo produto. A empresa Epic Games, dona do jogo Fortnite, também está desenvolvendo projetos para o metaverso, que em breve poderão ser incorporados ao game. A Snap, controladora da rede social Snapchat, anunciou que vai construir óculos de realidade aumentada. A Nvidia, fabricante de chips, anunciou a criação da Nvidia Omniverse. Já a Nike criou a Nikeland.

> *NA UTOPIA PENSADA PARA O METAVERSO, TODOS ESSES MUNDOS VIRTUAIS SERIAM INTERCONECTADOS. SERIA POSSÍVEL, POR EXEMPLO, TRANSITAR LIVREMENTE ENTRE ELES. OU ATÉ COMPRAR UMA ARTE VIRTUAL EM UM MUNDO E EXIBI-LA EM OUTRO.*

2.3 SETOR DE ENTRETENIMENTO

O Metaverso está se expandindo rapidamente. Onde antes era limitado a projetos de jogos, hoje a tecnologia se tornou uma parte inevitável de reinos industriais de bilhões de dólares. Sua aplicação é amplamente apreciada no setor de esportes, mundo do entretenimento, campo de negócios, etc. Marcas e produtores musicais globais estão mudando para o Metaverso para sediar shows e interagir com os fãs. Clubes esportivos populares como o Manchester City estão construindo estádios virtuais para os amantes do esporte desfrutarem de suas partidas favoritas no conforto de suas casas. O Metaverso abre oportunidades para marcas e celebridades lançarem suas mercadorias oficiais para os fãs comprarem.

Entretenimento no metaverso está ganhando muito interesse, particularmente de consumidore s mais jovens que são susceptíveis de impulsionar o crescimento do metaverso.

A série de concertos de Ariana Grande em 2021 dentro do universo de jogos Fortnite e eventos similares sugerem como um metaverso proporcionará novas experiências imersivas de entretenimento os grandes nomes Justin Bieber, Marshmello e Travis Scott também exploraram o entretenumento metaverso.

Importante dizer que este cenário ainda não é totalmente possível. Muitas das tecnologias necessárias para que o metaverso se torne real ainda precisam ser desenvolvidas. Equipamentos como óculos de realidade virtual precisam se tornar mais acessíveis à população em geral. A ideia é que o metaverso vá muito além dos jogos, oferecendo experiências completas de entretenimento. Elas incluem shows, filmes, televisão, esportes e também videogames.

Mas também poderiam embarcar em viagens, obras de arte e muito mais. Até mesmo cassinos dentro do ambiente do metaverso poderiam ganhar vida. E os usuários poderiam fazer apostas com criptomoedas. O rapper Travis Scott, a cantora Ariana Grande e o DJ Marshmello já fizeram shows virtuais dentro do jogo de videogame Fortnite, da empresa Epic Games. Em abril de 2020, cerca de 12 milhões de pessoas se reuniram em tempo real para assistir ao lançamento de uma música de Scott. Eventos como esse, portanto, seriam comuns no metaverso.

2.4 SETOR IMOBILIÁRIO

Compras de terrenos virtuais: Adquirindo terras virtuais em algum metaverso você pode alugá-las ou vendê-las no futuro. Também é possível construir um imóvel por lá e capitalizá-lo de diversas maneiras, assim como fazemos no mundo físico. Em novembro, um terreno virtual de 566 metros quadrados de um game foi vendido por US$ 2,4 milhões em criptomoedas. Tokens dos principais games relacionados ao metaverso ganham valor conforme o projeto desperto interesse entre seus usuários. Roupas, objetos, veículos, itens colecionáveis, obras de arte, tudo isso pode ser tokenizados. Investir em ações de empresas que apostam em

soluções e funcionalidades do metaverso, pode ser uma boa alternativa de investir nesse mundo também. Empresas como o Facebook/Meta já têm ações à venda.

Comprar criptomoedas associadas ao metaverso é outra maneira de investir nesse mercado. Decentreland (MANA), Sandbox (SAND) e Enjin Coin (ENJ) são algumas delas. Essas moedas digitais podem ser adquiridas por meio de empresas especializadas. Geralmente há taxas de saques e transferências. Apesar de existir há mais de uma década, o Metaverso ainda está em seu estágio primário de desenvolvimento. Há muito a ser explorado, decifrado e decodificado antes de finalmente progredirmos no campo.

Quando se trata de uma estrutura regulatória, o Metaverso falha miseravelmente, pois atualmente não há leis que possam ser diretamente anexadas a ele. Isso o torna um local de risco para aqueles que defendem a necessidade de regulamentos e leis para o bom funcionamento de uma indústria global. Para tornar as coisas um pouco melhores, o reino do Metaverso aceitou cumprir as leis gerais que se aplicam à web para trazer uma sensação de uniformidade, segurança e transparência em seu ecossistema. Nas dicas fornecidas abaixo, aprenderemos sobre as leis da Internet que se aplicam ao Metaverso e aos espaços virtuais relacionados.

2.5 PERIGOS / RISCOS

Assim como a internet em geral o metaverso também pode esconder perigos ao usuário e à sociedade, sendo alguns deles: assédio, violação de privacidade, circulação de informações falsas (fake news) e golpes financeiros. A privacidade das informações no metaverso é uma área de preocupação porque as empresas envolvidas provavelmente coletarão informações pessoais dos usuários por meio de dispositivos vestíveis e interações com os usuários. O metaverso pode se tornar um espaço de projeções pouco saudável. Isso porque um dos apelos do conceito é justamente ser um ambiente onde o usuário pode criar seu próprio avatar 3D, seja representando a si mesmo ou criando um personagem fictício -- o que poderia fazer com que pessoas com problemas de autoestima usem o ambiente para projetar uma "vida perfeita" impactando diretamente no psicológico desses usuários.

O vício do usuário e o uso problemático das mídias sociais são outra preocupação para o desenvolvimento do metaverso. O transtorno do vício em Internet , mídia social e vício em videogame podem ter repercussões mentais e físicas por um período prolongado de tempo, como depressão, ansiedade e obesidade. Os especialistas também estão preocupados que o

metaverso possa ser usado como uma 'fuga' da realidade de uma forma semelhante às tecnologias existentes da Internet.

O metaverso pode ampliar os impactos sociais das câmaras de eco online e dos espaços alienantes digitalmente.Uma vez que os desenvolvimentos do metaverso podem ser feitos para adaptar os mundos virtuais algoritmicamente com base nas crenças de cada pessoa, o metaverso pode distorcer ainda mais as percepções dos usuários sobre a realidade com conteúdo tendencioso para manter ou aumentar o envolvimento.

Para acessar o metaverso, é necessário um conjunto de acessórios e hardwares especializados para estabelecer ligações entre o usuário e o mundo virtual. Assim como acontece com celulares, esses novos aparelhos podem conter uma série de sensores capazes de armazenar dados dos usuários. Grandes volumes de informações podem ser vazados e usados indevidamente.

Violência: já há relatos de situações envolvendo assédio sexual e agressão no metaverso. Assim como em outros espaços virtuais, como em canais de games online, essas experiências têm encorajado comportamentos agressivos de alguns usuários que se sentem protegidos pelo anonimato da internet.Desinformação: A disseminação de notícias falsas já afeta as redes sociais atuais e pode aparecer no metaverso, aumentando a propagação delas e contribuindo para a desinformação da população.

O Facebook está planejando persistir em publicidade direcionada dentro do metaverso, levantando mais preocupações relacionadas à disseminação de desinformação e perda de privacidade pessoal. Se não for regulado corretamente, o metaverso pode funcionar como uma "terra de ninguém" e ser explorada por criminosos para roubar quantias de dinheiro, criptomoedas e dados pessoais dos usuários.

2.6 LEIS QUE REAGEM O METAVERSO

DIREITOS AUTORAIS

A lei de direitos autorais se esforça para fornecer proteção ao trabalho original de criadores, artistas e escritores. Quando falamos sobre o Metaverso, o estatuto incorpora conteúdo digital gerado pelo usuário, como avatares, imóveis virtuais e outras obras de arte. Plataformas como The Sandbox permitem que os usuários construam, desenvolvam e possuam áreas virtuais chamadas 'LANDS'. As pessoas estão gastando contas no valor de milhares de dólares para se apoderar de um pedaço dos bens imóveis do Metaverso. Com o

aumento da popularidade dos ativos digitais, a lei de direitos autorais torna-se significativa para o domínio do Metaverso.

O criador de um item protegido por direitos autorais tem o direito exclusivo de recriar, comercializar e exibir o trabalho para outros. Eles também podem autorizar outras pessoas a fazer o trabalho em seu nome. Se a pessoa autorizada violar a lei, o criador original pode processá-la por violação de direitos autorais. Se um artista criar conteúdo no Metaverso semelhante a um conteúdo protegido por direitos autorais no mundo físico, ele poderá ser responsabilizado por violação dos direitos autorais.

Por exemplo, se uma pessoa criou um avatar de um NFT semelhante a um avatar protegido por direitos autorais ou NFT, o proprietário dos direitos autorais pode processar o primeiro por violação. Eles podem buscar a ajuda do tribunal para impedir que a outra parte distribua os itens aos investidores. A parte inadimplente também pode ter que pagar pelos danos causados ao criador original.

LEIS DE PROPRIEDADE INTELECTUAL

A lei de PI preserva o direito dos criadores contra suas invenções, marcas registradas ou outras criações. Com o aumento da popularidade dos tokens não fungíveis , que são uma parte inevitável do espaço do Metaverso, a lei de propriedade intelectual tornou-se muito importante para uma governança adequada. As empresas de tecnologia competirão em breve para desenvolver ferramentas AR e VR mais avançadas, incluindo óculos de alta tecnologia, fones de ouvido, etc. Isso abrirá novas oportunidades para direitos de propriedade intelectual no setor, como novas patentes para software e dispositivos. Novas marcas surgirão abrindo caminho para novas marcas para os usuários do mundo virtual.

A criação de portais on-line aprimorados abrirá caminho para novas medidas de segurança de patentes e direitos autorais para invenções e jogos focados em software relacionados a blockchain e criptografia.

CONTRATO

No Metaverso, a lei contratual impõe a formação e execução de contratos feitos entre os usuários. Os acordos feitos aqui incorporam uma infinidade de atividades, como comércio de bens virtuais e aluguel de terras virtuais. Como qualquer outro contrato, um acordo no

Metaverso obriga ambas as partes a seguir os termos do pacto. Caso uma das partes não cumpra os termos do contrato, a outra parte tem o direito de processá-la por quebra de contrato.

Suponha que um usuário concorde em vender um produto virtual no Metaverso para outro usuário e entre em um contrato para o mesmo. No entanto, o comprador não efetua o pagamento do bem. Em seguida, o autor pode solicitar ao tribunal que busque o valor principal, bem como os danos do inadimplente.

DIREITO PENAL

A lei de responsabilidade civil dirige-se a danos civis, incluindo danos materiais e danos pessoais. No Metaverso, o estatuto rege qualquer atividade prejudicial causada pelos usuários a outros participantes. Isso pode incluir estresse emocional, agressões físicas e danos materiais. Por exemplo, se uma pessoa fere fisicamente outra pessoa dentro do ecossistema do Metaverso, esta última pode processar a outra por isso. A parte acusada será então forçada pela lei a pagar pelos ferimentos, despesas médicas e danos relacionados ao ato.

DIFAMAÇÃO

O estatuto protege as pessoas de falsas acusações e comentários prejudiciais de qualquer outra pessoa. No Metaverso, refere-se ao conteúdo gerado pelo usuário que é crítico de outra marca. Acusar alguém falsamente e prejudicar seu status social pode fazer com que o inadimplente seja acusado de acordo com a lei de difamação. Os programas de treinamento do metaverso geralmente fornecem conhecimento elaborado sobre as leis do metaverso para melhor compreensão sobre o assunto.

REGULAMENTAÇÃO DE NFTS E TRIBUTOS

Tokens não fungíveis no Metaverso estão sujeitos a regulamentações financeiras tradicionais, como leis de commodities, bancos e valores mobiliários. A forma como esses ativos são criados e as trocas podem estabelecê-los como contratos de investimento e, assim, colocá-los sob a alçada das leis de valores mobiliários. A emissão, empréstimo e negociação de criptomoedas no metaverso provavelmente aplicarão serviços bancários, transferência de dinheiro e outros regimes financeiros ao sistema.

A compra e venda de bens virtuais atrai implicações fiscais envolvendo os regimes de imposto sobre vendas e imposto de renda. As autoridades financeiras já trouxeram ativos virtuais ou criptomoedas sob o guarda-chuva tributário, tornando os lucros tributáveis para os assalariados. Isso faz com que os NFTs usados no Metaverso também atraiam implicações fiscais semelhantes às criptomoedas.

III PUNIBILIDADE E PREVENÇÃO

Até os dias atuais, o posicionamento do legislador brasileiro, versa no sentido de em todos os casos punir a conduta e a prática delitiva informática, o que de todo não está errado. Contudo, cabe trazer à discussão que dentro do ordenamento jurídico, o direito penal tem como princípio norteador a *Ultima ratio*, ou seja, teoricamente deveria ser a lei aplicada nos casos em que somente ela é capaz de evitar o ato ilícito ou de puni-lo à altura em que ofendeu ou lesou o bem jurídico. Nesse sentido, o Direito Penal, só deveria ser aplicado quando estritamente necessário, porém, conforme o ânimo e a pressão social, não é o que se verifica no cenário jurídico brasileiro. Percebemos que caminha o Direito Penal informático ao mesmo cenário, sendo utilizado como primeira solução aos embates virtuais que nossa sociedade enfrenta.

Foucault, em Vigiar e punir, mostra que a evolução das práticas punitivas demonstram ser o resultado de uma série de processos sociais, políticos, históricos e econômicos sobrepostos. Assim sendo, cada época e cada sistema de punição tem suas características inerentes e sua premissa de existência. A vista disso, a prisão cumpre um papel social que transcende o limite da punição ou correção do infrator. O comportamento do delinquente torna-se matéria prima do sistema industrial carcerário. Dessa forma uma legislação que está na maioria das vezes objetivada na punição de determinado ato, alimenta a forma mais comum de manifestação do poder nas instituições sociais modernas.

Não há o que se negar que é necessário uma cibecriminologia para compreender a nova modalidade de crime, o informático, a pessoa do infrator, da vítima e do controle social do comportamento delitivo. Conforme diz SYDOW (2022), há um novo perfil de delinquente que surgiu na rede, que se mostrou, por sua alta velocidade e multiplicidade, quiçá o mais importante meio de cometimento de delitos, pela simultaneidade e pela sofisticação necessária para sua investigação.

> *A LINGUAGEM MUDOU. AS PALAVRAS MUDARAM. O CRIME MUDOU. A CONCEPÇÃO DE UMA SOCIEDADE DE RISCOS VOLTOU POTENCIALIZADA, COMO BEM APRESENTADO POR PIERPAOLO CRUZ BOTTINI AO APRESENTAR SEU "PARADOXO DO RISCO" EM QUE TECNOLOGIAS SURGEM PARA COMBATER O DELITO, MAS SERVEM DE FERRAMENTAS TAMBÉM PARA O COMETIMENTO DE NOVOS DELITOS. POR SUA VEZ, NOVAS TECNOLOGIAS SURGEM PARA COMBATER ESSES NOVOS DELITOS E ASSIM O CICLO SE PERPETUA. (SYDOW.2022. P.734)*

Pois bem, a criminologia é essencial para compreendermos de forma completa todo o cenário do ciberespaço e os delitos nele inseridos. Para isso, é necessário um estudo profundo das tecnologias e a cada novo avanço uma reanalise do processo acadêmico. A imprescindibilidade de se estudar, explorar e debater o delito informático é para que, através disso, possamos permitir o Poder Público identificar espécies de usuários mais ou menos propensos a serem vítimas e agentes de delitos. (SYDOW, 2022).

O fato de o Brasil possuir uma legislação fraca, com pouca técnica e repressora, permite os altos índices de impunidade, o que diretamente impulsiona o aparecimento de novos delinquentes informáticos e ao surgimento de novos golpes. Em relação ao usuário brasileiro, nós representamos um número massivo de consumidores nas principais redes sociais da atualidade como Instagram, TikTok e Twitter. Contudo o entendimento dos riscos e de como se configura cada rede social é pequeno, o usuário geralmente tem pouca ou nenhuma noção de educação digital.

> *OUTRO FATO FUNDAMENTAL É O DE QUE APESAR DO BRASILEIRO SER AFIM DA TECNOLOGIA, APENAS RECENTEMENTE CRESCEU O ACESSO DA POPULAÇÃO À TAIS APARATOS, INICIANDO A QUEBRA DO DIGITAL DIVIDE (SEGREGAÇÃO ACERCA DOS EXCLUÍDOS DIGITAIS). OUTROSSIM, OS USUÁRIOS AINDA ENGATINHAM NA COMPREENSÃO DOS FUNDAMENTOS E RISCOS DA REDE.*
>
> *HÁ UMA VÍTIMA VIRTUAL DIFERENTE DA VÍTIMA DO MUNDO REAL. O USUÁRIO BRASILEIRO VIA DE REGRA NÃO TEM COMPREENSÃO BOA DA LÍNGUA INGLESA, QUE PREDOMINA O AMBIENTE ELETRÔNICO E ISSO FACILITA GOLPES EM TAL SEARA. (SYDOW.2022. P.740)*

Os indivíduos serão capazes de usar avatares para experimentar versões digitais de ro upas reais; treinar e praticar tarefas de trabalho complexas, como cirurgias de alto risco; e se e nvolver em experiências simuladas como mergulho no céu enquanto sentem as sensações físic as reais. Dessa forma, urge a necessidade de dispor ao usuário elementos suficientes de conhecimento para informatizá-los e gerar a consciência do que versa nos contratos de serviços informáticos, o que se disponibiliza, quais os riscos da atividade, qual o grau de exposição da imagem, tudo potencializado aos efeitos a longo prazo. É necessário criar uma sociedade que seja educada digitalmente para criar uma consciência informática e assim gerar uma prevenção primária. O usuário precisa entender que ele é responsável pelos dados que ele aceita inserir na rede, sendo conscientizado ainda pelas consequências e riscos que existe na rede. Logicamente, é mais prático modificar o comportamento do usuário, que é potencialmente uma vítima do delito informático, que modificar o comportamento do agente delitivo. Se conseguirmos trazer ao público, que tanto adora a interação virtual e as facilidades que a tecnologia proporciona a vida, a noção de que uma postura mais educada digitalmente colabora na prevenção do crime informático, provavelmente construiríamos uma sociedade mais consciente e menos vulnerável no ciberespaço. Portanto, tutelar sobre os delitos informáticos e tentar regular o ciberespaço isoladamente sem a conduta da educação digital, se mostra pouco eficaz contra o cibercrime. O ideal é alinhar o estudo da criminologia com o Poder Público e uma sociedade digitalmente educada para seja possível estabelecer um risco tolerável no ciberespaço.

CONCLUSÃO

O Metaverse está crescendo exponencialmente com o apoio constante de investidores e entidades empresariais. O mundo virtual faz com que os usuários desfrutem de experiências da vida real em um ambiente simulado com potencial incomparável de entretenimento e ganhos. As leis explicadas neste artigo ajudarão os leitores a obter uma imagem clara do que podem encontrar ao explorar o campo do Metaverso. Se você deseja aprender mais sobre o metaverso, o Blockchain Council pode ser seu melhor parceiro. A plataforma oferece uma ampla gama de programas de certificação metaverse.

A lista de cursos do metaverso disponível oferece conhecimento subjetivo e treinamento prático aos usuários. A expansão da era digital, modificou os padrões sociais e impactou diretamente no modo como vivemos. A tecnologia permitiu a cada dia o surgimento de um novo fato prático provocando as autoridades e órgãos julgadores a tutelarem sobe um

novo bem jurídico que surgiu a partir do uso da internet. Surge a necessidade, no atual momento, da criação de uma legislação e de todo um aparato para regulamentar o meio ambiente digital, proteger e educar os usuários, a fim de que se construa uma estrutura onde se puna os delitos informáticos e se forme uma sociedade educada digitalmente gerando uma maior consciência a respeito do uso da internet.

O mundo virtual trouxe e continua trazendo, ao passo que se atualiza, novos conflitos e novas tipificações delitivas que possuem características não pensadas dentro da realidade que nos encontramos. Com essa nova realidade, tipos penais, territorialidade, bem jurídico, jurisdição e competência precisaram ser reinterpretados sob novos desdobramentos do Direito identificados dentro do direito informático. Nesse sentido, este trabalho propôs um pensamento maduro e sistemático objetivando a solução do problema aqui discutido, pretendendo falar não somente da punição do criminoso digital, mas a trazer a noção de que uma postura mais educada digitalmente colabora na prevenção do crime informático. Atualmente, na legislação brasileira já existem alguns tipos legais em relação as

de impunidade que diretamente impulsiona o aparecimento de novos delinquentes informativos e o surgimento de novos golpes.Portanto, foi a partir dessa realidade que se pensou o presente trabalho com a intenção de demostrar a importância do Direito digital e de problematizar o surgimento de possíveis novos comportamentos delitivos para que se preserve a harmonia da sociedade informatizada. Não há o que se negar que a virtualização das coisas provoca modificações sociais imediatas, assim sendo, requer-se da sociedade jurídica uma maior atenção ao tema de forma a promover um equilíbrio entre a sociedade e o ambiente digital.

DIGITAL CRIMESB IN THE METAVERSE ERA IN BRAZIL

ABSTRACT

This work, theoretical in nature, aims to analyze the scenario of cybercrimes and the performance of the Brazilian State on cybercrimes, as well as to understand the issues to the digital world and the importance of digital education. The research begins by unraveling elements of the virtual environment and explaining concepts such as network, IP, microprocessor. After the concepts, the importance of the virtual world as an essential tool is discussed today and anonymity in the virtual environment is analyzed, explaining the "layers" of the internet, being surface web, deep web, and dark web. After analyzing the virtual world, the research brings up the debate of what are virtual crimes and computer crimes and how Brazilian legislation provides for them, complementing bringing a focus to the importance of expertise in cases of virtual crimes. Finally, it is debated within cybercriminology whether the best path to be chosen for solving crimes would be punishment or prevention, deepening research into the field of prevention with digital education.

Keywords: cybercrimes; digital; education; law; Internet.

REFERÊNCIAS

ARAUJO, Yuri Saramago Sahione de. **Adesão à Convenção de Budapeste sobre o crime cibernético é importante, mas também impõe desafios ao Brasil.** Disponível em: https://www.migalhas.com.br/depeso/357721/adesao-a-convencao-de-budapeste-sobre-o-crime-cibernetico-e-desafios. Acesso em: 05 de abril de 2022.

ARAUJO, Luís Guilherme N. de. **Resenha Vigiar e punir: poder, punição, disciplina e indústria.** São Paulo: Editora Primeiros Escritos. 2018.

BARRETO, Alessandro Gonçalves. **Cibercrimes e seus reflexos no Direito brasileiro**. 2 ed. rev. e. atual. São Paulo: Editora JusPodivm, 2021.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. **Combate ao Crime Cibernético**. 1. ed. Rio de Janeiro: Mallet Editora, 2020.

BUDAPESTE. **Convenção sobre o Cibercrime,** 2001**.**Hungria: Conselho da Europa. Disponível em: https://rm.coe.int/16802fa428. Acesso: em 05 de abril de 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso: em 05 de abril de 2022.

BRASIL. **Lei N° 8.078, de 11 de setembro de 1990.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 12.735, de 30 de novembro de 2012.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 12.965, de 23 de abril de 2014.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 13.7019, de 14 de agosto de 2018.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 14. 155, de 27 de maio de 2021.** Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm?msclkid=5041b729c69011eca04eb0ba2b483db0. Acesso em: 06 de abril de 2022.

BRASIL. **Lei N° 14.197 de 1 de setembro de 2022.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm. Acesso em: 06 de abril de 2022.

BRASIL. **Resolução Nº 423.** Brasília, DF: Presidência da República, 2021. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4147. Acesso em 06 de abril de 2022.

Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em: 04 de abril de 2022.

FERREIRA, Poliana Agostinho Calheiros; COELHO, Vânia Maria Bemfica Guimarães Pinto. **Crimes Virtuais.** Varginha: FADIVA,2014. E-book. Disponível em: http://www.fadiva.com.br/documentos/jusfadiva/2014/18.pdf. Acesso em: 06 de abril de 2022.

LEMOS, Ronaldo**. REVISTA OBSERVATÓRIO ITAÚ CULTURAL**.N-16. Jan/Jun 2014. São Paulo: Itaú Cultural.2007. ISSN 1981-125X versão online. Disponível em: https://itsrio.org/wp-content/uploads/2017/01/OBSERVATORIO16_0.pdf. Acesso em: 30 de out. de 2021. (perguntar se pode usar o nome do editor).

O que são bots? - definição e explicação. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-are-bots. Acesso em: 04 de abril de 2022.

RODRIGUES, Marco Antonio; TAMER, Maurício. **Justiça digital: O Acesso à Justiça e as Tecnologias da Informação na Resolução de Conflitos**. São Paulo: Editora JusPodiv, 2021.

SABINO, Marco Antônio da Costa. **Afinal, existe mesmo anonimato na internet.** Disponível em: https://fia.com.br/blog/anonimato-na-internet/.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A Convenção de Budapeste e as leis Brasileiras.** João Pessoa: UFPB, 2009. E-book. Disponível em: https://www.charlieoscartango.com.br/Images/A%20convencao%20de%20Budapeste%20e%20as%20leis%20brasileiras.pdf. Acesso em: 06 de abril de 2022.

SYDOW, SPENCER TOTH. **Curso de Direito Penal Informático**. 2. ed. rev. e. atual. Salvador: Editora JusPodivm, 2021.

SYDOW, SPENCER TOTH. **Curso de Direito Penal Informático**. 3. ed. rev. e. atual. Salvador: Editora JusPodivm, 2022.

TANENBAUM, Andrew S.; WETHERALL, David J.; **Rede de Computadores**. 5. ed. Person Education, 2017. E-book.

VIANA, Gabriela. **O que é um Host**?. Disponível em: https://www.techtudo.com.br/noticias/2012/02/o-que-e-um-host.ghtml. Acesso em: 17 de nov. de 2022.

Agência EY . **Entenda o que é metaverso e como vai funcionar a "nova internet**?. Disponível em: https://www.ey.com/pt_br/agencia-ey/noticias/entenda-o-que-e-metaverso-e-com-vai-funcionar-a--nova-internet-. Acesso em: 08 de dez. de 2022.

CASTRO, Johnatan. **Metaverso: o que é esse novo mundo virtual**?. Disponível em: https://blog.nubank.com.br/metaverso-o-que-e/ . Acesso em: 27 de nov. de 2022.

BAPTISTA, Rodrigo. **Lei com penas mais duras contra crimes cibernéticos é sancionada.** Disponível em: https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada . Acesso em: 27 de nov. de 2022.

MALAR, João. **Entenda o que é o metaverso e por que ele pode não estar tão distante você.** Disponível em: https://www.cnnbrasil.com.br/business/entenda-o-que-e-o-metaverso-e-por-que-ele-pode-nao-estar-tao-distante-de-voce/ . Acesso em: 27 de nov. de 2022.

COZZI, Paola. **Quali opportunià di crecita per il mercato globale dela cyber security**?. Disponível em: https://tech4future.info/mercato-cyber-security-2023/. Acesso em: 27 de nov. de 2022.

VERMA, Smita. **What Laws Govern The Metaverse**?. Disponível em: https://www.blockchain-council.org/metaverse/what-laws-govern-the-metaverse/#:~:text=If%20an%20artist%20creates%20content,sue%20the%20former%20for%20infringement. Acesso em: 27 de nov. de 2022.

TUCCI, Linda. **What is the metaverse**?. Disponível em: https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know. Acesso em: 27 de nov. de 2022.

MACHADO, Simone. **Mataverso: como participar do ´futuro da tecnologia´**?. Disponível em: https://www.uol.com.br/tilt/faq/metaverso-o-que-e-como-entrar-e-mais.htm?cmpid=copiaecola. Acesso em: 27 de nov. de 2022.