

**VI ENCONTRO VIRTUAL DO
CONPEDI**

DIREITO CIVIL CONTEMPORÂNEO I

THAIS JANAINA WENCZENOVICZ

IARA PEREIRA RIBEIRO

CILDO GIOLO JUNIOR

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Napolini - UNIVEM/FMU - São Paulo

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade - UNIMAR/FEPODI - São Paulo

Conselho Fiscal:

Prof. Dr. Caio Augusto Souza Lara - ESDHC - Minas Gerais

Prof. Dr. João Marcelo de Lima Assafim - UCAM - Rio de Janeiro

Prof. Dr. José Filomeno de Moraes Filho - Ceará

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Prof. Dr. Valter Moura do Carmo - UNIMAR - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Daniela Marques De Moraes - UNB - Distrito Federal

Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM - São Paulo

Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie - São Paulo

Comunicação:

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - Paraíba

Prof. Dr. Matheus Felipe de Castro - UNOESC - Santa Catarina

Relações Internacionais para o Continente Americano:

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Relações Internacionais para os demais Continentes:

Prof. Dr. José Barroso Filho - ENAJUM

Prof. Dr. Rubens Beçak - USP - São Paulo

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicritiba - Paraná

Eventos:

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - Minas Gerais

Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC - Paraná

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - Mato Grosso do Sul

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UMICAP - Pernambuco

D597

Direito civil contemporâneo I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Cildo Giolo Junior; Iara Pereira Ribeiro; Thais Janaina Wenczenovicz – Florianópolis; CONPEDI, 2023.

Inclui bibliografia

ISBN: 978-65-5648-726-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito civil. 3. Contemporâneo. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34



VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO CIVIL CONTEMPORÂNEO I

Apresentação

O GT DIREITO CIVIL CONTEMPORÂNEO I do VI Encontro Virtual do CONPEDI realizado em junho de 2023 abordou temas clássicos do direito privado, como propriedade, negócio jurídico, capacidade civil, contratos e bens revisitados pela perspectiva hodierna do Direito Civil, demonstrou o impacto da tecnologia, inclusão, solidariedade e globalização sem deixar de lado o rigor técnico conceitual e o apuro metodológico na produção da pesquisa dos artigos.

A devida publicação dos Anais do GT DIREITO CIVIL CONTEMPORÂNEO contém 12 artigos que apontam caminhos para o aprofundamento dos estudos civilistas no Brasil.

O primeiro artigo intitulado LÉON DUGUIT E O DIREITO DE PROPRIEDADE: CONTRIBUIÇÕES PARA O TEMA de Jorge Aurênio Ribeiro Júnior aborda o direito de propriedade e sua função social de acordo com os postulados definidos pelo jurista Léon Duguit. Como contribuições ao debate atual sobre propriedade, o artigo destaca que a propriedade não pode ser vista como um fim em si mesmo e que possui como característica marcante a solidariedade social; trata do evolucionismo positivista e suas consequências para a propriedade; e aponta que a análise da propriedade como um fato social pode conduzir a reducionismos que retiram seu sentido valorativo.

A reflexão seguinte sobre A FUNÇÃO SOCIOAMBIENTAL DA MULTIPROPRIEDADE E A ANÁLISE JURÍDICO-AMBIENTAL ACERCA DO MODELO MAIS LONGEVO DO BRASIL com autoria de Rannia Tameirão Oliveira, Johan Guilherme Alvino Pontes e Flavia de Paiva Medeiros de Oliveira analisa o instituto da multipropriedade como modalidade especial de condomínio instituído pela Lei nº 13.777/2018 que alterou o art. 1.358 do CC para incluir as alíneas a a u e apresenta o estudo do modelo multiproprietário Paúba-Canto Sul no município de São Sebastião, considerado o mais antigo do Brasil com mais de 60 anos de existência, comprovando a hipótese de que o parcelamento temporal multiproprietário reduz impactos ambientais, atende às funções econômicas e socioambientais, democratiza a aquisição da segunda moradia no Brasil, e ajuda a promover o desenvolvimento sustentável, sendo possível instituir o regime de multiproprietário nas unidades imobiliárias já existentes. Conclui que a multipropriedade é um paradigma racional para o uso de recursos socioambientais e viável sob o aspecto econômico.

O terceiro texto sob o título RECONHECIMENTO DE PERSONALIDADE JURÍDICA DE PESSOA JURÍDICA DE DIREITO PRIVADO AOS CONDOMÍNIOS EDILÍCIOS de Luciano Monti Favaro analisa o Projeto de Lei n. 3.461, de 2019, já aprovado no Senado Federal, que intenta atribuir personalidade jurídica aos condomínios edilícios, considerando-o como pessoa jurídica de direito privado. O artigo conclui que o projeto representa um avanço e pode resultar em solução de problemas enfrentados por esses condomínios, mas que, entretanto, poderá resultar novos debates jurídicos como, por exemplo, a possibilidade de aplicação da teoria da desconsideração da personalidade jurídica em caso de abuso da personalidade pelo condomínio edilício.

Na sequência o artigo O PARADIGMA CLÁSSICO DO NEGÓCIO JURÍDICO REVISITADO PELO DIREITO CIVIL-CONSTITUCIONAL CONTEMPORÂNEO com autoria de Guilherme Augusto Giroto, Daniela Braga Paiano, Arthur Lustosa Strozzi parte de considerações sobre como o negócio jurídico e o contrato emergiram no período de dominância do liberalismo como uma forma de conferir segurança jurídica à transmissão de propriedade e à circulação de riquezas para apontar que ao se instalar Estados Democráticos de Direito, com constituições que colocam a pessoa como eixo central, foi necessária uma releitura das relações privadas. O artigo pretende, desta forma, verificar num primeiro momento os preceitos clássicos destes institutos, e, em seguida, traçar quais preceitos constitucionais podem ser aplicados, revisitando esses dois institutos (negócio jurídico e contrato) sob o paradigma civil-constitucional.

O artigo REPERCUSSÕES NA CAPACIDADE DA CRIANÇA E DO ADOLESCENTE COM O ESTATUTO DA PESSOA COM DEFICIÊNCIA de Lucas Fagundes Isolani e Andressa Kézia Martins busca examinar as mudanças na teoria das (in)capacidades em razão do Estatuto da Pessoa com Deficiência para discutir as repercussões quanto a capacidade das crianças e dos adolescentes a partir da obra cinematográfica Uma Lição de Amor. O artigo também analisa a “Competência Gillick” do ordenamento jurídico inglês, que estabelece critérios para determinar se a criança ou o adolescente possui discernimento para decidir os atos de sua vida civil, com a autonomia dos jovens no ordenamento jurídico brasileiro.

No mesmo tema, o artigo A (DES)NECESSIDADE DA REINTERPRETAÇÃO DA INCAPACIDADE CIVIL ABSOLUTA PELO CRITÉRIO CRONOLÓGICO RÍGIDO de Larissa Lassance Grandidier propõe, por meio de pesquisa bibliográfica, que o melhor entendimento do dispositivo legal que restringe a capacidade civil de forma absoluta para crianças e adolescentes com idade inferior a 16 anos (art. 3º do CC) seja restringi-lo aos atos extrapatrimoniais para que seja preservada seus direitos da autonomia e liberdade nos atos personalíssimos.

Sobre autonomia privada, também discorreram Ana Clara da Silva Ortega e Galdino Luiz Ramos Junior no artigo O PRINCÍPIO DA FUNÇÃO SOCIAL DOS CONTRATOS E A NECESSIDADE DE LIMITAÇÃO DA AUTONOMIA PRIVADA: ANÁLISE DO CONTEXTO DA LEI DE LIBERDADE ECONÔMICA ao examinarem o papel limitador do princípio ao conceito de autonomia e sobressalente à Lei de Liberdade Econômica.

As incitações trazidas pela tecnologia foram objetos de três artigos. Os autores Éfren Paulo Porfírio de Sá Lima e Alisson Santos Rocha em O REGIME DE PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS NO BRASIL analisaram o tema a partir de estudos sobre o direito à privacidade para afirmar que existe um regime jurídico específico de proteção de dados pessoais sensíveis em prevalência ao regime geral e que esse sistema está presente em outros ordenamentos na Europa e no Estados Unidos. Os autores Bruno Santos Lima, Sebastião Patrício Mendes da Costa e Deborah Dettmam Matos se debruçaram sobre OS NOVOS DESAFIOS DA JURISDIÇÃO NO MUNDO VIRTUAL E A HERANÇA DIGITAL realizando uma reflexão acerca da judicialização e da atuação do poder judiciário frente à suposta ausência de legislação específica para regulamentar as relações no ambiente virtual e suas consequências post mortem. Já Matheus Massaro Mabtum, José Ricardo Marcovecchio Leonardeli e Natália Peroni Leonardeli no artigo O METaverso E SEUS REFLEXOS JURÍDICOS analisam os desafios legais que envolvem esse ambiente virtual, ao qual por meio de avatares, os usuários interagem entre si e como essa interação pode impactar as pessoas fora do ambiente virtual deve ser objeto de regulação governamental.

O artigo O ENFRAQUECIMENTO DO ESTADO NO CONTEXTO DA GLOBALIZAÇÃO sob autoria de Horácio Monteschio, Luiz Gustavo do Amaral e Lucas Leonardi Priori realizou estudo sobre as mudanças trazidas pelo compliance e os acordos de leniência em práticas corruptivas nas atividades das empresas privadas e a participação do Estado frente a essas mudanças globais. Por fim, o artigo DIREITO CIVIL NA CONSTITUIÇÃO SOCIAL-SOLIDARISTA: BREVES APONTAMENTOS de Jason Soares de Albergaria Neto e Luiz Henrique Murici se debruça sobre o debate entre o viés social e o viés econômico-liberal do direito no âmbito da constitucionalização do direito civil.

Excelente leitura!

Thais Janaina Wenczenovicz / Universidade Estadual do Rio Grande do Sul e PPGD UNOESC.

Iara Pereira Ribeiro / Faculdade de Direito de Ribeirão Preto - Universidade de São Paulo - USP.

Cildo Giolo Junior / Universidade do Estado de Minas Gerais.

O METAVERSO E SEUS REFLEXOS JURÍDICOS

THE METAVERSE AND ITS LEGAL REFLECTIONS

Matheus Massaro Mabtum ¹
José Ricardo Marcovecchio Leonardeli ²
Natália Peroni Leonardeli ³

Resumo

Em um mundo em transformação digital, a palavra metaverso é cada vez mais ouvida. Este termo é usado para se referir a um ambiente virtual compartilhado ao qual podemos nos conectar por meio de dispositivos especiais para interagir com outras pessoas por meio de avatares. Este universo, que oferece oportunidades onde a presença física será cada vez mais dispensável, continua a crescer dia a dia. O presente estudo tem como objetivo analisar quais são os desafios legais que envolvem o Metaverso. De modo específico este trabalho busca: evidenciar a importância da Revolução 4.0 e seus impactos; descrever Metaverso; explicar os desafios legais que envolvem o Metaverso. A metodologia empregada é a qualitativa exploratória. O presente estudo traz à luz conceitos de autores da área, bem como expõe a relevância da informática no ambiente escolar de forma holística. Concluiu-se que os desafios legais do metaverso são variados, mas podemos limitá-los à proteção dos direitos e liberdades das pessoas, especialmente se for criada apenas uma linha tênue entre o metaverso e o mundo real, onde as ações em um lado e o outro pode ser visto. Os metaversos não devem se tornar lugares sem lei ou com uma lei marcada pela empresa que os controla, governos e organizações internacionais também devem se preocupar com o cumprimento das leis neles vigentes e modificar e criar novas regulamentações decorrentes dos desafios que envolve o mercado digital.

Palavras-chave: Metaverso, Direito digital, Tecnologia, Direitos da personalidade, Responsabilidade civil

Abstract/Resumen/Résumé

In a world undergoing digital transformation, the word metaverse is increasingly heard. This term is used to refer to a shared virtual environment to which we can connect through special devices to interact with other people through avatars. This universe, which offers opportunities where physical presence will be increasingly unnecessary, continues to grow day by day. The present study aims to analyze what are the legal challenges involving the Metaverse. Specifically, this work seeks to: highlight the importance of Revolution 4.0 and its impacts; describe Metaverse; explain the legal challenges surrounding the Metaverse. The

¹ Doutor em Direito Civil pela PUCSP; mestre em Direito pela UNESP; advogado; parecerista e professor.

² Graduado em Direito

³ Graduada em Direito

methodology used is exploratory qualitative. The present study brings to light concepts of authors in the area, as well as exposes the relevance of informatics in the school environment in a holistic way. It was concluded that the legal challenges of the metaverse are varied, but we can limit them to protecting people's rights and freedoms, especially if only a fine line is created between the metaverse and the real world, where actions on one side and the another can be seen. The metaverses must not become lawless places or with a law marked by the company that controls them, governments and international organizations must also be concerned about complying with the laws in force in them and modifying and creating new regulations arising from the challenges that the digital market involves.

Keywords/Palabras-claves/Mots-clés: Metaverse, Digital law, Technology, Personality rights, Civil liability

1 INTRODUÇÃO

Em um mundo em transformação digital, a palavra metaverso é cada vez mais mencionada. Este termo é usado para se referir a um ambiente virtual compartilhado ao qual podemos nos conectar por meio de dispositivos especiais para interagir com outras pessoas por meio de avatares. Este universo, que oferece oportunidades onde a presença física será cada vez mais dispensável, continua a crescer dia a dia (FALCÃO, 2013).

Especula-se que em 2025, o metaverso global pode valer US\$ 280 trilhões, de acordo com pesquisa da Strategy Analytics. Sendo um cenário em franca expansão e completamente novo, é interessante analisar seus aspectos jurídicos e as oportunidades que surgem para aqueles profissionais que se dedicam ao direito (LONGO; TAVARES, 2022).

O metaverso precisará de um marco legal que regule o funcionamento das empresas e marcas que ali interagem e se desenvolvem. Da mesma forma, a propriedade intelectual e sua proteção são questões que merecem a atenção dos profissionais do direito devido à quantidade de informações e bens que circulam digitalmente nesse ecossistema. Será necessário ajustar, redefinir ou adaptar a regulação de privacidade e controle de informações. Por exemplo, instrumentar como as licenças de conteúdo serão usadas para evitar roubo, plágio e infrações (LONGO; TAVARES, 2022).

Por outro lado, garantir a segurança dos usuários é essencial e requer também a colaboração de profissionais da área jurídica para preservação dos direitos da personalidade. Neste sentido, surgem desafios jurídicos em matéria de proteção de dados, uma vez que não será tarefa fácil estabelecer quem é o responsável pelo seu tratamento e o alcance das obrigações associadas (BACKES; SCHLEMMER, 2014).

Não se pode olvidar que os direitos da personalidade são as condições mínimas para que um ser humano seja considerado como tal. São os direitos essenciais, o mínimo exigido para uma vida digna, devendo contemplar além de elementos patrimoniais, passíveis de valoração econômica, como também, e principalmente, os valores existenciais, abrangendo os reflexos biológicos estruturais, interações sociais e valores morais e psicológicos. (MABTUM, 2021)

O metaverso, como qualquer plataforma ou aplicativo virtual, tem suas próprias regras. O novo regulamento deve complementar as normas, termos e condições que regem esta realidade multidimensional. Ainda há um longo caminho a percorrer em termos jurídicos e, sem dúvida, o metaverso ainda está em plena fase de desenvolvimento. No entanto, necessita de profissionais capacitados e responsáveis não apenas por definir e estabelecer o arcabouço legal para as interações que ali ocorram, mas também por regular a forma como os usuários serão

protegidos (ABREU, 2022).

Nesta perspectiva, a exploração da presente pesquisa gerou a seguinte problematização: Quais os desafios legais que envolvem o Metaverso? Tendo por objetivo analisar quais são os desafios legais que envolvem o Metaverso, bem como evidenciar a importância e os impactos da Revolução 4.0 e, principalmente, explicar os desafios legais que envolvem o Metaverso.

A exploração desta pesquisa tem como justificativa o atual reconhecimento da importância da Revolução digital contemporânea. O metaverso é um dos termos mais recorrentes atualmente, embora nem todos saibam seu significado, para que serve, quais são seus efeitos jurídicos e princípios éticos que o regem, entre outras coisas.

A metodologia utilizada na pesquisa teve abordagem qualitativa exploratória. Segundo Spector (2021) a pesquisa quantitativa pode ser definida em exploratória, descritiva e causal. Tendo-se a base da flexibilidade e criatividade buscando conhecer o assunto. O presente trabalho se desenvolveu por meio de pesquisas bibliográficas.

2 REVOLUÇÃO 4.0: A QUARTA REVOLUÇÃO INDUSTRIAL

Para compreender a revolução 4.0, é importante ter uma visão histórica das revoluções que a precederam. Segundo Del Val Román (2016), na primeira revolução, ocorrida por volta do século XVIII (1784), com a implantação de equipamentos mecânicos movidos a vapor, desenvolveram-se paradigmas para a produção de bens e serviços. Então, por volta do século XIX (1870), uma segunda revolução pode ser identificada, considerando que as fábricas e os processos de produção requerem eletricidade para aumentar a capacidade de trabalho e produção. Posteriormente, chega a automação nos processos, o que implica a entrada do computador no século XX (1970), melhorando os níveis de eficiência e produtividade nas empresas.

Há década, em 2011, a inteligência artificial e os sistemas físico-cibernéticos trouxeram aos processos de produção um novo mundo de opções, oportunidades e riscos, todos esses termos têm em comum o reconhecimento de que os processos de manufatura estão em processo de transformação digital, uma espécie de "revolução industrial" produzida pelo avanço das tecnologias da informação e, particularmente, da tecnologia da informação e do software (DEL VAL ROMÁN, 2016).

Essa seria a quarta revolução industrial, ou revolução 4.0, uma nova etapa comprometida com maior automação, conectividade e globalização. Vislumbra-se a inter-

relação entre diferentes áreas, como produtos, processos e modelos de negócios, penetrou no mundo industrial, trazendo consigo a *Internet of Things (IoT)* e o mundo do *Big Data* e *Analytics*. São os avanços tecnológicos que nos permitem otimizar os processos de fabricação, sua supervisão e integração com outros processos e sistemas utilizados na fábrica, oferecendo ganhos quantitativos e qualitativos na organização e gestão das cadeias de valor (SANTOS et al., 2018).

Esse fenômeno consiste na fusão dos planos físico e digital, favorecendo a apresentação da informação em formato compreensível para todos os utilizadores, promovendo uma colaboração reforçada e partilha de dados, apoiada na automatização dos processos de manutenção. Inteligência artificial (BRETTEL; FRIEDERICHSEN; KELLER.; ROSENBERG, 2014).

Trata-se de tecnologias e ferramentas como realidade virtual e aumentada, *IoT* (*Internet of Things*), inteligência artificial e visão, assistentes virtuais, *Big Data*, computação em nuvem, design moderno e programas de software. Simulação de processos, Impressão 3D, segurança, nano e biotecnologia ou computação quântica, entre outros (KAGERMANN; WAHLSTER; HELBIG, 2013).

A principal característica da Indústria 4.0 é a maior velocidade em fornecer resultados visíveis e o grau em que isso afeta os usuários. É sobre a Internet como base de interconexão e suas implicações em termos de facilidade de acesso à informação, identidade digital, privacidade, segurança, etc. Espera-se que ela gere impacto sobre a sociedade, a economia e a política de alguma forma. Fornecendo informação quase que instantaneamente. (KAGERMANN; WAHLSTER; HELBIG, 2013).

O ambiente por ser mais inteligente, apresenta muitas oportunidades e desafios, tais como, a criação de novos produtos que apresentem valores agregados em relação à concorrência e impactem positivamente o bem-estar pessoal (KHAN; TUROWSKI, 2016). A segurança cibernética é outro exemplo, sendo uma das questões-chave para esse novo mundo interconectado. A nova realidade exigirá habilidades e conhecimentos diferentes dos que são exigidos atualmente, e é provável que as relações de trabalho também se modifiquem (LEE; BAGHERI; KAO, 2016).

As tecnologias relacionadas à Indústria 4.0 também podem levar a produtos e serviços totalmente novos. O uso de sensores e dispositivos vestíveis, análises e robótica, entre outros, possibilitará melhorias no produto de várias maneiras, desde a prototipagem e teste até a adição de conectividade a produtos anteriormente desconectados. Essas mudanças nos produtos se traduzem, por sua vez, em mudanças na cadeia de suprimentos e, conseqüentemente, nos

clientes (SCHRÖDER et al., 2015).

No Brasil existem alguns setores globalmente competitivos, processos integrados que garantem uma produção sob medida e produtos inovadores da revolução 4.0. (ZANCUL, 2016). Algumas indústrias brasileiras desenvolveram projetos que podem ser considerados 4.0, como, por exemplo, a multinacional Ambev, que em 2015 adotou um sistema de automação para melhor controle do processo de resfriamento da cerveja e redução das variações de temperatura, com redução dos custos de energia e a Volkswagen Brasil, em que todos os projetos são criados a partir de um modelo digital. Os produtos são simulados em ambiente 3D, agilizando o processo, garantindo flexibilidade, otimizando os tempos de produção e gerando mais empregos para profissionais qualificados (ABC STUDIO, 2016).

Em 2017, o governo federal lançou o Plano Nacional para a Internet das Coisas, com o objetivo proporcionar capacitação às pessoas, inovação e empreendedorismo.

3 METAVERSO: POSSIBILIDADE DE UMA NOVA REALIDADE

Metaverso se revela como um novo horizonte de possibilidades, um recomeço que permite criar algo novo, ou aprimorar o que já existe, muito parecido com a expectativa trazida pelo desenvolvimento da Internet. Quantias vultuosas estão sendo investidas na construção do metaverso, e os magnatas da tecnologia chamam isso de futuro, mas o que é metaverso? O termo metaverso foi forjado em 1992 pelo escritor de ficção científica Neal Stephenson. Sua definição mais básica refere-se ao conceito de um mundo virtual totalmente imersivo, onde as pessoas se reúnem para socializar, brincar e trabalhar (FALCÃO, 2013).

É um ambiente digital simulado que combina realidade aumentada (AR), realidade virtual (VR), *blockchain* e princípios de mídia social para criar áreas para interação rica do usuário que imitam o mundo real. O conceito de metaverso, recentemente divulgado pelo *rebranding* do Facebook como Meta, revolucionará a forma como interagimos com o mundo. O CEO do Facebook, Mark Zuckerberg, afirmou que a próxima geração da internet é o metaverso e que as mídias sociais existentes ficarão sob o guarda-chuva dessa nova onda. Ele descreve o metaverso como um ambiente virtual onde se pode se apresentar com pessoas em espaços digitais. Pode se pensar nisso como uma Internet incorporada na qual a pessoa está dentro, em vez de apenas olhar (LONGO; TAVARES, 2022).

O metaverso é uma convergência perfeita de nossas vidas físicas e digitais, criando uma comunidade virtual unificada onde podemos trabalhar, brincar, relaxar, fazer transações e socializar. O metaverso ainda está no início de sua evolução e não há uma definição única e

abrangente para a qual as pessoas possam recorrer. Temas do que o metaverso é e poderia ser, no entanto, estão surgindo. Um ponto chave é que não existe um mundo virtual, mas muitos mundos, que estão tomando forma para permitir que as pessoas aprofundem e ampliem as interações sociais digitalmente.

Isso é feito adicionando uma camada tridimensional imersiva à web, criando experiências mais autênticas e naturais (LONGO; TAVARES, 2022). O metaverso ainda tem a promessa de facilitar a acessibilidade a partir do conforto do lar, rompendo fronteiras e democratizando o acesso a bens, serviços e experiências essenciais. Antes de mergulhar mais fundo no metaverso, é importante estabelecer as bases entre os recursos do metaverso de hoje – as características da Web 2.0 e as características emergentes da Web 3.0. Enquanto a tabela abaixo destaca nossa avaliação dos principais recursos do metaverso entre os dois, as linhas estão se esvaindo à medida que mais e mais mundos virtuais tradicionais estão adotando elementos dos mundos baseados em blockchain (BACKES; SCHLEMMER, 2014).

Abreu (2022) afirma que o conceito de metaverso não é novo. Segundo a autora, de muitas maneiras, esta é uma progressão linear. Mundos online, multijogador e RPG como “The Sims” ou “Second Life” existem há quase 20 anos, com os jogadores gastando uma média de 20 horas por semana nesses mundos. Equivalentes modernos como Minecraft, World of Warcraft e Fortnite têm centenas de milhões de usuários e enormes economias de suporte. Estamos agora em um ponto de inflexão, onde parece que não passa um dia sem que uma empresa ou celebridade anuncie que está construindo uma presença em um universo virtual.

Embora o burburinho possa ser parcialmente atribuído às manchetes que chamam a atenção, há uma convergência de tendências emergentes (ANACONA; MILLÁN; GÓMEZ, 2019). Uma série de novas tecnologias se uniu para permitir essa visão do metaverso. Os headsets de realidade aumentada (AR) e realidade virtual (VR) tornaram-se mais baratos e mais poderosos, melhorando a experiência do usuário. Blockchain habilitou moedas digitais e NFTs. Os novos métodos para realizar transações e possuir bens digitais estão permitindo que os criadores monetizem suas atividades por meio de tokens. Além da monetização, e como meio de troca de valor, os detentores de tokens também podem participar da governança da plataforma (por exemplo, votar nas decisões) (CABRAL, 2022).

Essa economia de propriedade democrática, juntamente com a possibilidade de interoperabilidade, pode abrir imensas oportunidades econômicas, pelas quais bens e serviços digitais não são mais cativos de uma plataforma ou marca de jogo singular (OYELUDE, 2018). De uma perspectiva social, o desenvolvimento de experiências virtuais mais imersivas está ajudando as pessoas a construir comunidades baseadas em valores compartilhados e a se

expressar de maneiras mais autênticas. Enquanto isso, o COVID-19 acelerou a digitalização de nossas vidas e normalizou o envolvimento e a comunicação online mais persistentes e multifuncionais. É essa combinação de fatores tecnológicos, sociais e econômicos que está resultando no interesse explosivo pelo metaverso (HUGGETT, 2020).

4 O METAVERSO: QUAIS SÃO AS IMPLICAÇÕES LEGAIS?

Como acontece com qualquer inovação tecnológica, o metaverso levantará questões legais novas e complexas. À medida que as aplicações práticas do metaverso continuam a se ampliar e evoluir com melhorias na tecnologia, o mesmo acontecerá com os desafios legais e regulatórios. Adicionando a um campo de jogo já complexo, o metaverso foi projetado para ser profundamente interconectado, sem costura e sem ancoragem no espaço físico. Cada uma das questões jurídicas discutidas abaixo exigirá que os profissionais naveguem por questões de jurisdição, territorialidade e conflitos de leis, nenhuma das quais foi bem resolvida mesmo para a iteração atual da Internet, muito menos mundos virtuais totalmente realizados com um grau ainda maior de interação e imersão do usuário (CHIN, 2017).

O avanço proporciona a expectativa de gerar grandes benefícios a situações até então sem perspectiva de solução, contudo, traz consigo o risco do surgimento de danos desconhecidos, com desdobramentos inimagináveis.(MABTUM, 2018)

A segurança digital e a privacidade estarão entre os problemas legais mais significativos enfrentados pelos proprietários de plataformas. Essas preocupações não são novidade para as empresas de tecnologia, que enfrentam crescente escrutínio de reguladores e usuários. Mas os dados no metaverso se tornarão exponencialmente mais valiosos do que já são, e as tecnologias se tornarão cada vez mais integradas em vários aspectos da vida dos usuários. Essa tecnologia em desenvolvimento testará as leis existentes e pressionará ainda mais os reguladores para que correspondam à sofisticação da tecnologia (MARSDEN, 2021).

A segurança de dados também conhecida como segurança da informação ou segurança do computador é um aspecto essencial da TI em organizações de qualquer tamanho e tipo. Este é um aspecto que tem a ver com a proteção dos dados contra o acesso não autorizado e com a proteção de possíveis corrupções ao longo do seu ciclo de vida (ALBRECHTSEN, 2017).

A segurança de dados inclui conceitos como criptografia de dados, *tokenização* e práticas de gerenciamento de chaves que ajudam a proteger os dados em todos os aplicativos e plataformas de uma organização. Hoje, organizações em todo o mundo investem fortemente

em tecnologia da informação relacionada à defesa cibernética para proteger seus ativos críticos: sua marca, capital intelectual e as informações de seus clientes (FURNELL; THOMSON, 2019).

Em todas as questões de segurança de dados, existem elementos comuns que todas as organizações devem levar em consideração ao aplicar suas medidas: pessoas, processos e tecnologia (FURNELL; THOMSON, 2019). A segurança dos dados é um problema crítico que afeta quase todos nós. São cada vez mais os produtos tecnológicos que de uma forma ou de outra devem ser tidos em conta nas questões de segurança e que estão a ser introduzidos no nosso cotidiano, desde *smartwatches* até veículos sem condutor. Chegou a era da Internet das Coisas (IoT) e, claro, dos hacks relacionados à IoT (GAIVÉO, 2018).

Todos esses dispositivos conectados criam novas “conversas” entre dispositivos, interfaces, infraestruturas privadas e a nuvem, o que, por sua vez, cria mais oportunidades para os hackers escutarem. Tudo isso gerou uma demanda por especialistas em segurança de dados e soluções capazes de construir redes mais fortes e menos vulneráveis (GAIVÉO, 2018).

Tendências recentes têm mostrado que os ataques de *ransomware* estão aumentando em frequência e gravidade. Tornou-se um negócio em expansão para ladrões cibernéticos e *hackers*, que acessam a rede e sequestram dados e sistemas. Nos últimos meses, grandes empresas e outras organizações, bem como usuários privados, foram vítimas desses tipos de ataques e tiveram que pagar o resgate ou correr o risco de perder dados importantes (ALVES, 2016).

Circunstâncias semelhantes às anteriores estão frequentemente presentes em locais onde as operações são suportadas por tecnologias de informação e comunicação (FONTES, 2016). É crescente a importância dos sistemas de informação nas rotinas diárias, cuja consequência é a significativo impacto que pode gerar nas pessoas, bem como nas entidades, causando diversas espécies de perdas (IMONIANA, 2015).

A questão é que com o aumento da informatização aumenta a dependência das tecnologias, de modo que quando estas falham e não existem alternativas que garantam a continuidade das operações, os processos que delas dependem falham e se apresentam. Situações mais complexas em processos críticos associados a essas tecnologias, como as relacionadas à saúde das pessoas, atividade industrial ou controle de tráfego aéreo, apenas para citar algumas, nas quais um simples desvio dos parâmetros operacionais poderia causar consequências terríveis (VIDAL, PIERRAT, 2015).

Adicionalmente, a informação processada, contida e transmitida através das tecnologia da informação adquire características únicas que tornam a sua proteção mais

complexa, pois não basta preservar a sua disponibilidade para evitar as situações desagradáveis mencionadas acima, mas também é necessário proteger a sua integridade e sua confidencialidade (IMONIANA, 2015).

Os especialistas em TI desejam que a rede e o equipamento terminal não falhem; o pessoal encarregado da segurança e proteção visa prevenir o furto de equipamentos e componentes e o vazamento de informações; auditores tentam por todos os meios reduzir a probabilidade de fraude e aqueles com um computador em casa aspiram a fazer com que dure para sempre (CITTADIN, 2018).

Por outro lado, alguns acreditam que a segurança digital consiste na proteção adequada contra vírus e outros programas maliciosos e alguns consideram que seu objetivo está concentrado em impedir que os funcionários acessem sites inadequados ou enviem e-mails para o exterior. Embora todo mundo tenha razão, a segurança do computador é muito mais do que descrito (SECURITY OFFICE FOR COMPUTER NETWORKS, 2013). O termo segurança vem da palavra latina “seguro” e, de um modo geral, é sinônimo de “estar seguro” (CITTADIN, 2018).

A segurança geralmente é definida como a ausência de risco ou também a confiança em algo ou alguém. No entanto, o termo pode ter significados diferentes dependendo da área ou campo a que se refere (AVOGADRO, 2015). A segurança do computador visa proteger a infraestrutura de computação e tudo relacionado a ela (incluindo as informações nela contidas) (CITTADIN, 2018).

Para isso, existem normas, protocolos, métodos, regras, ferramentas e leis que visam minimizar possíveis riscos à infraestrutura ou às informações. Existem três princípios ou aspectos fundamentais relacionados à segurança do computador: confidencialidade, integridade e disponibilidade (PIERRAT, 2043). A confidencialidade, às vezes chamada de sigilo ou privacidade, é a condição que garante que as informações não possam ser disponibilizadas ou descobertas por pessoas, entidades ou processos não autorizados. Integridade é entendida como a condição que garante que as informações somente possam ser modificadas, incluindo sua criação e exclusão, por pessoal autorizado (OLIVEIRA; MOURA; ARAÚJO, 2013).

Garante que as informações são precisas e completas e que o sistema não as modifica ou corrompe, nem permite que uma pessoa não autorizada o faça. Disponibilidade é a propriedade que garante o acesso aos ativos de informação e o uso de recursos de informática a qualquer momento por pessoas autorizadas. Um sistema seguro deve manter as informações disponíveis aos usuários (FONSECA, 2019; PERINI, 2013; OLIVEIRA; MOURA; ARAÚJO,

2013).

Disponibilidade significa que o sistema, tanto hardware quanto software, funciona de forma eficiente e é capaz de se recuperar rapidamente em caso de falha. A abordagem à segurança e os mecanismos utilizados para a sua implementação são influenciados em cada caso pelo mais importante destes três aspectos no local em questão (TANENBAUM; WETHERALL, 2013; REZENDE, 2018).

É evidente a importância da segurança digital, tanto para os gestores, que têm a máxima responsabilidade pela organização da política e estratégia de utilização e preservação de todos estes processos informacionais e tecnológicos tão necessários à tomada de decisões na esfera que dirigem; funcionários que operam as tecnologias e as informações nelas contidas, especialistas em informática que são responsáveis por garantir o suporte seguro onde essas técnicas operam; os responsáveis pela segurança e proteção que garantem o cumprimento das políticas, medidas e contramedidas utilizadas para proteger os meios de comunicação, os repositórios e a própria informação (CAROCIA, 2019).

Em linha com o ponto anterior, a interação com o metaverso gerará muito mais dados do que os gerados atualmente, incluindo dados pessoais. Assim, a proteção de dados e a privacidade digital também é um desafio legal que governos e órgãos reguladores nacionais e internacionais precisam começar a antecipar e enfrentar (WACHTER; MITTELSTADT, 2019). Ambientes digitais descentralizados, como o metaverso, dificultarão a aplicação de leis como a lei de proteção de dados pessoais, pois será necessário estabelecer quem são os responsáveis pelo processamento de dados e as obrigações dele derivadas. Além disso, pode ser necessário criar novas formas de obter o consentimento dos usuários ou informá-los sobre os riscos à sua privacidade (PIRONTI; KEPPEN, 2021).

Não se pode esquecer que para que o metaverso seja completamente imersivo, serão utilizados dispositivos com todos os tipos de sensores que coletarão todo tipo de dados dos usuários, inclusive dados especialmente protegidos, como biometria (isso é algo que já começou a acontecer com óculos de realidade virtual e que crescerá exponencialmente com o desenvolvimento deste tipo de tecnologia e tecnologias hápticas) (MUCELIN, 2021).

Além disso, um metaverso singular, se operado por várias entidades, exigirá padrões de interoperabilidade que metaversos isolados e díspares não exigirão. As informações do usuário estarão em risco particular de exploração, dadas as vulnerabilidades envolvidas quando os dados forem transferidos de um aplicativo para outro, e os operadores de plataforma precisarão de acordos abrangentes para controlar as transferências de dados, padrões de segurança da informação e responsabilidade pela conformidade (bem como violações de dados,

o que poderia causar ainda mais caos do que eles fazem hoje) (MUCELIN, 2021).

Não obstante, os direitos fundamentais do usuário devem ser tutelados, nenhuma violação que afronte a dignidade da pessoa humana será tolerada, visto ser esse o cerne axiológico do ordenamento jurídico, sendo tutelada contra atos de particulares e do próprio Estado. (MABTUM; MARCHETTO, 2015)

As principais empresas de tecnologia já estão enfrentando um escrutínio antitruste significativo e uma regulamentação crescente em todo o mundo, e o desenvolvimento do metaverso pode estimular o escrutínio e a ação adicionais dos agentes antitruste. A interoperabilidade entre plataformas, que se acredita ser um componente essencial do metaverso, requer padrões da indústria para ser eficaz. Embora a lei antitruste geralmente permita que as empresas criem conjuntamente certificações técnicas pró-competitivas, incluindo padrões que melhorem a interoperabilidade, o processo de definição de padrões pode, no entanto, dar origem a preocupações antitruste (DOMINGUES; GABAN, 2019).

Além das preocupações em torno de um processo justo de definição de padrões, acordos de cooperação e padrões da indústria correm o risco de restringir a produção e podem violar as leis antitrustes se não forem suficientemente adaptado ao seu propósito pró-competitivo. À medida que as grandes empresas de tecnologia procuram construir a infraestrutura para o metaverso, elas podem encontrar alegações de violações antitrustes e escrutínio adicional de legisladores e aplicadores antitruste (DOMINGUES; GABAN, 2019).

As questões de propriedade intelectual também são altamente relevantes. Por exemplo, determinar a identidade dos criadores de uma determinada obra no metaverso pode ser mais difícil quando a obra resulta de um processo colaborativo descentralizado realizado por usuários anônimos por trás de avatares. Essa incerteza também pode mudar o entendimento dos tribunais sobre o uso justo. Enquanto isso, os advogados de marcas registradas estão se concentrando em questões como a diluição de marcas registradas pode ocorrer no metaverso, se os ativos digitais devem ser qualificados como "bens" para fins das leis de marcas registradas e quem deve ser responsabilizado quando a identidade do infrator não é clara (PIRONTI; KEPPEN, 2021).

De acordo com os autores, surgirão questões legais relacionadas a fintech cada vez mais no metaverso, especialmente à medida que mais empresas oferecem ativos digitais e serviços à venda. Vendas de virtual mercadorias já estão sendo feitas usando criptomoedas e outros ativos digitais, e eles podem, em última análise, ser suportados por as mesmas tecnologias blockchain que permitir o essencial do metaverso funções de interoperabilidade. As marcas podem distribuir "bens" digitais no metaverso, seja vendendo mercadorias idênticas para muitos usuários (como pares de marca de tênis) ou vendendo direitos ou indícios de

propriedade de bens individuais, como uma obra de arte única.

Compradores do último podem adquirir tais bens como investimento ou mantê-los para seu próprio coleção, mesmo exibindo-os em um ambiente virtual (por exemplo, "pendurando" eles na sala de estar da sua virtual "Casa de verão"). A autenticidade da arte pode ser verificado no blockchain por meio de NFTs usando um processo semelhante à verificação do valor da própria criptomoeda. As questões jurídicas certamente surgirá em relação a adequada verificação de propriedade e potencial violação ou conversão de documentos autênticos e compras verificadas. Se a criptomoeda é tratado como um instrumento financeiro ou segurança, o que parece cada vez mais provável em certas jurisdições, os consumidores enfrentará obstáculos usando criptomoeda como moeda para o compra de bens digitais (LONGO; TAVARES, 2022).

Quanto mais indivíduos adquirem ativos digitais, operadores de plataformas onde os ativos digitais existentes provavelmente enfrentarão um dever de cuidado para garantir a segurança dos ativos digitais. O metaverso como um todo é estimado em ser uma oportunidade de receita de US\$ 8 trilhões. Os investidores tomaram nota da "metaverse landgrab" e acionistas estão cada vez mais pedindo às empresas que expliquem suas estratégias de metaverso. O sucesso do metaverso, em qualquer forma que toma, exigirá enormes investimentos de capital em digital conteúdo, ativos digitais e hardware para gerar espaços virtuais (por exemplo, GPUs), como bem como a infraestrutura digital (por exemplo, fibra e redes 5G) para conectá-los (LONGO; TAVARES, 2022).

O capital de risco inundou o setor, com mais de US\$ 10 bilhões arrecadados ano passado em jogos, aumentou realidade e mundos virtuais. Grandes empresas de tecnologia estão escalando rapidamente aumentar suas atividades de metaverso e continuar a fazê-lo através de M&A. Isto é uma tendência global, com um pico no metaverso negócios em mercados nos EUA, Reino Unido, Europa e Ásia-Pacífico. Um aumento de meios de negociação transfronteiriça navegando pelas complexidades jurídicas destacado acima, ao mesmo tempo em que enfrenta maior escrutínio dado o papel central das empresas de tecnologia no mundo digital economia e políticas regulatórias tendência para controles de dados e soberania tecnológica (BACKES; SCHLEMMER, 2014).

Continuando com o exposto, surgem as seguintes questões evidenciadas por Abreu (2022): quem governará o metaverso, quem criará suas leis? Serão as grandes corporações de tecnologia? Os governos nacionais terão reflexo no metaverso? Serão aplicadas as mesmas leis do mundo real? Será necessário criar novas leis? Ou será suficiente fazer cumprir as existentes? , transferindo para o mundo digital? A Internet e, principalmente, as redes sociais já revelaram

alguns dos problemas que poderiam ser transferidos para o metaverso e em que as leis vigentes por vezes parecem ser limitadas por elementos como o anonimato.

Embora o metaverso ou metaversos sejam mundos digitais à parte do mundo real, um dos objetivos de seus criadores é que ele possa ser operado indistintamente em um mundo e em outro, ou seja, que o que fazemos no metaverso se reflita na realidade e vice-versa (Por exemplo, se eu for fazer compras no metaverso, receberei os itens comprados no mundo real, desde que sejam físicos). Portanto, nesses metaversos também devem ser respeitados os direitos dos usuários. Novamente, a descentralização pode representar um desafio nesse sentido, embora existam leis como a Lei Orgânica 3/2018, que já inclui a proteção de uma série de direitos digitais das pessoas. No entanto, esse tipo de legislação pode ficar aquém da aplicação no metaverso (PIRONTI; KEPPEL, 2021).

5 CONSIDERAÇÕES FINAIS

O metaverso trata de um mundo digital imersivo, no qual os usuários, através do uso de avatares e diferentes tecnologias convergentes (visualizadores de realidade virtual, vestuário háptico, conexão à Internet, etc.), poderão realizar todo tipo de atividades e ações, como trabalhar, estudar, desfrutar de diferentes atividades de lazer (ir ao cinema, viajar, festejar, entre outros), interagir com outros usuários, etc., tudo dentro de um ambiente totalmente virtual, mas que deve parecer o mundo real.

Embora a realidade virtual atual já tenha conseguido imergir seus usuários em ambientes 3D interativos, ainda estamos longe da proposta da Meta e de outras empresas para seus metaversos (ainda não podemos sentir ou interagir livremente em um mundo digital alternativo). No entanto, o desenvolvimento de novas tecnologias que as tornarão possíveis continua a avançar e a médio-longo prazo podemos começar a viver entre a realidade e o mundo virtual de um ou mais metaversos.

Como aconteceu com diferentes aspectos da Internet, o desenvolvimento do metaverso e as ações que poderemos realizar nele, bem como interagiremos com o ambiente e o restante dos usuários e o que seremos capaz de criar, expor, compartilhar e até comercializar ali, coloca uma série de desafios jurídicos aos quais devemos estar atentos: identidade digital; Proteção de dados e privacidade; Direitos Digitais; e, Propriedade Intelectual.

Os desafios legais do metaverso são variados, mas podemos limitá-los à proteção dos direitos e liberdades das pessoas, componentes dos diversos atributos tutelados pelos direitos da personalidade, garantindo a efetividade da dignidade da pessoa humana, especialmente se

for criada apenas uma linha tênue entre o metaverso e o mundo real, onde as ações em um lado e o outro pode ser visto.

Os metaversos não podem se tornar lugares sem normatização ou com uma regras específicas, determinadas exclusivamente pela empresa que os controla. Os governos e as organizações internacionais também devem se preocupar com o cumprimento das leis neles vigentes e modificar e criar novas regulamentações decorrentes dos desafios que envolve o mercado digital.

REFERÊNCIAS

ABC Studio, SIMENS. **Como será o Industry 4.0 Professional?** 2016.

ABREU, F. de. O metaverso poderá ser crucial para a aniquilação da humanidade. **RECISATEC - Revista Científica Saúde e Tecnologia**, vol. 2, no. 4, 2022.

ALBRECHTSEN, E. A qualitative study of users' view on information security. **Computers & Security**, vol. 26, no. 4, 2017, pp. 276-289.

ALVES, G. A. **Segurança da Informação: uma visão inovadora da gestão**. Rio de Janeiro: Ciência Moderna Ltda, 2016.

ANACONA, J. D.; MILLÁN, E. E.; GÓMEZ, C. A. Aplicación de los metaversos y la realidad virtual en la enseñanza. **Entre Ciencia e Ingeniería**, vol. 13, no. 25, 2019, pp. 59-67.

AVOGADRO, M. Security and new technologies: a necessary pairing. **Miscelânea**, vol. 6100, 2015.

BACKES, L.; SCHLEMMER, E. O processo de aprendizagem em metaverso: formação para emancipação digital. **Revista de Gestão do Unilasalle**, Canoas, vol. 3, no. 1, 2014.

BALOG, M. M.; DEMIDOVA, S. E.; TROYAN, V. V. The influence of digital transformation on the shadow economy. **ETAP: Economic Theory, Analysis, and Practice**, vol. 4, 2020, pp. 58-72.

BRETTEL, M.; FRIEDERICHSEN, N.; KELLER, M.; ROSENBERG, M. How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. **International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering**, vol. 8, no. 1, 2014, pp. 37-44.

CABRAL, L. R. P. **Realidade virtual em bibliotecas universitárias: tecnologias e aplicações**. 2022. 69f. Monografia (Graduação em Biblioteconomia) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2022.

CAROCIA, M. **Sistemas de informação**. São Paulo: Pearson Education do Brasil, 2019.

CHIN, B. M. Regulating Your Second Life: Defamation in Virtual Worlds. **Brooklyn Law Review**, vol. 72, no. 4, 2017.

CITTADIN, J. O. B. **Gestão da segurança da informação: desafios e perspectivas**. Trabalho Conclusão de Curso, Universidade Federal de Santa Catarina, Araranguá, 2018.

DEL VAL ROMÁN, J. L. **Industria 4.0: la transformación digital de la industria**. Facultad de Ingeniería de la Universidad de Deusto. Espanha: Conferência de Directores y Decanos de Ingeniería Informática, 2016. Disponível em: <<http://coddii.org/wp-content/uploads/2016/10/Informe-CODDII-Industria-4.0.pdf>>. Acesso em 27 de setembro de 2022.

DEMIDOVA, S. E.; CHIRKOVA, T. Y.; BALOG, M. M.; PETROVA, O. S. **Development of human capital in the aspect of financial security**. Paris: Atlantis Press, 2019, pp. 582-588.

DOMINGUES, J.; GABAN, E. Direito Antitruste e Poder Econômico: o movimento populista e “neo-brandeisiano”. **Revista Justiça Do Direito**, 2019.

FALCÃO, T. Universo, Metaverso, Multiverso: Mundos Virtuais como Híbridos entre Jogos Eletrônicos e Comunidades Virtuais. **Researchgate**, 2013.

FONSECA, P. F. **Gestão da segurança da informação: o fator humano**. PUCPR, 2019.

FONTES, E. **Segurança da Informação: o usuário faz a diferença**. São Paulo: Saraiva, 2016.

FROLOVA, E. V.; ROGACH, O.; RYABOVA, T. M. Digitalization of education in modern scientific discourse: new trends and risks analysis. **European journal of contemporary Education**, vol. 9, no. 2, 2020, pp. 313- 336.

FURNELL, S.; THOMSON, K. L. From Culture to disobedience: recognising the varying user acceptance of IT security. **Computer Fraud & Security**, vol. 2, 2019, pp. 5-10.

GAIVÉO, J. M. **As pessoas nos sistemas de gestão da segurança da informação**. Tese de doutoramento, Lisboa, Portugal, 2018.

GARCIA, P. **“Robôs Autônomos”**. 2016. Disponível em: <<https://pedrogarcia-12av1.wordpress.com/about/robos-autonomos/>>. Acesso em 27 de setembro de 2022.

GIL, A.C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2013.

GIMPELSON, V. E. Does the Russian economy Need human capital? Ten doubts. **Economic Issues**, vol. 10, 2016, pp. 129-143.

GORTAZAR, L. Transformación digital y consecuencias para el empleo en España. **Una revisión de la investigación reciente**, no. 04, 2018.

HERMANN, M.; PENTEK, T.; OTTO B. Design Principles for Industrie 4.0 Scenarios: A Literature Review, Working Paper, no. 01, 2015.

HERNÁNDEZ, J. V. Internal control and organizational culture in small businesses: A conjunction to competitiveness. **Reuna**, vol. 21, no. 2, 2016, pp. 05-22.

HOFMANN, E.; RÜSCH, M. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry*. Elsevier, 2017.

HUGGETT, J. Virtually real or really virtual: towards a heritage metaverse. *Studies in Digital Heritage*, vol. 4, no. 1, 2020, pp. 1–15.

IMONIANA, J. O. **Auditoria de Sistemas de Informação**. São Paulo: Atlas, 2015.

KAGERMANN, H.; WAHLSTER, W.; HELBIG, J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. **Final report of the Industrie 4.0 Working Group**, 2013, 82 p.

KHAN, A.; TUROWSKI, K. **A Perspective on Industry 4.0: From Challenges to Opportunities in Production Systems**. IoTBD 2016 - International Conference on Internet of Things and Big Data, 2016.

KNOX, B. J. The effect of cyberpower on institutional development in Norway. *Frontiers in psychology*, vol. 9, no. 717, 2018.

KONEVA, A. V.; LISENKOVA, A. A. Identity matrix in the digital age: social challenges to overcome the anonymity. *Tomsk state university journal of cultural studies and art history*, vol. 35, 2019, pp. 14–28.

KUMAR, S. A. et al. Security in internet of things: Challenges, solutions and future directions. **Hawaii International Conference on System Sciences (HICSS)**, vol. 39, 2013, pp. 5772-5781.

LAASER, W. Economic implications and stakeholder reactions in a digital university environment. *Red-revista de educacion a distancia*, vol. 57, no. 4, 2018.

LEE, J.; BAGHERI, B.; KAO, H. A. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, vol. 3, 2015, pp. 18–23.

LONGO, W.; TAVARES, F. **Metaverso**. Editora: Alta Books, 2022, 224 p.

MABTUM, Matheus Massaro; MARCHETTO, Patrícia Borba. **O debate bioético e jurídico sobre as diretivas antecipadas da vontade**. São Paulo: Cultura Acadêmica, 2015.

MABTUM, Matheus Massaro. **A autonomia nas diretivas antecipadas de vontade (testamento vital): entre a autodeterminação do declarante e a responsabilidade civil do mandatário de saúde**. Londrina: Thoth, 2021.

MABTUM, Matheus Massaro. Wrongful actions: um breve relato desde sua origem até sua apreciação pelo Tribunal de Justiça do estado de São Paulo. In: **Risco, dano e responsabilidade civil**. Coordenador: Rogério Donnini. Organizadora: Andrea Cristina Zanetti. Salvador: Editora JusPodivm, 2018.

MACDOUGALL, W. **Industrie 4.0: Smart Manufacturing for the Future**. Berlin: Gtai, 2014.

MARSDEN, C. T. **Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace**. Cambridge University Press: Cambridge, 2021.

MARTIN, D. et al. US SEC report calls for better internal accounting controls for cyber-related threats. **Journal of Investment Compliance**, vol. 20, no. 1, 2019, pp. 5-9.

MCKEE, M.; SCHALKWYK, M. C. I.; STUCKLER, D. The second information revolution: digitalization brings opportunities and concerns for public health. **European journal of public health**, vol. 29, 2019, pp. 3-6.

MUCELIN, G. Garantias do Consumo: Metaverso e vulnerabilidade digital. **Conjur**, 2021.

NAÇÕES UNIDAS. **As cidades continuarão a crescer, especialmente nos países em desenvolvimento**. Nova York: ONU, 2018.

OESTERREICH, T. D.; TEUTEBERG, F. Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. **Computers in Industry**, vol. 83, 2016, pp. 121–139.

OLIVEIRA, G. D. de; MOURA, R. C. G.de; ARAÚJO, F. de A. N. G. de. **Gestão da segurança da informação: perspectivas baseadas na tecnologia da informação**, 2013.

OYELUDE, A. A. Virtual reality (VR) and augmented reality (AR) in libraries and museums. **Library Hi Tech News**, vol. 35, no. 5, 2018, pp. 1–4.

PERINI, L. C. **Administração de sistemas de informação**. São Paulo: Pearson Prentice Hall, 2013.

PIERRAT, G. G. **Seguridad Informática**. La Habana: G.L.D., 2013.

PIRONTI, R.; KEPPEM, M. Metaverso: novos horizontes, novos desafios. **International Journal of Digital Law – IJDL**, vol. 2, no. 3, 2021.

REZENDE, D. A. **A evolução da tecnologia da informação nos últimos 45 anos**. Udesc, 2018.

RYMARCZYK, J. Technologies, opportunities and challenges of the industrial revolution 4.0: theoretical considerations. **Entrepreneurial business and economics review**, vol. 8, no. 1, 2020, pp. 185-198

SANTOS, B. et al. Indústria 4.0: desafios e oportunidades. **Revista Produção e Desenvolvimento**, vol. 4, no. 1, 2018, pp. 111-124.

SCHRÖDER, R. et al. Análise da Implantação de um Processo Automatizado em uma Empresa Calçadista: Um Estudo de Caso a Luz do Sistema Hyundai de Produção e a Indústria 4.0. **Revista Espacios Caracas**, vol. 36, no. 18, 2015, pp. 19.

SECURITY OFFICE FOR COMPUTER NETWORKS. **Methodology for Information Security Management (project)**. Havana: OSRI, 2013.

SHAMIM, S. et al. **Management approaches for Industry 4.0: A human resource management perspective**. IEEE Congress on Evolutionary Computation (CEC), 2016, pp. 5309-5316.

SOMOS SOCIAIS. **We Are Social**. New York: Digital Report, 2019.

SONY, M.; NAIK, S. Ten Lessons for managers while implementing Industry 4.0. **IEEE Engineering Management Review**, 2019.

SPECTOR, N. **Manual para redação de teses, projetos de pesquisa e artigos científicos**. 2ed. Rio de Janeiro: Guanabara Koogan, 2021. 150p.

SUNG, T. K. Industry 4.0: A Korea perspective. **Technological Forecasting and Social Change**, vol. 132, 2018, pp. 40-45.

TANENBAUM, A. S.; WETHERALL, D. J. **Rede de computadores**. 5. ed. São Paulo: Saraiva, 2013.

VIDAL, L. M.; PIERRAT, G. G. Seguridad, información y salud. **Revista Cubana de Informática Médica**, vol. 1, no. 5, 2015.

XU, L. da; XU, E. L.; LI, L. Industry 4.0: state of the art and future trends. **International Journal Of Production Research**, vol. 1., 2018, pp.1-22.

WACHTER, S.; MITTELSTADT, B. **A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI**. *Columbia Business Law Review*, 2019.

ZHOU, Y. et al, Investigation of the impact of main control room digitalization on operators cognitive reliability in nuclear power plants. **Work-a journal of prevention assessment & rehabilitation**, vol. 41, 2013, pp. 714-721.