REVISTA ELETRÔNICA

DIREITO & TI

DIREITO & TI – PORTO ALEGRE / RS

WWW.DIREITOETI.COM.BR

Nº 18 [JAN./ABR.]

ANO 2024

VOL. 1

ISSN 2447-1097

WB EDUCAÇÃO

WB EDUCAÇÃO [CNPJ:41.653.466/0001-73]

Site: https://wbeduca.com.br/pt/

E-mail: revista@wbeducacional.com.br

REVISTA ELETRÔNICA DIREITO & TI [QUALIS CAPES B1]

Regras de submissão, cadastro e publicações: https://direitoeti.com.br/direitoeti

Editor-chefe: Emerson Wendt

Editora revisora: Valquiria P. C. Wendt

Dados Internacionais de Catalogação na Publicação (CIP)

Revista Direito e TI [recurso eletrônico] / WB Educação, v. 1, n. 18, (jan./abr. 2024).
Porto Alegre: WB Educação, 2024.

Trimestral.
ISSN: 2447-1097.
Acesso em: <https://direitoeti.com.br/direitoeti>.

1. Direito - Periódicos. I. WB Educação.

CDD 340

Ficha catalográfica elaborada pela Bibliotecária Taís Amorim, CRB 10/2547

DADOS PESSOAIS, SEGURANÇA PÚBLICA, INTELIGÊNCIA ARTIFICIAL, CRIPTOATIVOS E NFT'S

Prezados leitores e entusiastas da interseção entre o Direito e a Tecnologia da Informação,

É com grande entusiasmo que apresentamos o Volume 1 da Edição nº 18 da Revista Eletrônica Direito & TI. Nesta edição, reunimos uma seleção de artigos que abordam questões jurídicas relacionadas à tecnologia da informação, refletindo sobre os desafios e oportunidades que surgem na intersecção entre o direito e a inovação tecnológica.

No primeiro artigo, cujo título é *Incidentes de Segurança envolvendo Dados Pessoais: formas de tutela jurídica*, os autores Sergio Marcos Carvalho de Avila Negri e Carolina Fiorini Ramos Giovanini procuram demonstrar diferentes formas de tutela que podem ser aplicadas diante dos incidentes de segurança. Baseados na LGPD, que adota uma abordagem baseada no risco, buscam demonstrar que a tutela preventiva assume papel de especial relevância no ordenamento jurídico.

Destacam que, em que pese a adoção de medidas preventivas, é possível que incidentes de segurança ocorram e, nesses casos, procuram apontar que a tutela específica poderá ser utilizada. Por fim, no que diz respeito à tutela ressarcitória em matéria de privacidade e proteção de dados, o texto investiga os desafios de identificação do nexo causal e de demonstração e quantificação do dano, concluindo que meios alternativos de reparação não pecuniária devem ser avaliados nas situações concretas. Ou seja, os autores destacam a importância da tutela preventiva e ressarcitória, além dos desafios na identificação do dano e na quantificação dos prejuízos.

Sob o título *Os "Novos Olhos" da Segurança Pública na Bahia: Ruídos de uma Necropolítica nos Programas de Reconhecimento Facial*, Bárbara D'angeles Alves

Fagundes explora o impacto dos programas de reconhecimento facial na segurança pública do estado da Bahia. A autora procura demonstrar, criticamente, como essas tecnologias, inicialmente apresentadas como solução, acabaram por intensificar questões como racismo, xenofobia e preconceito de gênero, gerando um debate sobre sua aplicabilidade e consequências. Com isso, tem-se um paradoxo, pois o que seria uma solução, acabou apresentando-se como uma verdadeira ameaça à segurança pública. Para substanciar sua pesquisa, Bárbara parte das seguintes problemáticas: *a) como o direito e a tecnologia se integram na sociedade e no sistema judiciário brasileiro; b) o caminho que a tecnologia percorreu, apontando a sua (in)eficiência do sistema judiciário brasileiro, pela via da segurança pública, a possibilitar o acesso à justiça c) demonstrando que os resultados práticos tem sido mais quantitativos que qualitativos na utilização dessas ferramentas.*

No texto *A Relação entre Trabalhadores e Empresas de Aplicativos de Transporte de Pessoas e de Entregas*, os autores Francisco Alex de Oliveira, Gabriel Ap. Anizio Caldas e Gabriela Sroczynski Fontes, analisam a relação de trabalho entre os motoristas e entregadores de aplicativos e as empresas que os contratam.

Os autores investigam os requisitos caracterizadores da relação de emprego, destacando divergências jurisprudenciais e propostas legislativas em andamento sobre o tema. Destacaram a divergência entre Turmas do TST, estando em análise no Pleno daquele Tribunal. Destacam que, diante do impasse, *a CLT continua sendo o diploma legal que traz os requisitos caracterizadores do vínculo empregatício, que ao serem procurados na relação ora abordada, não foram encontrados cumulativamente, o que impede que os trabalhadores por intermediação de aplicativos sejam classificados como empregados*.

Já o quarto artigo desta edição traz um tema contemporâneo, tratando sobre *Criptoativos e Prevenção à Lavagem de Dinheiro: Governança Multissetorial como Instrumento de Compatibilização de Normas*. Nele, a autora Emiliane Alencastro discute o papel da governança multissetorial na prevenção à lavagem de dinheiro envolvendo criptoativos. A autora propõe que essa abordagem é fundamental para alinhar as

regulamentações antilavagem de dinheiro com a dinâmica dos criptoativos, garantindo sua eficácia e aceitabilidade.

No texto *Inteligência Artificial: Desafios para Regulação Jurídica*, os autores Eric Fiuza Bueno e Marcelo Fonseca Santos abordam os desafios da regulação da Inteligência Artificial na sociedade contemporânea. Os autores destacam a importância da normatização para mitigar problemas como viés, preconceito e segurança, discutindo métodos de regulação e iniciativas legislativas em andamento. Abordam, especialmente, sobre o Projeto de Lei 2.838/2023, que visa à regulação da IA no Brasil, para combater seu uso prejudicial.

A Proteção dos Robôs Sociais em Equiparação aos Animais, de Gabriel de Oliveira Cavalcanti Neto e Alexandre Freire Pimentel, exploram a possibilidade de estender direitos legais aos robôs sociais, equiparando-os aos animais. Os autores investigam como a antropomorfização e a capacidade de despertar empatia podem influenciar a disposição das pessoas em apoiar a proteção legal para esses robôs.

Destacam que *a percepção dos robôs sociais como entidades com características humanas e a capacidade de despertar empatia são fatores que podem influenciar a disposição das pessoas em apoiar a extensão da proteção legal a esses robôs, devendo-se considerar fatores psicológicos e emocionais nessa decisão, além de uma abordagem mais ampla para refletir sobre as implicações éticas e sociais do uso dessas tecnologias*.

No último artigo, sobre *A Importância da Propriedade Intelectual para o Desenvolvimento da Nova Tecnologia Non-Fungible Token (NFT)*, as autoras Luciana de Paula Soares e Suelen Bianca de Oliveira Sales, discorrem sobre a importância da propriedade intelectual no contexto da tecnologia *Non-Fungible Token* (NFT), destacando suas peculiaridades e aplicabilidades, bem como os desafios enfrentados na regulação e proteção jurídica desses ativos digitais.

Assim, pontuam sobre NFT: *O NFT é criado em Blockchain (tecnologia oriunda da criptomoeda Bitcoin), que garante a transparência e a imutabilidade do ativo digital. Por meio de plataformas próprias focadas em registro de jogos e obras de arte, as pessoas têm a possibilidade de registrar suas criações e comercializá-las dentro destes marketplaces, onde já aconteceram leilões milionários*.

Convidamos todos os interessados a mergulhar nesses fascinantes debates que marcam a interseção entre o direito e a tecnologia da informação, trazendo contribuições valiosas para o avanço e a compreensão dessas temáticas em constante evolução.

Boa leitura!

Emerson Wendt,

Editor-Chefe,

Mestre e Doutor em Direito pela Universidade La Salle – Canoas,

Delegado de Polícia Civil PCRS, membro do Conselho Superior de Polícia Civil/PCRS.

SUMÁRIO

ARTIGOS

INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS: FORMAS DE TUTELA JURÍDICA

PERSONAL DATA BREACHES: LEGAL REMEDIES

Sergio Marcos Carvalho de Avila Negri[1]

Carolina Fiorini Ramos Giovanini[2]

RESUMO

A partir do cenário de vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, abreviada como "LGPD") e do registro de ocorrência de diversos incidentes de segurança envolvendo dados pessoais, o presente artigo, a partir de uma abordagem exploratória, procura demonstrar diferentes formas de tutela que podem ser aplicadas diante de tais eventos. Considerando-se que a LGPD adota uma abordagem baseada no risco, buscou-se demonstrar que a tutela preventiva assume papel de especial relevância no ordenamento jurídico. No entanto, em que pese a adoção de medidas preventivas, é possível que incidentes de segurança ocorram e, nesses casos, procura-se apontar que a tutela específica poderá ser utilizada. Por fim, no que diz respeito à tutela ressarcitória em matéria de privacidade e proteção de dados, o presente artigo investiga os desafios de identificação do nexo causal e de demonstração e quantificação do dano, concluindo que meios alternativos de reparação não pecuniária devem ser avaliados nas situações concretas.

Palavras-chave: Incidentes de segurança; Lei Geral de Proteção de Dados; Proteção de dados; Tutela específica; Tutela ressarcitória.

ABSTRACT

Based on the enforcement of the Brazilian General Data Protection Law (Federal Law No. 13,709/2018, abbreviated as "LGPD") and the occurrence of several security incidents involving personal data, this paper, from an exploratory approach, seeks to demonstrate different forms of protection that can be applied in the face of such events. Considering that the LGPD adopts a risk-based approach, we seek to demonstrate that preventive protection plays a particularly important role in the legal system. However, despite the adoption of preventive measures, it is possible that security incidents may

[1] Professor da Faculdade de Direito da Universidade Federal de Juiz de Fora (UFJF) e do Corpo Permanente do PPGD em Direito e Inovação da UFJF. Mestre e Doutor em Direito Civil pela Universidade do Estado do Rio de Janeiro. Lattes: http://lattes.cnpq.br/3282764176353256.

[2] Mestranda em Direito e Inovação no PPGD da Universidade Federal de Juiz de Fora (UFJF). Pós-graduada em Direito Digital pelo CEPED/UERJ. Lattes: http://lattes.cnpq.br/3480301751804187.

occur, and, in these cases, we pointed out that the specific remedy can be used. Finally, regarding the compensation of damages in matters of privacy and data protection, this paper investigates the challenges of identifying the causal nexus and the demonstration and quantification of damage, concluding that alternative means of non-pecuniary compensation must be considered in concrete situations.

Keywords: Brazilian General Data Protection Law; Compensation for damages; Data protection; Security incidents; Specific remedy.

1 INTRODUÇÃO

Os primeiros anos de vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, abreviada como "LGPD") foram marcados pela ocorrência de incidentes de segurança. Fato é que, diariamente, observa-se o surgimento de notícias relatando falhas de segurança e exposição de dados pessoais no setor público e no setor privado, configurando um fato jurídico que justifica estudo aprofundado em razão das inúmeras questões técnicas, sociais e jurídicas, bem como potenciais violações de direitos fundamentais decorrentes de tais eventos.

Para além das preocupações decorrentes das atividades de tratamento de dados[3], o cenário de crescente utilização de dados pessoais coloca em evidência a importância de garantir que as informações sejam tratadas com segurança adequada, de modo a evitar danos patrimoniais e extrapatrimoniais aos titulares de dados[4], seja em perspectiva individual, seja em perspectiva coletiva.

Nesse contexto, a LGPD apresenta disciplina específica para a segurança dos dados pessoais: (i) reconhece a segurança como um dos princípios a serem observados em atividades de tratamento de dados pessoais (artigo 6º, VII); (ii) disciplina a

[3] O tratamento de dados é compreendido como qualquer operação envolvendo dados pessoais. Nesse sentido, o artigo 5º, inciso X, da LGPD define o tratamento como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[4] Titular de dados é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, conforme prevê o artigo 5º, inciso V, da LGPD.

responsabilidade dos agentes de tratamento[5] pelos danos decorrentes de violações de segurança (artigo 44, caput e parágrafo único); (iii) determina a adoção de medidas de segurança (Capítulo VII); e (iv) autoriza e incentiva a formulação de regras de boas práticas e de governança que estabeleçam normas de segurança (artigo 50).

Para além do aspecto jurídico, é importante notar que incidentes de segurança envolvendo dados pessoais podem gerar uma série de consequências para organizações, como quebra da confiança de clientes e investidores, impactos reputacionais, paralisação de operações e custos relacionados ao gerenciamento do evento e do cumprimento do dever de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, quando aplicável.

Em síntese, a ocorrência de um incidente de segurança poderá impactar ativos da organização e comprometer suas operações, sendo necessário direcionar esforços de prevenção. Além disso, caso tais eventos ocorram, é essencial que os agentes de tratamento tenham uma estrutura de governança em privacidade e proteção de dados, com rotinas e procedimentos internos formalizados, de modo que seja efetivamente possível implementar medidas de contenção e mitigação de riscos e potenciais danos.

Nesse contexto, o presente trabalho pretende analisar de que modo a tutela preventiva, a tutela específica e a tutela ressarcitória podem ser aplicadas a incidentes de segurança envolvendo dados pessoais. Para tanto, o trabalho será metodologicamente estruturado como uma pesquisa de abordagem exploratória, que busca delinear uma visão geral do problema, tornando-o evidente e compreensível (GIL, 2008).

Referida metodologia de pesquisa é adotada em razão do ainda curto período de vigência da LGPD e, consequentemente, do baixo número de posicionamentos da Autoridade Nacional de Proteção de Dados (ANPD)[6] em casos envolvendo incidentes de

[5] Os agentes de tratamento são os controladores e os operadores (art. 5º, IX, da LGPD). Em síntese, o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, da LGPD), tendo total autonomia para agir. Assim, o controlador atua em uma camada essencialmente estratégica, tomando decisões essenciais para o tratamento de dados. Por outro lado, o operador pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, da LGPD), sendo responsável somente por decisões operacionais e não essenciais.

[6] A Autoridade Nacional de Proteção de Dados é o órgão responsável por fiscalizar o cumprimento da Lei Geral de Proteção de Dados.

segurança. Desse modo, a partir da abordagem exploratória, busca-se uma familiaridade com o problema de pesquisa desenvolvido, com intuito de formulação de hipóteses mais robustas posteriormente.

Para tanto, o tema será desenvolvido a partir de análise das disposições da Lei Geral de Proteção de Dados, com o objetivo de investigar os conceitos delineados pela norma e as obrigações impostas aos agentes de tratamento. Em complementação, analisa-se a minuta de "Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais" divulgada pela ANPD para consulta pública.

Adota-se a estratégia de revisão bibliográfica de trabalhos que abordam a estrutura da disciplina de privacidade e proteção de dados na União Europeia e no Brasil, bem como trabalhos nacionais que abordam especificamente os incidentes de segurança à luz do ordenamento jurídico brasileiro.

Desse modo, a presente investigação pretende, em primeiro lugar, traçar os principais conceitos e referenciais teóricos que orientarão o desenvolvimento dos temas. Posteriormente, o trabalho discutirá possíveis formas de tutela jurídica passíveis de aplicação em situações de incidentes de segurança envolvendo dados pessoais.

2 PROTEÇÃO DE DADOS E INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS

A tutela jurídica de dados pessoais ganha cada vez mais relevância diante do crescente uso de dados pessoais em atividades econômicas. Nesse contexto, diversas normas sobre privacidade e proteção de dados surgiram ao redor do mundo, sendo que, de acordo com a Conferência das Nações Unidas sobre Comércio e Desenvolvimento, 137 de 194 países adotaram legislação sobre este tema.

No Brasil, foi publicada a Lei Geral de Proteção de Dados (Lei n° 13.709/2018, abreviada por "LGPD"), que estabelece regras para o uso lícito de dados pessoais. Acerca da norma, Negri e Korkmaz (2019) apontam que a LGPD é apresentada como imperativo da circulação controlada de dados pessoais, sendo um instrumento para a construção de uma cultura de proteção de dados no Brasil e, consequentemente, gerando mudanças

normativas no ordenamento jurídico nacional.

A relevância do tema é evidenciada na medida em que a proteção de dados passa a ser compreendida como um direito fundamental autônomo, que, inclusive, fornece instrumentos e garantias para o exercício de outros direitos, como a liberdade de expressão e a liberdade de associação. Nesse contexto, destaca-se que, em fevereiro de 2022 foi promulgada a Emenda Constitucional nº 115, consagrando expressamente o direito à proteção de dados como direito fundamental autônomo[7] no ordenamento jurídico brasileiro.

Ao tratar do direito à proteção de dados, é importante estabelecer sua relação com o direito à privacidade, que, em sua dimensão informacional, passa a ser compreendido como o direito de manter controle sobre as próprias informações (RODOTÀ, 2008). Tal compreensão é marcada pela noção de autodeterminação informativa, que, inclusive, é um dos fundamentos da disciplina de proteção de dados no Brasil, conforme artigo 2º, II, da LGPD, sendo concretizada pela implementação de instrumentos e práticas de *accountability* que assegurem o controle informacional por parte dos indivíduos.

A relação entre controle informacional e incidentes de segurança envolvendo dados pessoais é relevante porque incidentes de segurança são eventos marcados pela ocorrência de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados pessoais que, consequentemente, representam uma perda de controle informacional. Por tal razão, incidentes de segurança são situações que merecem atenção particular e ensejam a aplicação de proteções especiais, uma vez que, conforme apontava Doneda (2019), a disciplina da proteção de dados é marcada pela possibilidade de utilização combinada de formas de tutela jurídica.

É importante notar que nem todos os incidentes de segurança envolvem dados pessoais. Os dados pessoais[8] são informações que identificam uma pessoa natural

[7] Vale ressaltar que, no Brasil, em âmbito jurisprudencial o direito à proteção de dados já era reconhecido como direito fundamental autônomo, conforme decisão proferida pelo Supremo Tribunal Federal em sede da ADI 6.387 MC-Ref/DF, julgamento em 6 e 7.mai.2020.

[8] Em relação ao conceito de dados pessoais, destaca-se que alguns autores, como Pierre Catala e Massimo Durante, adotam o entendimento de que há uma distinção entre dado e informação na medida em que a informação seria alcançada apenas quando os dados passam por um processo de interpretação, ou seja, quando se atribui algum significado a eles. Por outro lado, para fins do presente trabalho, os termos

diretamente – como nome, CPF, RG e demais vínculos direitos – ou a tornam indiretamente identificável – por exemplo, número de telefone, geolocalização, número do cartão de crédito e outros vínculos indiretos. Ocorre que é possível que um incidente envolva somente informações que não são enquadradas nesta categoria jurídica, por exemplo, dados de pessoas jurídicas, informações referentes a segredo de negócio etc. Nesse contexto, faz-se necessário esclarecer que o presente trabalho busca investigar formas de tutela jurídica a serem aplicadas a eventos que efetivamente envolvam dados pessoais e atraiam a aplicação das disposições da LGPD.

A LGPD procurou endereçar em diversos dispositivos a importância da segurança das informações pessoais, mas não trouxe uma definição específica para conceituar o que seria um "incidente de segurança da informação envolvendo dados pessoais". Tal definição poderia ser extraída do princípio da segurança, previsto no artigo 6º, VII, da LGPD, segundo o qual um incidente de segurança seria quaisquer situações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Na mesma direção, a minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais divulgada pela ANPD para consulta pública conceitua o incidente de segurança com dados pessoais como qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.

Verifica-se que referido dispositivo é fundamentado pelos atributos da segurança da informação, quais sejam: (i) confidencialidade, isto é, garantia de que as informações sejam acessadas somente por aqueles que são devidamente autorizados; (ii) integridade, baseada na veracidade das informações, evitando perdas e alterações; e (iii) disponibilidade, ou seja, a garantia de que as informações estarão acessíveis às pessoas autorizadas. A definição trazida pela minuta divulgada pela ANPD considera também a autenticidade como uma das propriedades da segurança da informação, embora este não

"dados" e "informações" são compreendidos como sinônimos, uma vez que não se analisa atividades de tratamento e/ou processos decisórios que atribuem significado aos dados pessoais, mas tão somente a ocorrência de incidentes de segurança.

seja um elemento comumente reconhecido como atributo da segurança da informação. Menke e Goulart (2020) apontam, ainda, um quarto elemento: a resiliência, caracterizada pela capacidade de recomposição das estruturas e funcionalidades essenciais após a ocorrência de um evento adverso. Para fins de comparação, ressalta-se que, no âmbito da União Europeia, o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*, abreviado por "GDPR"), ao dispor sobre a segurança no tratamento de dados pessoais, elenca a resiliência como um dos atributos das medidas de segurança, ao lado da confidencialidade, da integridade e da disponibilidade.

Para Menke e Goulart (2020), os atributos de confidencialidade, integridade, disponibilidade e resiliência levam em consideração os conceitos de vulnerabilidade, ameaça, incidente e controle. A vulnerabilidade é caracterizada por ser uma fraqueza que atinge sistemas, ambientes, processos, protocolos etc., enquanto a ameaça é uma situação que explora vulnerabilidades e pode causar um evento de segurança classificado como incidente de segurança. Por fim, os controles são as medidas adotadas para impedir que um incidente ocorra ou para diminuir a probabilidade de sua ocorrência.

Ainda em relação à definição de incidente de segurança, a Autoridade Nacional de Proteção de Dados (ANPD), em suas orientações sobre o tema[9], esclarece que tal evento pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estão armazenados. Além disso, a ANPD destaca que a mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança, porém, a exploração da referida vulnerabilidade pode resultar em um incidente.

Observa-se que a definição adotada pela ANPD acertadamente restringe os incidentes somente aos eventos adversos confirmados, ou seja, a mera suspeita não é

[9] A ANPD publicou página de orientações sobre a comunicação de incidentes de segurança, porém, ressalta-se que tais orientações são recomendações e não se confundem com a regulamentação da comunicação de incidentes e especificação do prazo de notificação, que está prevista para a Fase 1 da Agenda Regulatória para o biênio 2023-2024. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de incidentes de segurança. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 07 mar. 2023.

categorizada como incidente de segurança com dados pessoais. Entende-se que tal restrição conceitual é adequada pois, caso contrário, o escopo da definição seria demasiadamente amplo, podendo, inclusive, ensejar comunicações desnecessárias à ANPD e aos titulares de dados.

Desse modo, a partir da definição de incidentes de segurança envolvendo dados pessoais e seus respectivos aspectos, buscar-se-á refletir acerca do papel da segurança da LGPD e, posteriormente, debater acerca das possíveis formas de tutela aplicáveis em tais situações. Para tanto, na próxima seção, são abordados os principais dispositivos para compreensão das regras traçadas pela LGPD em relação à segurança dos dados pessoais.

3 SEGURANÇA NA LEI GERAL DE PROTEÇÃO DE DADOS

A compreensão de que incidentes de segurança envolvendo dados pessoais merecem tutela jurídica especial por parte do ordenamento também passa pela análise dos dispositivos previstos na LGPD. Além do princípio da segurança, comentado anteriormente, a LGPD estabelece que agentes de tratamento ou demais entidades que venham a intervir no tratamento de dados pessoais devem garantir a segurança de tais informações, mesmo após o término do tratamento (*security by design*), conforme se extrai do artigo 47 da referida norma. Na mesma direção, o artigo 49 da LGPD estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, os princípios gerais previstos na norma e às demais normas regulamentares.

Vale destacar que, no âmbito da União Europeia, o *European Data Protection Board* (EDPB)[10], ao tratar da metodologia de *Privacy by Design*, esclarece que a segurança dos dados pessoais requer medidas adequadas destinadas a prevenir e gerenciar incidentes de violação de dados, bem como garantir a boa execução das atividades de

[10] O *European Data Protection Board* é um órgão independente da União Europeia cujo objetivo é garantir a aplicação do *General Data Protection Regulation* (GDPR), regulamento europeu que prevê regras para o uso de dados pessoais.

tratamento, o cumprimento dos demais princípios e o exercício efetivo dos direitos dos titulares.

O artigo 44, parágrafo único, da LGPD, estabelece que o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no artigo 46, der causa aos danos decorrentes da violação da segurança dos dados, responderá por sua conduta. Nesse sentido, Bioni e Dias (2020) apontam que a LGPD estabelece duas hipóteses para a configuração da responsabilidade civil dos agentes de tratamento de dados: a "violação à legislação de proteção de dados pessoais" e a "violação da segurança dos dados".

Tais hipóteses devem ser analisadas em conjunto à noção de tratamento irregular, compreendido como a situação na qual (i) o tratamento de dados pessoais deixa de observar a legislação; ou (ii) tratamento de dados pessoais não fornece a segurança que o titular pode esperar, conforme previsto no caput artigo 44 da LGPD. Nesse contexto, Bioni e Dias (2020) questionam se, em caso de violação da segurança dos dados, o agente seria responsabilizado (i) se não adotasse as medidas de segurança aptas a proteger os dados pessoais; ou (ii) se o tratamento não fornecesse a segurança que o titular dele pode esperar. Diante do questionamento apresentado, os autores entendem que a hipótese de adoção de medidas aptas é demasiadamente ampla e, por isso, apontam que a análise da segurança esperada pelo titular seria mais frutífera.

Embora Bioni e Dias (2020) entendam que a irregularidade do tratamento deve ser analisada com base nas legítimas expectativas de segurança que um titular médio pode esperar do tratamento de dados em questão, entende-se que é necessário considerar que a análise a partir da perspectiva do "titular médio" ainda ensejaria elevado nível de subjetividade – especialmente considerando que o conhecimento sobre padrões técnicos de segurança é essencialmente restrito aos profissionais que atuam na área – e, até mesmo, poderia contrariar parâmetros e boas práticas de segurança da informação.

Considerando tais argumentos, entende-se que a violação da segurança dos dados deve ser analisada a partir das justificativas técnicas que fundamentaram a adoção das medidas de segurança analisadas no caso concreto, isto é, quais orientações, boas práticas e parâmetros foram considerados ao estabelecer determinado nível de segurança (por

exemplo, natureza e volume de dados tratados, risco do tratamento, titulares de dados afetados etc.). Posteriormente, a partir da definição das medidas de segurança por parte do agente de tratamento, é possível construir a visão de confiança esperada pelo titular por meio do fornecimento de informações, advertências e instruções qualificadas, conforme apontam Menke e Goulart (2020).

Ainda que a LGPD tenha tratado das medidas de segurança e padrões técnicos de forma neutra e aberta, é importante que os agentes de tratamento estejam implementando tais ações conforme as operações que realizam. Palhares, Prado e Vidigal (2021) ressaltam que a liberdade de determinação de quais medidas de segurança serão adotadas não significa que padrões de segurança insuficiente serão legitimados pela LGPD, na verdade, tal abertura legislativa tem a função de assegurar que as medidas adotadas sejam compatíveis aos riscos presentes em cada contexto específico de tratamento de dados pessoais.

Inclusive, a ANPD poderá dispor sobre padrões técnicos mínimos, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia. Além disso, no que diz respeito ao tratamento de dados pessoais que ocorre por meio da Internet, haverá aplicação do Decreto n° 8.771/2016, que regulamenta o Marco Civil da Internet (Lei nº 12.965/2014). O artigo 13 do referido Decreto apresenta diretrizes sobre padrões de segurança, que devem ser observadas por provedores de conexão e de aplicações durante a guarda, armazenamento e tratamento de dados pessoais e comunicações privadas.

Ressalta-se que o Decreto n° 8.771/2016 já apresentava relevante preocupação com o acesso às informações e, consequentemente, com a construção da expectativa de segurança por parte do usuário, determinando que as informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, respeitado o direito de confidencialidade quanto aos segredos empresariais.

Em síntese, para fins de avaliação da irregularidade de determinada atividade de tratamento de dados pessoais, entende-se que é necessário avaliar, à luz do caso concreto,

as medidas de segurança adotadas e as respectivas justificativas técnicas para adoção, de modo a avaliar se tais medidas, de fato, poderiam ser consideradas aptas naquele contexto específico. Diante da definição das medidas de segurança, o agente de tratamento poderá contribuir para a construção da expectativa de segurança dos titulares por meio da implementação de medidas de transparência e disponibilização de informações sobre o tema.

Outra disposição relevante é a previsão de que o controlador deverá comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, conforme artigo 48 da LGPD. Observa-se que o dever de notificação previsto pela LGPD busca, de um lado, assegurar que a ANPD tenha ciência do ocorrido e possa atuar junto aos agentes de tratamento, determinando a adoção de medidas de contenção e providências que auxiliem na reversão ou mitigação dos efeitos decorrentes do incidente. Por outro lado, a comunicação aos titulares concretiza os preceitos de transparência e possibilita que os afetados adotem práticas mitigatórias e estejam atentos às possíveis consequências do incidente (por exemplo, tentativas de fraudes e golpes).

É importante notar que nem todos os incidentes de segurança envolvendo dados pessoais deverão ser notificados, mas somente aqueles que tenham o potencial de causar risco ou dano relevante aos titulares. No entanto, a LGPD não prevê critérios e metodologia para fins de avaliação do risco de incidentes de segurança envolvendo dados pessoais. Diante desse cenário, a ANPD iniciou, em 2021, o processo de regulamentação sobre incidentes de segurança, conforme prevê o artigo 48 da LGPD e como parte de sua agenda regulatória, aprovada pela Portaria nº 21 de 27 de janeiro de 2021.

Nesse contexto, a minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais divulgada pela ANPD para consulta pública apresenta critérios para avaliação de risco ou dano relevante, lista as informações que controladores devem apresentar à ANPD e aos titulares e define o prazo razoável para notificação do evento à ANPD e aos titulares. Ressalta-se que, até o presente momento, em que pese a divulgação da minuta do Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais para consulta pública, o processo de regulamentação ainda não foi

concluído. No entanto, ainda que não haja regulamentação do tema via resolução administrativa, a ANPD fornece aos agentes de tratamento uma página de orientações acerca do tema, caracterizadas como recomendações e, portanto, não vinculantes e obrigatórias.

A partir das orientações da ANPD, é possível extrair os seguintes fatores - não cumulativos - de avaliação de criticidade do incidente: (i) envolvimento de dados pessoais sensíveis, nos termos do artigo 5º, II, da LGPD; (ii) envolvimento de dados pessoais de indivíduos em situação de vulnerabilidade, como crianças, adolescentes e idosos; (iii) potencial de ocasionar danos materiais/morais aos indivíduos afetados; (iv) volume significativo de dados pessoais; (v) volume significativo de titulares afetados; (vi) intenções maliciosas da pessoa responsável pela concretização do evento; e (vii) facilidade de identificação dos indivíduos afetados pelo evento.

Além dos critérios elencados pela ANPD, destaca-se a existência de diversas metodologias para avaliação de criticidade de incidentes, desenvolvidas, por exemplo, por organizações do setor privado. Nesse sentido, ressalta-se a metodologia globalmente reconhecida e desenvolvida pela *European Union Agency for Network and Information Security* (ENISA), a qual considera os seguintes fatores: (i) contexto, compreendido como o elemento que analisa a natureza dos dados pessoais envolvidos no evento; (ii) facilidade de identificação, isto é, a probabilidade de os dados pessoais envolvidos no evento levarem à identificação dos indivíduos afetados; e (iii) circunstâncias do incidente, para fins de avaliação de eventual intenção maliciosa de exposição/tratamento inadequado dos dados pessoais envolvidos no evento.

No que diz respeito ao prazo para comunicação, a LGPD prevê que esta deverá ser realizada em "prazo razoável". A ANPD, em caráter de recomendação, orienta que, após a ciência do evento adverso e havendo risco relevante, a comunicação seja feita com a maior brevidade possível, indicando o prazo de 2 dias úteis, contados da data do conhecimento do incidente, prazo inspirado no Decreto nº 9936/2019, que regulamenta a Lei do Cadastro Positivo (Lei nº 12.414/2011).

Por sua vez, a minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais divulgada pela ANPD para consulta pública prevê que a

comunicação do incidente à ANPD e aos titulares deverá ser realizada no prazo de três dias úteis, contados do conhecimento do incidente de segurança. Possivelmente, referido prazo tem como referência o *General Data Protection Regulation* (GDPR) – legislação de proteção de dados vigente no âmbito da União Europeia – que prevê o prazo de 72 horas.

Além disso, é interessante notar que, à luz da LGPD, incidentes de segurança podem desencadear uma série de violações às normas de proteção de dados, indo além das disposições relacionadas à comunicação do evento aos titulares e à ANPD. A título de exemplificação, incidentes que acarretem alteração de dados pessoais ensejam violação ao princípio da qualidade (artigo 6º, V, da LGPD), assim como incidentes que tenham como consequência a perda de dados pessoais podem inviabilizar o atendimento de direitos exercidos pelos titulares (artigo 18, da LGPD).

Nessa direção, o *European Data Protection Board* aponta que as violações de dados são problemas em si, mas também podem ser sintomas de um regime de segurança de dados vulnerável e possivelmente insuficiente. Portanto, a implementação de medidas de segurança e padrões técnicos adequados durante todo o ciclo de vida dos dados pessoais é essencial, de modo que a segurança deve ser um fator considerado antes mesmo do início das atividades de tratamento.

Desse modo, constata-se que, sob a perspectiva da LGPD, há a exigência de adoção de medidas de segurança técnicas e administrativas, o que pressupõe uma estrutura de governança em privacidade e proteção de dados. A partir deste contexto, questiona-se quais seriam as possíveis formas de tutela jurídica aplicáveis a incidentes de segurança envolvendo dados pessoais.

4 TUTELA PREVENTIVA: DIÁLOGOS ENTRE PREVENÇÃO, PRECAUÇÃO E ABORDAGEM BASEADA NO RISCO

A LGPD estabelece o princípio da prevenção (artigo 6º, VIII), segundo o qual é necessário observar a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Nesse sentido, a partir de uma interpretação sistemática

da LGPD, é possível compreender que o agente de tratamento deverá agir com cautela e adotar as medidas de segurança aptas a prevenir a ocorrência de incidentes de segurança.

Para além da prevenção, expressamente prevista pela LGPD, o princípio da precaução também pode ser observado no ordenamento jurídico brasileiro. Bioni e Luciano (2019) apontam que o princípio da precaução surge em decorrência da insuficiência dos métodos tradicionais de regulação de risco diante de incertezas. Tal princípio originou-se na década de 1970 a partir de iniciativas de proteção ambiental que buscavam evitar danos ambientais marcados pela incerteza e indeterminação do tipo de dano.

No âmbito da privacidade e da proteção de dados, a aplicação do princípio da precaução poderá contribuir para a consolidação de uma abordagem baseada no risco (*risk based approach*). Tal abordagem é comumente adotada por normas de proteção de dados, inclusive pela LGPD, e, assim como o princípio da precaução, está relacionada a condutas baseadas em prudência e transparência. Nesse sentido, a partir de uma abordagem baseada no risco, os agentes de tratamento devem implementar rotinas de avaliação de riscos em atividades de tratamento de dados pessoais e endereçar as medidas para mitigação dos riscos identificados.

Costa (2012) aponta que, pelo princípio da precaução, em situações nas quais existam ameaças de danos graves ou irreversíveis, mesmo que não haja plena certeza científica, é necessário tomar medidas de proteção sem esperar que esses riscos se tornem plenamente aparentes. Nessa direção, o autor destaca que a avaliação de risco e o princípio da precaução são instrumentos que caminham juntos, pois determinam conjuntamente a atribuição da avaliação dos riscos e do custo dos danos.

Em relação à matéria de privacidade e proteção de dados, o princípio da precaução apresenta-se como uma garantia contra riscos potenciais que, no atual momento do tratamento de dados pessoais, podem não ser identificados. Para Costa (2012) o princípio da precaução beneficia a proteção da privacidade na medida em que coloca em evidência os valores normativos de prudência e transparência, criando para os agentes de tratamento um dever de cuidado. Conjuntamente, prudência e precaução implicam que as atividades devem ser realizadas de forma a evitar que seus potenciais efeitos prejudiciais atinjam

outras pessoas, possibilitando a realização do tratamento de dados pessoais com segurança.

Considerando-se especificamente os incidentes de segurança da informação envolvendo dados pessoais para uma leitura sob a ótica do princípio da precaução, verifica-se que tais eventos são marcados pela incerteza técnica de sua ocorrência, porém, isso não elimina a necessidade de implementar medidas que possam prevenir a ocorrência de incidentes e, consequentemente, evitar potenciais danos aos titulares de dados.

Nessa direção, ressalta-se o artigo 47 da LGPD, que estabelece o dever de garantir a segurança da informação em relação aos dados pessoais, mesmo após o término do tratamento. Conforme mencionado anteriormente, esta abordagem – também denominada *security by design* – exige que os agentes de tratamento considerem os requisitos de segurança durante todo o ciclo de vida das informações, isto é, desde o momento inicial de concepção da atividade até o momento de encerramento e eliminação dos dados pessoais envolvidos, prevenindo a ocorrência de danos.

Entende-se que os agentes de tratamento devem adotar medidas, rotinas e práticas que contribuam para a efetivação do princípio da prevenção e concretizem a tutela preventiva em matéria de privacidade e proteção de dados pessoais. O desenvolvimento e a efetiva implementação de normas e procedimentos internos (como a política de segurança da informação) que estabeleçam medidas e padrões de segurança a serem adotados, regras para uso de sistemas, acesso a instalações e equipamentos também é essencial para incorporar a tutela preventiva nas rotinas de uma organização.

Além disso, é necessário assegurar que eventuais terceiros envolvidos em atividades de tratamento, como prestadores de serviços e parceiros, adotem padrões de segurança adequados. Por tal razão, a gestão de terceiros deve ser incorporada como uma forma de tutela preventiva, evitando que agentes de tratamento que não adotam medidas de segurança adequadas sejam engajados nas cadeias de atividades que envolvem dados pessoais.

Nessa direção, Menke e Goulart (2020) apontam que a segurança é aplicada aos sistemas e estruturas utilizadas no tratamento de dados (medidas técnicas) e ao ambiente geral do agente de tratamento (medidas organizativas), de modo que a adoção de medidas

técnicas não será suficiente se não for complementada por rotinas essencialmente organizacionais, como os treinamentos e as políticas internas. Portanto, a atuação preventiva do agente de tratamento é concretizada não só a partir de padrões técnicos, mas também por meio de uma estrutura de governança sólida.

5 TUTELA ESPECÍFICA: O INCIDENTE DE SEGURANÇA COMO MOMENTO PATOLÓGICO DA RELAÇÃO CONTRATUAL

Ainda que os agentes de tratamento atuem preventivamente, a ocorrência de incidentes de segurança é possível. Inclusive, por vezes, tais eventos estão relacionados a elementos externos, como a atuação de outros agentes na cadeia de tratamento de dados pessoais. Assim, para além das rotinas e medidas que buscam prevenir a ocorrência de incidentes de segurança, também é necessário analisar eventuais cláusulas contratuais relacionadas à atividade de tratamento de dados pessoais.

Um contrato que define direitos e deveres relacionados ao tratamento de dados pessoais poderá prever cláusulas que disponham sobre a adoção de medidas de segurança e ações a serem tomadas em caso de incidentes de segurança. Por exemplo, no caso de uma relação entre controlador e operador, é possível estipular cláusula contratual para que, em caso de indícios de ocorrência de incidente de segurança, o operador notifique o controlador acerca da situação. Por outro lado, no caso de relações entre controladores, cita-se a possibilidade de previsão de cláusula contratual que estabelece o dever de comunicação acerca da suspeita de incidente de segurança, bem como cláusulas sobre tomada de decisão conjunta acerca das medidas necessárias para contenção e prestação de auxílio mútuo.

Diante do contexto de definição de obrigações contratuais, ressalta-se que Negri (2021) aponta que o caráter dinâmico da relação obrigacional coloca em evidência o fato de que o adimplemento está relacionado a execução da prestação em toda sua complexidade, incluindo os deveres anexos inerentes à complexidade intra-obrigacional. Em síntese, é importante notar que o adimplemento não mais se confunde com a mera realização da prestação principal, podendo ocorrer também em razão de deveres anexos.

Ao trazer esta discussão para o âmbito da privacidade e da proteção de dados pessoais, nota-se que é possível que a prestação principal relacionada a um tratamento de dados seja cumprida, mas o dever de segurança – que visa impedir a ocorrência de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão – seja descumprido. Em cenários como este narrado, ainda que a prestação principal relacionada ao tratamento de dados pessoais tenha sido cumprida, o descumprimento do dever anexo de segurança caracteriza inadimplemento.

Diante da possibilidade de previsão de cláusulas contratuais acerca da segurança dos dados em relações envolvendo atividades de dados pessoais, faz-se necessário refletir sobre as consequências de eventual inadimplemento, uma vez que o incidente de segurança poderá ser compreendido como um momento patológico da relação contratual se originado pelo descumprimento dos deveres de segurança estabelecidos pelas partes. Nesse contexto, o ordenamento jurídico brasileiro prevê diferentes remédios passíveis de aplicação em situações envolvendo inadimplemento.

O Artigo 389 do Código Civil estabelece que, caso a obrigação não seja cumprida, o devedor responderá por perdas e danos, mais juros e atualização monetária segundo índices oficiais regularmente estabelecidos, e honorários de advogado. No entanto, ressalta-se que tal dispositivo não deve ser interpretado no sentido de que a tutela ressarcitória seria o único ou o principal remédio para casos de inadimplemento contratual. Na verdade, verifica-se que a tutela ressarcitória é subsidiária, enquanto o principal remédio disponibilizado pelo ordenamento jurídico é o cumprimento específico da obrigação, ou seja, o cumprimento daquilo que foi contratualmente prometido.

Nesse sentido, o artigo 499 do Código de Processo Civil determina que a obrigação somente será convertida em perdas e danos se o autor o requerer ou se impossível a tutela específica ou a obtenção de tutela pelo resultado prático equivalente. Na mesma direção, o parágrafo primeiro do artigo 84 do Código de Defesa do Consumidor estabelece que a conversão da obrigação em perdas e danos somente será admissível por opção do autor ou em caso de impossibilidade de tutela específica ou de obtenção do resultado prático correspondente.

Verifica-se, portanto, que a tutela específica é o principal remédio para a promoção da tutela satisfativa da obrigação em concreto, enquanto a tutela ressarcitória assume caráter subsidiário ou complementar. Tepedino (2012) destaca que deve ser atribuído ao credor exatamente aquilo que lhe foi estabelecido contratualmente, ou seja, a prioridade é a execução *in natura* e, caso seja verificada a impossibilidade de execução específica, busca-se alcançar o resultado prático equivalente e, somente em último caso, a reparação por perdas e danos.

Inclusive, mesmo no caso da obrigação de fazer (por exemplo, obrigação de implementar determinadas medidas de segurança durante o tratamento de dados pessoais), a tutela obrigacional não está atada à tutela ressarcitória. Fato é que, atualmente, o ordenamento jurídico conta com mecanismos de execução indireta para persuadir o agente inadimplente a realizar o comportamento pactuado.

Nesse sentido, o artigo 536 do Código de Processo Civil estabelece que, no cumprimento de sentença que reconheça a exigibilidade de obrigação de fazer ou de não fazer, o juiz poderá, de ofício ou a requerimento, determinar, entre outras medidas, a imposição de multa, a busca e apreensão, a remoção de pessoas e coisas, o desfazimento de obras e o impedimento de atividade nociva, podendo, caso necessário, requisitar o auxílio de força policial.

É inegável que, a depender do caso concreto, a execução específica da obrigação restará prejudicada, por exemplo, quando se verificar em concreto a impossibilidade da prestação. A título de exemplificação, é possível imaginar cenário no qual há obrigação de devolução dos dados pessoais envolvidos na atividade, porém, tais dados foram apagados em razão da ocorrência de incidente de segurança e não há um *backup*. Neste exemplo, observa-se a impossibilidade de execução específica da obrigação de devolução dos dados pessoais em razão da perda de disponibilidade e integralidade, gerada pelo incidente de segurança.

Desse modo, nos casos de inadimplemento absoluto, além da execução pelo equivalente, a parte lesada pelo inadimplemento possui o direito potestativo de resolver o contrato, havendo a extinção da relação obrigacional, cabendo em qualquer dos casos, indenização por perdas e danos, conforme artigo 475 do Código Civil. Ressalta-se que a

qualificação do inadimplemento como absoluto ou relativo não é uma escolha das partes, trata-se, na verdade, de uma qualificação que decorre do fato objetivo de a prestação ter ou não se tornado inútil à parte lesada pelo inadimplemento, ou ter ou não se impossibilitado para a parte inadimplente.

Tratando-se do tema de privacidade e proteção de dados pessoais, é possível que – em relações contratuais – um agente de tratamento envolvido na atividade ou o próprio titular de dados peça a execução específica de cláusulas contratuais, com destaque para aquelas que envolvem a adoção de medidas de segurança adequadas, o dever de comunicação sobre incidentes de segurança envolvendo dados pessoais e a prestação de auxílio mútuo diante da ocorrência de tais eventos, conforme mencionado anteriormente.

Especificamente em relação à tutela coletiva, Zanatta e Souza (2019) apontam que, a partir da interpretação conjunta da Lei da Ação Civil Pública (Lei nº 7.347/1985), do Código de Defesa do Consumidor (Lei nº 8.078/1990) e da LGPD, observa-se que a ação civil pública poderá ser proposta não só para a reparação de danos, mas também para a obtenção da tutela específica, ou seja, aplicando-se também uma tutela inibitória coletiva. No caso de situações envolvendo somente a tutela individual da proteção de dados, entende-se que o racional de possibilidade de obtenção da tutela específica também seria aplicável.

Na mesma direção e, especificamente no que diz respeito aos direitos da personalidade, observa-se o enunciado 140 na III Jornada de Direito Civil, promovida pelo Centro de Estudos Judiciários do Conselho da Justiça Federal, em 2004, segundo o qual a primeira parte do artigo 12 do Código Civil refere-se às técnicas de tutela específica, aplicáveis de ofício, enunciadas no artigo 461 do Código de Processo Civil (nesse caso, faz-se referência ao CPC de 1973), devendo ser interpretada com resultado extensivo.

Desse modo, verifica-se que a tutela específica poderá estar presente em situações individuais ou coletivas, envolvendo relações contratuais travadas entre agentes de tratamento e entre agentes de tratamento e titulares de dados. Em relação aos incidentes de segurança envolvendo dados pessoais, é possível vislumbrar – exemplificativamente, uma vez que a tutela específica varia a depender das peculiaridades do caso concreto –

obrigações como (i) a adoção de medidas voltadas para a contenção do incidente; (ii) atividades de monitoramento e varredura para remoção de bancos de dados expostos na *web* e na *deep web*; (iii) a criação de página e canal de comunicação específico para orientações acerca do incidente; (iv) o dever de comunicação previsto pelo artigo 48 da LGPD etc.

O direito privado, ao priorizar a tutela específica das obrigações, deixou de lado a compreensão de que obrigações de fazer e não fazer seriam inexequíveis. Ainda que não haja previsão expressa de mecanismos típicos de tutela específica, esta assume o papel de principal remédio para o inadimplemento contratual. Esse é um cenário relevante para relações contratuais envolvendo o tratamento de dados pessoais, especialmente diante de cláusulas que estabeleçam deveres anexos de segurança.

5 TUTELA RESSARCITÓRIA: SUBSIDIARIEDADE E POSSIBILIDADES DE REPARAÇÃO NÃO PECUNIÁRIA

Conforme se procurou demonstrar, a tutela ressarcitória, concretizada a partir da verificação das perdas e danos e consequente indenização, assume caráter subsidiário no ordenamento jurídico brasileiro. Em que pese a possibilidade de tutelar a privacidade e a proteção de dados por meio da responsabilidade civil, é necessário reconhecer que a tutela ressarcitória não deve ser o principal instrumento de tutela, privilegiando-se uma atuação específica em prol da pessoa humana.

Nesse sentido, de acordo com Doneda (2019), a tutela baseada na responsabilidade civil oferece uma visão predominantemente patrimonialista do problema. Desse modo, entende-se que a lesão à personalidade humana, por estar relacionada aos interesses existenciais, não é compatível com a mera recondução do prejudicado ao estado anterior.

Em que pese a subsidiariedade da tutela ressarcitória, sua análise é importante e assume especial relevância em situações nas quais se verifica a impossibilidade da tutela específica. Nesse sentido, a LGPD estabelece que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano

patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, nos termos do artigo 42, da LGPD.

Desse modo, considerando-se os elementos da responsabilidade civil, é necessário que, no caso concreto, seja verificada a existência de um dano. A demonstração do dano é o primeiro desafio a ser enfrentado para responsabilização em matéria de privacidade e proteção de dados. Nessa direção, Citron e Solove (2020) apontam que os tribunais reconhecem impactos menores porque são tangíveis, mas deixam de reconhecer problemas graves relacionados à privacidade porque, geralmente, são marcados pela intangibilidade.

Em segundo lugar, Citron e Solove (2020) chamam atenção para o fato de que, por vezes, os danos à privacidade são pequenos, mas numerosos. Tais danos podem atingir o mesmo indivíduo diversas vezes, mas em razão da conduta de diferentes atores e, consequentemente, se tornarem significativamente mais prejudiciais. Por outro lado, também é possível que uma organização cause um dano pequeno, mas em escala muito grande, atingindo diversos indivíduos, sendo que, nesses casos, do ponto de vista de cada indivíduo, o dano é mínimo, mas há uma agravação pela agregação.

Citron e Solove (2020) esclarecem, ainda, que o dano pode não ser totalmente reconhecível por estar na forma de um risco futuro de lesões, que podem ser variadas, ou seja, o dano poderá vir a se manifestar somente no futuro. Por fim, os autores destacam que o desafio relacionado ao fato de que os danos à privacidade geralmente envolvem não apenas os interesses individuais, mas também interesses coletivos.

Para além dos desafios relacionados à demonstração do dano, nota-se que a aferição do nexo causal também poderá ser particularmente complexa. Por exemplo, em relação aos incidentes de segurança, Schreiber (2021) ressalta que, por vezes, um vazamento de dados pessoais envolverá sucessivas transferências ou apropriações de dados, de modo que a fonte originária de dados pessoais expostos indevidamente nem sempre é passível de identificação.

Desse modo, em relação aos incidentes de segurança envolvendo dados pessoais, é importante que, no caso concreto, seja possível demonstrar (i) a existência de dano gerado pelo evento; e (ii) o nexo de causalidade entre o dano sofrido e o incidente de

segurança. Nesse sentido, o parágrafo único do artigo 44 da LGPD estabelece que o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no artigo 46, der causa aos danos decorrentes da violação da segurança dos dados, responderá por tais danos.

Acerca deste tema, em que pese a relevância da reparação civil, é importante notar que o cenário de banalização das condenações – no qual é possível verificar diminuição de valores, confusões entre critérios patrimoniais e existenciais – demanda reflexões acerca da despatrimonialização da reparação, conforme ensina Konder (2021), isto é, meios não pecuniários que podem ser aplicados para maximizar a promoção de interesses existenciais.

Nesse sentido, destaca-se que o Supremo Tribunal Federal já entendeu que os mecanismos de reparação *in natura* permitem a tutela mais efetiva dos direitos fundamentais, sendo plenamente compatíveis com a Constituição Federal, que assegura o direito à indenização pelos danos morais, mas não elege um meio específico para efetivação do ressarcimento, ou seja, nem sempre é necessário realizar a reparação pecuniária, havendo margem para discussão sobre métodos de reparação não pecuniária.

O enunciado 589 da VII Jornada de Direito Civil, realizada pelo Conselho da Justiça Federal, ao tratar da interpretação da cláusula geral de responsabilidade civil prevista no caput do artigo 927 do Código Civil, estabelece que a compensação pecuniária não é o único modo de reparar o dano extrapatrimonial, sendo admitida a reparação *in natura*, na forma de retratação pública ou outro meio.

Como bem sintetiza Leonardo Fajngold (2021), a reparação não pecuniária pode ser compreendida a partir das situações nas quais a reparação de um dano extrapatrimonial não consiste na transferência de dinheiro à vítima com o objetivo de incremento do seu capital. O autor destaca que a lógica não pecuniária não significa que os mecanismos a serem empregados não possuem expressão patrimonial. Na verdade, nota-se que a implementação de mecanismos de reparação não pecuniária, em regra, gera custos pecuniários ao ofensor.

No âmbito da privacidade e da proteção de dados pessoais, observa-se que incidentes de segurança podem vir a causar danos de natureza patrimonial (por exemplo,

perdas financeiras, perda de oportunidades e demais situações passíveis de valoração econômica) ou extrapatrimonial, como danos à reputação, discriminação e restrições de liberdades civis.

O dano extrapatrimonial decorrente de um incidente de segurança envolvendo dados pessoais representa a lesão a um interesse jurídico referente à personalidade humana. Por exemplo, Citron e Solove (2020) apontam que as violações de privacidade podem causar danos ao inibir as pessoas de exercerem a liberdade de expressão e de se envolverem em atividades políticas, religiosas e associativas. Os autores ressaltam, inclusive, que tais violações podem ser especialmente impactantes para mulheres, minorias e grupos marginalizados, dada a vigilância desproporcional que recai sobre esses grupos.

Em tais situações, o movimento de deslocamento do foco do direito privado para a pessoa, coloca em evidência a necessidade de adotar formas de tutela que possibilitem a máxima promoção dos interesses existenciais. Como esclarece Fajngold (2021), uma forma de reparação não pecuniária pode ter maior aptidão reparatória do que o mero recebimento de uma determinada quantia.

Desse modo, entende-se que o debate sobre a aplicação de mecanismos de reparação não pecuniária diante de danos gerados por incidentes de segurança envolvendo dados pessoais é essencial. Por vezes, diante da perda de confidencialidade, integridade ou disponibilidade de dados pessoais, a tutela *in natura* se apresentará como meio que possibilita a maior promoção dos interesses existenciais dos titulares envolvidos em determinado incidente.

Portanto, em que pese a existência de diversos mecanismos voltados para a tutela preventiva e a possibilidade de exigência de tutela específica, a tutela ressarcitória também representa papel relevante para a efetivação dos preceitos da lei. Especificamente no campo da reparação de danos extrapatrimoniais, caberá refletir acerca das possibilidades de reparação não pecuniária diante de incidentes de segurança envolvendo dados pessoais e empreender esforços para assegurar a adequada tutela de interesses existenciais.

6 CONSIDERAÇÕES FINAIS

O crescente uso de tecnologias e o aumento do fluxo informacional são fatores que impulsionam o tratamento de dados pessoais. Evidentemente, na sociedade de informação, as relações evoluíram e são travadas em ambientes digitais cada vez mais complexos e dinâmicos. Nesse contexto, é possível observar – em diversos setores, no setor público e no setor privado, em organizações de portes variados – um crescente número de ataques cibernéticos e incidentes de segurança envolvendo dados pessoais.

A partir do cenário de vigência da Lei Geral de Proteção de Dados e aumento da ocorrência de incidentes de segurança envolvendo dados pessoais, procurou-se demonstrar que, diante da ocorrência de incidentes de segurança envolvendo dados pessoais, é possível aplicar diferentes formas de tutela, que oferecem respostas mais eficazes aos efeitos gerados por estes eventos e, consequentemente, oferecer melhor proteção aos interesses jurídicos.

A tutela preventiva assume especial relevância na LGPD, que adota abordagem baseada no risco e institui mecanismos de avaliação de riscos à proteção de dados. Inclusive, para fins de verificação da necessidade de comunicar a ocorrência de um incidente à ANPD e aos titulares, é necessário avaliar se tal incidente pode acarretar risco ou dano relevante aos titulares. Nesse contexto, foi demonstrado que a participação da Autoridade Nacional e a divulgação do fato aos titulares também poderá contribuir para a adequada tutela da proteção de dados.

Em relação à tutela contratual, procurou-se demonstrar que a tutela específica deve ser considerada como o principal remédio em casos de inadimplemento dos deveres contratuais, incluindo deveres anexos. Desse modo, entende-se que, diante da ocorrência de incidentes, deve-se buscar, primeiramente, o resultado que decorreria do cumprimento da obrigação estabelecida, caso seja verificada utilidade e possibilidade desta prestação.

Por fim, foram abordados os desafios da tutela ressarcitória, caracterizada pela determinação das perdas e danos, em matéria de privacidade e proteção de dados, demonstrando-se que esta não deve ser considerada como o único ou o principal remédio para situações envolvendo incidentes de segurança com dados pessoais.

Portanto, procurou-se demonstrar que a construção de uma cultura de proteção de dados e a efetivação da proteção da privacidade da pessoa humana dependem de instrumentos de tutela adequados para incidentes de segurança. As formas de tutela em matéria de privacidade e proteção de dados não devem se resumir aos pedidos de indenização pecuniária, pelo contrário, é necessário considerar a abordagem baseada no risco para implementar formas de tutela preventiva e, em caso de ocorrência de incidentes, avaliar as possibilidades de tutela específica no caso concreto.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Comunicação de incidentes de segurança**. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 07 mar. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Minuta de Regulamento de Comunicação de Incidentes com Dados Pessoais. **Consulta Pública Plataforma Participa + Brasil**. Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-comunicacao-de-incidente-de-seguranca-com-dados-pessoais#:~:text=A%20ANPD%20determinar%C3%A1%20ao%20controlador,tenha%20sido%20comunicado%20pelo%20controlador. Acesso em: 21 jun. 2023.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/. Acesso em: 07 mar. 2023.

BIONI, Bruno; LUCIANO, Maria. O princípio da precaução da regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência Artificial e Direito**. São Paulo: Thomson Reuters Brasil, 2019. p. 207-232.

CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy Harms. **Boston University Law Review**, Boston, v. 102, p. 1-62, 2021. Disponível em: https://ssrn.com/abstract=3782222. Acesso em: 07 mar. 2023.

CONSELHO DA JUSTIÇA FEDERAL. **III Jornada de Direito Civil**. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/iii-jornada-de-direito-civil-1.pdf. Acesso em: 07 mar. 2023.

CONSELHO DA JUSTIÇA FEDERAL. **VII Jornada de Direito Civil**. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/vii-jornada-direito-civil-2015.pdf. Acesso em: 07 mar. 2023.

COSTA, Luiz. Privacy and the precautionary principle. **Computer Law & Security Review**, v. 28, n. 1, p. 14-24, 2012. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364911001804?via%3Dihub. Acesso em: 31 jan. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 4/2019 on Article 25 Data Protection by Design and by Default**. Disponível em https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en. Acesso em: 07 mar. 2023.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. **Recommendations for a methodology of the assessment of severity of personal data breaches**. Disponível em: https://www.enisa.europa.eu/publications/dbn-severity. Acesso em: 07 mar. 2023.

FAJNGOLD, Leonardo. **Dano moral e reparação não pecuniária**: sistemática e parâmetros. São Paulo, Thomson Reuters Brasil, 2021.

KONDER, Carlos Nelson. Prefácio. *In*: FAJNGOLD, Leonardo. **Dano moral e reparação** não pecuniária: sistemática e parâmetros (prefácio). São Paulo, Thomson Reuters Brasil, 2021.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. *In*: DONEDA, Danilo et al (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 339-360.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral De Proteção De Dados: ampliação conceitual e proteção da pessoa humana. **Revista de Direito, Governança e Novas Tecnologias**, Goiânia, v. 5, n. 1, p. 63-85, jun. 2019, p.81.

Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 3 jan. 2023.

NEGRI, Sergio Marcos Carvalho de Avila. A tutela específica nos contratos de computação em nuvem (cloud computing). *In*: TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz (org.). **Inexecução das Obrigações Volume II**: pressupostos, evolução e remédios. Rio de Janeiro: Processo, 2021. p. 967-988.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. **Compliance Digital e LGPD**. Coleção Compliance. Coord. NOHARA, Irene; Almeida, Luiz Eduardo. São Paulo: Thomson Reuters Brasil, 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. **Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais**. *In*: DONEDA, Danilo et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 319-338.

TEPEDINO, Gustavo. **Inadimplemento contratual e tutelas específicas das obrigações**. Soluções práticas de direito. São Paulo: Revista dos Tribunais, v. II, 2012.
UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Data Protection and Privacy Legislation Worldwide**. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 3 jan. 2023.

ZANATTA, Rafael; SOUZA, Michel. A tutela coletiva na proteção de dados pessoais: tendências e desafios. *In*: DE LUCCA, Newton; ROSA, Cíntia. **Direito & Internet IV**: Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.

OS "NOVOS OLHOS" DA SEGURANÇA PÚBLICA DA BAHIA: RÚIDOS DE UMA NECROPOLÍTICA NOS PROGRAMAS DE RECONHECIMENTO FACIAL

THE "NEW EYES" OF PUBLIC SECURITY IN BAHIA: NOISES OF A NECROPOLICY IN FACIAL RECOGNITION PROGRAMS

Bárbara D'angeles Alves Fagundes[1]

Patrick Wendell Teixeira Fernandes [2]

RESUMO

A garantia da manutenção da segurança pública é compromisso primordial em todos os estados brasileiros. Nesse intuito, o estado da Bahia, buscando promover ações de segurança pública, investiu milhões na implantação de programas de reconhecimento facial no território baiano, denominados de "novos olhos da segurança pública". Paradoxalmente, o que seria uma possível solução acabou apresentando-se como uma verdadeira ameaça à segurança pública, operando racismo, classicismo, xenofobia e preconceito de gênero como principais resultados dessa investida, surgindo então o debate da utilização dessas tecnologias, levantando um debate sobre como deve se dar a sua aplicabilidade, e de que modo a sua má utilização, como na situação em comento, pode intensificar uma necropolítica no território baiano. Para tanto, traça-se uma metodologia de revisão bibliográfica, partindo de problemáticas: a) como o direito e a tecnologia se integram na sociedade e no sistema judiciário brasileiro; b) o caminho que a tecnologia percorreu, apontando a sua (in)eficiência do sistema judiciário brasileiro, pela via da segurança pública, a possibilitar o acesso à justiça c) demonstrando que os resultados práticos tem sido mais quantitativos que qualitativos na utilização dessas ferramentas. Por fim entrelaça-se a utilização dos sistemas de reconhecimento facial com o enviesamento algorítmico, o que resulta em uma política de extermínio e vilanização de corpos negros e pobres.

Palavras-chave: big data; enviesamento algorítmico; necropolitica; reconhecimento facial; segurança pública.

[1] Mestre em Direito pelo PPGD -UniFG enquanto bolsista e pesquisadora da Fundação de Amparo à Pesquisa do Estado da Bahia (FAPESB). Graduada em Direito pelo Centro Universitário UniFG. Pesquisadora do Centro de Estudos sobre Acesso à Justiça (CAJU). Lattes: http://lattes.cnpq.br/0646316056898987.

[2] Graduado em Direito pelo Centro Universitário UNIFG. Graduado em Licenciatura em História pela Universidade do Estado da Bahia.Lattes: http://lattes.cnpq.br/4851652863645276.

ABSTRACT

Ensuring the maintenance of public safety is a primary commitment in all Brazilian states. To this end, the state of Bahia, seeking to promote public security actions, invested millions in the implementation of facial recognition programs in the Bahian territory, called “new eyes of public security”. Paradoxically, what would have been a possible solution ended up presenting itself as a true threat to public security, with racism, classicism, xenophobia and gender prejudice as the main results of this onslaught, giving rise to the debate on the use of these technologies, raising a debate about how its applicability must be considered, and how its misuse, as in the situation under discussion, can intensify necropolitics in the Bahian territory. To this end, a bibliographic review methodology is outlined, based on issues: a) how law and technology are integrated into society and the Brazilian judicial system; b) the path that technology has taken, pointing out its (in)efficiency of the Brazilian judicial system, through public security, enabling access to justice c) demonstrating that the practical results have been more quantitative than qualitative in the use of these tools. Finally, the use of facial recognition systems is intertwined with algorithmic bias, which results in a policy of extermination and villainization of black and poor bodies.

Keywords: big data; algorithmic bias; necropolitics; facial recognition; public security.

1 INTRODUÇÃO

A utilização de inteligência artificial na sociedade é algo que se faz cada dia mais presente, não mais como uma promessa futura, mas imposição atual, dinamizando-se pelas mais diversas veias, sobretudo do poder público, que necessita do manejo e controle de dados e informações de milhares de pessoas, todos os dias. A segurança pública, nesse contexto, sempre esteve vinculada às mais simples formas de tecnologia, justamente por ser um dos setores que mais necessitam de virtualização, e hoje as ferramentas postas à sua disposição são incontáveis.

Considerando isso, proposta do presente trabalho é a de realizar um estudo das tecnologias de reconhecimento facial a serviço da segurança pública do Estado da Bahia, que prometem o cumprimento de requisitos de eficiência, produtividade e celeridade, guardando relação com resultados quantitativos.

O tema desenvolve-se sob a lupa da implementação voluptuosa dessas ferramentas no mapa baiano, que vêm recebendo cada vez mais verba governamental, se propagando

como o maior investimento em segurança pública da história da Bahia, incluídos até mesmo em campanhas políticas e recebendo o apreço popular. Trata-se de uma implementação milionária de câmeras de segurança pelo território baiano, visando automatizar a função da polícia ostensiva de identificar criminosos, suspeitos, armas e placas de veículos, se tornando, segundo o atual governador do Estado, os novos olhos da segurança pública.

Contudo, o sistema, a contrassenso de toda a euforia na sua implementação, aponta diversos caminhos opostos aos trunfos de um ambiente social seguro, representando um verdadeiro risco à liberdade e à integridade da população de pele preta. Como já apontou Shalini Kantayya (2020), no documentário "*Coded Bias*", trata-se de uma ferramenta cujo sistema norteia-se por uma identificação facial que guarda identificação apenas com traços brancos e masculinos, desprezando faces femininas ou negras. Na falta de precisão na identificação de faces pretas, o produto final é a generalização: todo preto é culpado, suspeito, e perde naturalmente o direito à intimidade, chegando a ser verdadeiramente "perseguido" por câmeras de segurança públicas.

Essa imprecisão se deve ao formato de programação da Inteligência Artificial, responsável pelo reconhecimento facial, que perpassa por um processo de *machine learning*, em que há ação inicial humana para que a máquina seja alimentada com os dados a que deverá utilizar como base para "raciocinar", processo conhecido como *input* e *output* de dados. Esse pontapé inicial é que faz com que, posteriormente, identifiquemos correntes racistas na atuação das máquinas, pois essa alimentação, indispensável, carrega consigo vieses cognitivos, comuns à atividade decisional humana. Tratam-se de uma manifestação da nossa (i)racionalidade. São desvios cognitivos decorrentes de equívocos em simplificações de pensamento, que fazem com que, em momentos em que deveríamos realizar raciocínios deliberativos e onerosos, ocorra uma distorção cognitiva, que leva a resultados subótimos. É a partir daí que se identificam pronunciamentos maculados de subjetividade, preconceitos, preconcepções e impressões. No caso dos programas de reconhecimento facial, esses vieses recebem a denominação de *coded bias*, e revelam-se pelo desprezo de traços e características singulares de pretos e rostos femininos, em uma manifestação racista e sexista.

Assim, delineia-se uma metodologia exploratória, que tem como base a premissa de que a utilização do sistema de reconhecimento facial aplicado pela secretaria de segurança pública do estado da Bahia, embora em publicidade estariam ativas no intuito de proporcionar políticas de segurança no estado, intensificando uma maior vigilância sobre a sociedade, facilitando as atividades dos policiais e direcionando as abordagens, é nítido que o principal número de pessoas que são abordadas, são pessoas de peles pretas e de classes sociais baixas, ou oriundas de bairros pobres.

Justifica-se, então, um estudo que busca remontar como o estado, ao utilizar essas ferramentas, faz com que uma necropolítica seja ainda mais intensificada, uma vez que a definição desse termo é em como o Estado se utiliza de ferramentas a fim de controlar e punir de forma direta ou indireta pessoas de peles pretas, mesmo que seja sobre o pensamento de que tal ferramenta garanta mais agilidade, mas diretamente afeta e pune pessoas que são, em sua maioria, as mais frágeis no contexto social, em que a ferramenta utilizada, aponte diretamente os riscos da sua aplicação no território baiano e a utilização da mesma agrava ainda mais o racismo estrutural.

2 “OS NOVOS OLHOS DA SEGURANÇA PÚBLICA”

O Estado baiano, tem atingido no país números significativos de homicídios pelo quarto ano seguido, sendo esse um pódio infeliz, exposto no Atlas da Violência de 2020, produzido pelo Fórum Brasileiro de Segurança Pública sinalizando em que em 2018, 6.787 pessoas foram mortas por homicídio no Estado da Bahia (Cordeiro, 2020).

Apesar do tempo transcorrido, a Bahia, no ano de 2021, tornou a registrar uma quantidade significativa de mortes violentas, segundo dados do índice nacional de homicídios criado pelo g1, que utilizou dados dos 26 estados e do Distrito Federal, nesse ano, o estado contabilizou 5.099 mortes violentas (homicídios dolosos, latrocínios e lesões corporais seguidas de morte), deste número, 4.931 foram enquadradas como homicídio doloso, 122 como latrocínio e 46 como lesão corporal seguida de morte (Cordeiro, 2020). Portanto, não pode se deixar de pensar que é necessário que poder

público invista recursos e desprenda ações para se combater diretamente esses dados, minimizando os índices da frágil segurança pública baiana.

A possibilidade de transitar nos meios públicos e saber que existem câmeras capazes de reconhecer e registrar criminosos, armas, placas de carros e "atitudes suspeitas", demonstram que, o que pensávamos de uma sociedade tecnológica futura não está mais tão longe, com a prisão de mais de 200 suspeitos em Salvador só utilizando esses "robôs vigilantes" em pouco tempo, e estendendo a utilização desse recurso em mais 77 municípios, o governador do Estado da Bahia Rui Costa, no ano de 2021, autorizou a ampliação do investimento de R$ 665 (seiscentos e sessenta e cinco) milhões, totalizando até o momento o montante de quase R$ 900 (novecentos) milhões desprendidos dos cofres públicos do Estado, investindo-os em programas de reconhecimento facial, em uma solenidade no Centro de Operações e Inteligência (COI), parte da Secretaria de Segurança Pública (SSP), na capital baiana (Governo, 2021).

Após visitas feitas pelos representantes do Estado da Bahia a países da Europa e à china, foi apresentado o programa de reconhecimento facial, e assim, foi buscada a implementação desse programa, no qual o governador afirma ser ter a melhor tecnologia do país nesta área, que disse assim em entrevista:

> Nós temos agora talvez a melhor tecnologia do país nesta área. Há cerca de três anos, implementamos um projeto piloto de reconhecimento facial na cidade de Salvador, fruto de visitas que fizemos à Europa e à China. Essa tecnologia serve para prevenir crimes, socorrer pessoas e para a funcionalidade da cidade. No projeto piloto tivemos absoluto êxito, inclusive durante os carnavais, com a prisão de mais de 200 pessoas e a elevação substantiva da atividade da Segurança Pública. (Governo, 2021).

Ainda em entrevista no Centro de Operações e Inteligência, o Governador da Bahia, informa que se tem 23 centros de comunicação instalado no território baiano e conectados, afirma ainda que: "O planejamento é que todas as cidades que fazem parte do projeto tenham acesso a essa inteligência artificial, a esse recurso tecnológico. O que muda é que, antes, a identificação era feita pelo policial, visualmente. Agora, o próprio sistema identifica criminosos, suspeitos, armas e placas de veículos" (Governo, 2021).

Além do apresentado, sinaliza que apenas 5% dos crimes são julgados e tem a suas condenações decretadas pelos tribunais baianos, e afirma ainda que a impunidade acaba por estimular a prática criminosa, e que com o investimento, tem a possibilidade de prevenir crimes e assim possibilitar a prisão dos suspeitos, além de dar ao sistema judiciário provas suficientes para a comprovação dos delitos cometidos. (Governo, 2021).

A implantação das câmeras está localizada em postes, viaturas e até mesmo nas mãos dos policiais, o modo como funciona essa tecnologia na Bahia, que é prevista quatro pontos de imagens, sendo eles a câmeras de reconhecimento facial de fluxo aberto, a de fluxo controlado e tem câmeras de analise situacional e de leituras de placas, já os dispositivos alocados nas mãos dos policiais possuem a capacidade de fazer a captura do rosto do indivíduo, que é levado a central e assim faz o reconhecimento facial por meio do sistema, tendo o policial em mãos os equipamentos para reconhecer em tempo real a pessoa que ele abordar. (Governo, 2021).

Rui Costa, ainda em entrevista, sinalizou que levou em consideração o tamanho dos municípios, pois, quanto maior o município, maior a incidência de ocorrências de homicídios, já que são os mesmo que apresentam maiores índices, os municípios que receberam essa tecnologia ainda em 2021 foram salvador, Camaçari, Lauro de Freitas, Simões Filho, Candeias, Dias D´Ávila, Mata de São João, São Sebastião do Passé, Vera Cruz, São Francisco do Conde, Pojuca, Itaparica, Madre de Deus, Feira de Santana, Alagoinhas, Santo Antônio de Jesus, Vitória da Conquista, Jequié, Guanambi, Brumado, Juazeiro, Paulo Afonso, Jacobina, Senhor do Bonfim, Irecê, Itaberaba, Itabuna, Ilhéus, Teixeira de Freitas, Porto Seguro, Eunápolis, Valença, Itamaraju, Barreiras, Luís Eduardo Magalhães, Bom Jesus da Lapa, Santa Maria da Vitória, Ibotirama e Seabra totalizando 39 municípios e no ano de 2022 a implantação desse sistema em mais 39 municípios baianos (Governo, 2021).

2.1 A (in)eficiência do programa desde o projeto piloto

Por mais que se tenha a implantação oficial das Inteligências Artificiais somente recentemente, junto com a ampliação de investimentos sob essa nova ferramenta, foi

realizado um teste anterior para verificar a ação dessa IA, no que foi denominado de projeto piloto, estando em operação desde dezembro de 2018, e já no carnaval do ano seguinte, teve a sua implantação e resultados apresentados, como no caso em que Marcos Vinicius de Jesus Neri, com a fantasia do bloco As Muquiranas, foi identificado e preso pela polícia, quando entrava no circuito Dodô (Barra-Ondina), um dos locais ao qual ocorria a apresentação das principais atrações do carnaval baiano (Alves, 2019).

O suspeito teria sido denunciado à justiça pelo Ministério Público da Bahia (MP-BA), no mês de junho de 2018, após 7 (sete) meses do crime cometido na cidade de Lauro de Freitas, de acordo a investigação, Marcos Vinicius Passeava a pé no dia 6 de dezembro de 2017, quando a vítima, Sandro Barreto de Souza, passou de moto em alta velocidade perto dele e assim se irritando, o qual se armou e foi atrás da vítima em veículo automotor, ao alcançar a vítima, o indivíduo fez vários disparos pelas costas e após o ato, evadiu-se do local (Alves, 2019).

No carnaval de 2019 após ser identificado e abordado pelos policiais no carnaval, Marcos estava com mandado de prisão expedido e em aberto desde julho de 2018, após a denúncia do MP a Justiça, e foi a primeira pessoa a ser presa por essa tecnologia de reconhecimento facial, implantada pela SSP no carnaval de Salvador em 2019, e que a mesma teria sido utilizada no Festival da Virada daquele ano, com intuito de impedir a entrada de objetos que oferecerem risco à vida de baianos e turistas. O reconhecimento é feito por meio de comparação das imagens das pessoas que tiveram acesso aos circuitos e comparado com os bancos de dados da Secretaria de Segurança pública (SSP) tendo o investimento naquele período de mais de R$ 18 milhões de reais em softwares de reconhecimento, e o governo sinaliza que além dessa função, serve como sistema de ajuda a localizar pessoas desaparecidas (Alves, 2019).

Além da instalação dessas câmeras e da implantação da ferramenta, o governo do estado estendeu também o monitoramento em vários pontos da cidade, sendo eles o Pelourinho, que por meio do procedimento, sendo constatado mais de 90% de similaridade, o indivíduo é abordado e direcionado a delegacia (Alves, 2021). Ainda no sentido para a implantação das câmeras de monitoramento, o Governo anuncia também a

implantação em ônibus na Bahia, com intuito assim de reforçar o combate a assaltos, segundo o Governador do Estado Rui Costa (Redação, 2021).

A partir disso, se sucederam várias prisões por meio de identificação da face por meio do reconhecimento facial, e em novembro de 2021 chegou a marca de 221 pessoas identificadas e presas no Estado da Bahia por meio da utilização da tecnologia, todos com mandados de prisão expedidos, e que em muitos casos tem o seu mandado expedido a partir de 2018, e a tecnologia foi utilizada em outros foragidos que cometeram crimes por diferentes modalidades delituosas, onde a análise do programa chegando em torno de 95% de similaridade da feição, a polícia é acionada e então ocorre a abordagem e assim a verificação (Redação, 2021).

No dia 08 de janeiro de 2022, a Secretária de Segurança Pública identificou e informou para a polícia, onde mais um foragido da justiça estava localizado na cidade de Salvador e apontou que o suspeito teve 94 % de similaridade com o foragido e, portanto, a 9º Companhia Independe de Polícia Militar (CIPM/Pirajá), se deslocou, abordou o homem e o levou até a Polinter para apresentação e verificação de documentos, sendo constatado que se tratava de um homem que possuía mandado expedido em Castro Alves por sequestro, a SSP informou então que a utilização do sistema já permitiu a prisão de 227 pessoas no território baiano, desde do momento da sua implantação (Redação, 2022).

Nesse sentido ainda, se tem um apoio da mídia – especialmente a dedicada a matérias sensacionalistas - sobre como tem ocorrido essas abordagens e levando em consideração apenas os casos positivos. No entanto, tem muito a se observar sobre como está o caminho para a utilização do reconhecimento facial na capital baiana, o prefeito de Salvador Bruno Reis (DEM) destacou que o reconhecimento facial é o principal investimento na tecnologia para auxiliar as forças de segurança na cidade e que está sendo também implementado em todo o território brasileiro (Redação, 2021).

Embora, a Câmara Municipal do Rio de Janeiro tenha protocolado um projeto de lei, com intuito de proibir o uso dessas tecnologias pelo poder executivo municipal, no projeto proposto pelo Vereador Reimont (PT), diz-se que o reconhecimento facial é o "processamento automatizado ou semiautomotizado de imagens que contenham faces de indivíduos, com o objetivo de identificar, verificar ou categorizar esses indivíduos", tendo

a legislação baseada na Lei Geral de Proteção de Dados Pessoais, e notável que a tecnologia tem avançado cada dia mais no país sem um devida regulação ou procedimentos operacionais adequados concernentes as instituições que a utilizam (Redação, 2021).

Os números apresentados, de certo modo, são significativos, levando até então criminosos com mandados de prisão expedidos para que cumpram as suas penas, mas algo que não é mostrado pela mídia, pelo governo do estado e muito menos pela Secretária de Segurança Pública do Estado, são os erros, equívocos, e mesmo os riscos que a utilização de reconhecimento facial tem apresentado na sociedade baiana, existindo ainda questões que determinam em como essa ferramenta tem sido utilizada, e que surgiram muitas falhas de aplicação do sistema, não apenas em território baiano, mas também em outros Estados e até mesmo em outras nações.

A exemplo, no Estado do Ceará, ocorreu a chacina da Sapiranga, a qual deixou cinco mortos em Fortaleza, a Secretária de Segurança Pública do Estado do Ceará, tinha na sua lista de procurados pela polícia e em seu banco de dados cadastrado a foto do Ator americano Michael B.Jordan, astro dos filmes “Creed: Nascido para Lutar”(2015) e “Pantera Negra”(2018), a foto do astro do cinema americano é uma das três imagens presentes no Termo de reconhecimento Fotográfico da Polícia Civil do Ceará, e teve como resultado a apreensão de um adolescente de 17 anos como suspeito, por envolvimento na chacina (Redação, 2022).

O sistema de reconhecimento facial, também implantado em outros Estados, tem se mostrado falho, outros casos apontados foi o de uma mulher que foi detida por engano em Copacabana na Zona Sul do Rio de Janeiro, a polícia acreditava estar prendendo uma foragida da polícia, acusada de cometer os crimes de homicídio e ocultação de cadáver, após o sistema detectar, foi informado aos PMs que abordaram a mulher que se encontrava sem documentos no momento e assim foi levada para a 12º DP, mas ao chegar na delegacia, a mulher detida por engano teve sua identidade checada e assim os agentes confirmaram que não era a mesma pessoa que tinha o mandado de prisão expedido (G1 Rio, 2019).

A ferramenta de reconhecimento de suspeitos por meio de imagens coletadas é largamente usada pela polícia brasileira, e por se ter a ampliação dessa tecnologia nas cidades e o uso pelas corporações, é preciso que a informação seja divulgada de forma coerente sobre a sua utilização. Pois existem falhas graves, e são de uma precisão tão generalista que contribuírem para o perpetuamento do racismo. Essas tecnologias não causam de fato sequer essa tal eficiência no reconhecimento das pessoas, pois ainda se fazem necessárias outras etapas para constatar realmente que o suspeito abordado é o mesmo que cometeu o crime e precisa responder a justiça (Caixeta, 2022).

E não é de se pensar que esses casos estão restritos apenas no Brasil, um caso que ocorreu nos Estados Unidos, foi o de Nijeer Parks, um homem preto de 31 anos e que mora em Paterson, em New Jersey, recebeu um telefonema de sua avó, informando que a polícia de Woodbridge, uma cidade a 50 quilômetros da onde residia, teriam ido procurá-lo no apartamento em que eles dividiam, Parks já teve problemas com a lei anteriormente, mas desde que cumpriu sua pena na prisão por delitos de droga, se fixou em seu emprego como carpinteiro e levou a vida tranquilamente, mas quando se apresentou a delegacia para prestar depoimento, enquanto prestava esclarecimentos ao secretário, dois policiais se aproximaram e mandaram ele colocar as mãos atrás das costas e deram voz de prisão a ele (SARLIN, 2021).

Após tal evento, Parks ficou 11 (onze) dias na prisão sem ao menos saber o motivo de ter sido preso, e segundo o boletim de ocorrência obtido pela CNN, as provas que foram apresentadas pelos policiais que prenderam Parks foi a de que eram “compatíveis” com a foto que estava no sistema de reconhecimento facial, e por meio dessa compatibilidade, os promotores e um juiz assinaram sua prisão, Nijeer que levou mais de 1 ano para comprovar que era inocente, provando que no dia do crime cometido, ele se encontrava a mais de 50 quilômetros do local do crime, e isso só foi comprovado por conta de que no mesmo dia teria feito um deposito a sua noiva e o mesmo tirou foto do número de rastreamento do recibo o que serviu álibi (Sarlin, 2021).

3 A NECROPOLÍTICA COMO PROJETO PRINCIPAL: VIGILÂNCIA E CONTROLE DOS CORPOS PRETOS E POBRES

Potencializando a utilização desses métodos e inserindo ainda mais todos esses aparatos tecnológicos, faz surgir a transformação de um novo modelo de controle social, e consequentemente faz se alterar o modo como a sociedade se comporta, dando um ar de extrema vigilância da sociedade, e a inserção dessas tecnologias de vídeo monitoramento possibilitam, de fato, a garantia de alguns direitos, mas em contrapartida agrava e retira outros direitos da sociedade, portanto tem uma transformação do campo social e infere diretamente na tomada de decisões e sobre a busca por resultados (Rosa, 2019).

Apesar da evolução e do melhoramento constante das ferramentas de reconhecimento facial e dos resultados apresentados, é demonstrado que o sistema é falho e suscetível a erros, além claro do fator humano, que em muitos dos casos vem seus pré-conceitos estabelecidos e seguindo apenas um viés, e que em muitos casos, no lugar de trazer uma certa segurança para a sociedade, acaba por instaurar momentos traumáticos a vítimas que são acometidas por esses erros tecnológicos, além da perpetuação de maquinários de injustiças sociais historicamente sedimentadas, como o racismo, o preconceito de gênero, de classe, e outros.

A partir do que já foi apresentado, se tem ainda a necessidade de um olhar de que o Estado da Bahia é um dos estados mais violentos do Brasil, e o número de homicídios chega em 2018 a 6.787 pessoas mortas, sendo que desse número 90% das pessoas eram jovens negros, e esses impactos refletem de certo modo em como o estado tem atuado e combatido esses homicídios, e que se tem a guerra contra as drogas, e devendo assim o estado buscar meios para combater esses números e assim reduzir tais índices, mas que, no entanto, não é feito, e sim apenas instituindo formas e mais formas de encarceramento, fechando os seus olhos para o principal problema e apenas apresentando números e instituindo-os como resultados favoráveis para o combate à violência (CORDEIRO, 2020).

Além desses pontos levantados, se tem que o índice de pessoas mortas pela polícia, cresceu 47% entre os anos de 2019 e 2020, foram 773 pessoas mortas pela polícia em 2019, sendo o segundo estado que mais mata no Brasil, ficando atrás apenas do Rio de Janeiro, assim como o nº de policiais mortos cresceu 38% entre 2019 e 2020, foi de 8 agentes mortos em 2019 contra 11 agentes no ano de 2020 e assim a Bahia acaba por ocupar o sexto lugar em números absolutos de policiais mortos, e fica atrás dos estado de São Paulo, Rio de Janeiro, Pernambuco, Pará e Minas Gerias (Redação, 2021).

Além desses dados a Bahia é o estado mais letal do Nordeste, sendo que em 100% dos mortos pela polícia em Salvador são negros, em pesquisa feita pela "Pele Alvo: A cor da violência policial" da rede de Observatórios de segurança, afirma que todas as pessoas mortas pelas forças policiais no ano de 2020 eram pretas, tendo um aumento de 21,08% de mortes em ações policiais se comparado aos índices de 2019, no qual totalizou o número de 787 pessoas mortas pelas mãos do estado, sendo desse total 606 tiveram a identificação de raça, na qual 98% delas negras, ou seja 515 pessoas pardas e 80 pessoas pretas, e as outras 11 pessoas sendo brancas (Redação, 2021).

O desprendimento do governo baiano em fazer investimento na área de segurança pública para a implementação de aparatos tecnológicos de vigilância por meio do reconhecimento facial, mostra indiscutivelmente inserção e uma possibilidade do agravamento de uma necropolítica no estado, uma vez que, em definição simples, é o condão de determinar padrões em que a submissão da vida pela morte está validada, assim a necropolítica não é a apenas pela capacidade de instrumentalizar a vida, mas a de possibilita a destruição dos corpos e, em muitos casos, corpos de pessoas pretas, ou seja, não apenas deixar a pessoa morrer, a necropolítica implementa meio de fazer as pessoas morrerem (Mbembe, 2018).

Atualmente, os Estados, adotam em suas estruturas internas a força a utilização das forças em alguns momentos, sob uma perspectiva de uma política de segurança pública, o que traz de preocupação é que alguns desses discursos, vem como um reforço para estereotipar, segregar e também a de possibilitar o extermínio de alguns grupos alvos. Sobre esse pensamento e a sua caracterização se tem que:

> No pensamento filosófico moderno assim como na prática e no imaginário político europeu, a colônia representa o lugar em que a soberania consiste fundamentalmente no exercício de um poder à margem da lei (*ab legibus solutus*) e no qual a "paz" tende a assumir o rosto de uma "guerra sem fim". (Mbembe, 2018, p. 32 – 33)

Transmutando esse pensamento para a aplicação direta no estado brasileiro e ainda mais no contexto baiano, pode se interpretar que o Estado representa esse lugar de poder, e se fundamenta em leis e regramentos para a aplicação direta do seu domínio, instituindo assim uma guerra contra o crime e criminosos, se aproveitando de meios para possibilitar uma "paz" a sociedade, seja eles por meio da força policial e/ou de reconhecimento facial como ferramentas do biopoder do Estado, buscando estabelecer ordem, se faz de técnicas necessárias para justificar e até mesmo afirmar as decisões tomadas, Mbembe (2018) ainda diz que, " as colônias são o local por excelência em que os controles e as garantias de ordem judicial podem ser suspenso – a zona em que a violência do estado de exceção supostamente opera a serviço da "civilização", aplicando assim um regime no qual possibilite a aplicação de uma "justiça" punitiva.

4 RUIDOS DA NECROPOLÍTICA: ENVIESAMENTO ALGORÍTMICO

A utilização de ferramentas tecnológicas para possibilitar a dinamização das ações cotidianas, com intuito direto de simplesmente possibilitar a eficácia do serviço demandado, emerge na necessidade de constituir programas necessários para possibilitar tal objetivo, O'Neil (2020), aborda em sua obra, em como as tecnologias estão presentes na sociedade, trazendo vários pontos que, a *big data* desenvolve e aumenta a desigualdade na sociedade, gerando um impacto direto em uma sociedade democrática.

Os métodos, que em muitos casos são instituídos na sociedade para um tipo de controle ou mesmo aperfeiçoamento da sociedade encaminhando para o resultado do bem-estar social, assim abre a possibilidade de agravar ainda mais situações ainda presentes no meio social, se observando as desigualdades e a busca por um controle social eficaz, a sociedade é composta por diversos elementos que possibilitam a sua diversidade e pluralidade em vários âmbitos individuais das pessoas.

O'Neil (2020) discorre de forma clara e dinâmica em como a sociedade e os meios de coerção da sociedade quando inseridos em planos matemáticos e algorítmicos, dependendo da situação agrava ainda mais a desigualdade social, a exemplo, nos Estados Unidos, em 2013, buscando um método possível para a diminuição dos índices de violência e consequentemente a possibilidade de um apoio policial, então, investiu-se em 2013 em um *software* de previsão de crimes, tal programa, possibilitava o processamento de dados de históricos criminais e calculou, onde a cada hora era mais possível que crimes acontecessem, tal programa possibilitou assim que fosse desprendido força policial a um determinado quadrante para fazer rondas e alocar policiais para que tivesse a otimização de recursos, além de que a própria polícia é quem fazia a configuração no sistema, catalogando assim os crimes que iam ocorrendo, categorizando por níveis e quais os tipos de crimes cometidos, além de horários e lugares das ocorrências.

Assim, acaba por então criar um ciclo nocivo de *feedback*, onde a polícia cria as informações e consequentemente é direcionado a um mesmo local, e que em muitos casos são nos mesmo bairros empobrecidos e que em grande parte constituído por pessoas negras e hispânicas, e por mais que o sistema não diferencie a cor da pele, o próprio resultado faz, sob um olhar do indivíduo que inseriu os dados, e que ao final o que acaba por caracterizar é a pobreza e leva a acreditarmos que as ferramentas não são apenas cientificas, mas também justas (O'Neil, 2020).

Então ainda sobre a questão de categorizar, foi levantado a questão do departamento do polícia da cidade de Nova Iorque, que se utilizava do método que é chamado "parar, questionar e revistar", mas realmente conhecido apenas como o simples para-e-revistar, tal procedimento feito pela polícia buscava-se um esquema de filtragem de crimes, mas era de conhecimento de todos que a parte que mais passava por esse procedimento da polícia era homens, jovens de pele escura, e que cerca de 85% envolvia assim jovens afro-americanos ou latinos e assim os homens negros possuíam seis vezes mais de possibilidade de serem abordados por policiais e serem revistados, e por mais que esse método seja um Arma de Destruição em Massa (ADM), a mesma é dependente de julgamento humano e não se tem a formalização em um algoritmo (O'Neil, 2020).

Mas que se analisar esse método, o para-e-revistar é semelhante a ADMs, o mesmo possuía um ciclo vicioso, uma vez que se pegava milhares de homens negros e latinos, e muitos por terem cometidos crimes de pequenos delitos, e assim a busca da polícia por aquelas pessoas que poderiam já ter cometido algum crime, mas também aquelas que poderiam vim a cometer algum futuramente e levando assim a um ciclo ao qual vai se agravando com o tempo, a possibilidade assim de um melhoramento, seria o de inclusão de um sistema de reconhecimento facial (O'Neil, 2020).

Importante levar em consideração, é que a utilização da tecnologia de reconhecimento facial no Estado da Bahia, levanta um debate sobre a sua aplicabilidade, onde destaca que a utilização, sobre um discurso da segurança pública não se sustenta. Pois o que se busca com essas ferramentas é eficiência do sistema de punir, e não a sua efetividade em combater o crime ou mesmo trazer a real segurança pública, o debate da utilização da ferramenta como um agravante para a possibilidade de uma necropolitica se faz presente, o que leva a pensar que o sistema de reconhecimento facial por fim acaba por não se sustenta, uma vez que a constituição de informações do sistema, é enviesada e ruidosa, destacando assim o pré-conceito contra pessoas pretas na sociedade baiana, estado com o maior número de pessoas pretas do Brasil.

Tais analises e conhecimentos, levanta o debate que é tratado por Daniel Kahneman, Oliver Sibony e Cass R. Sunstein, abordam em como o ruído afeta as decisões humanas, que é constatado que o ruído é encontrado em todos os pontos em que leva a pessoa a tomar decisões, e quem em muitos dos casos está ligada a particularidades de cada caso, levando em consideração o grupo que está presente e até a ocasião, o ruído é presente em todos os âmbitos da sociedade, e portanto é caracterizado com uma variação dos julgamentos, que em muitos casos deveriam ser idênticos (Kahneman; Sibony; Sunstein, 2021).

Portanto, aplicando a utilização da ferramenta de reconhecimento facial, é possível apontar os vieses racista instituídos por meio da sociedade, levando em consideração um sistema ruidoso no qual muitas das vezes é ocasionado individualmente, mas no contexto do reconhecimento facial, o ruído é presente por parte individual do

sujeito que aplica e assim como um grupo que acaba por amplificar o ruído (Kahneman; Sibony; Sunstein, 2021).

Assim, compreender como o ruído surge nas decisões e nos sistemas da sociedade e consequentemente saber onde ele se aloca, traz a possibilidade de buscar um meio possível para combater ou mesmo balizar os vieses e os ruídos para que de certo modo possibilitar o equilíbrio e então permitir uma análise diferente dos casos e consagrar a possibilidade de levar a um caminho democrático e igualitário da sociedade (Kahneman; Sibony; Sunstein, 2021).

Portanto, a presença do ruído em pessoas que criam e aplicam a Inteligência Artificial, o reconhecimento facial podem ser um agravante para a política de segurança pública da Bahia, mas o ponto principal é entender as agravantes dessa política e o modo correto de aplicar, fazendo assim surge decisões e caminhos possivelmente corretos, trabalhando sempre o contexto necessário para uma devida aplicação do direito e os seus caminhos para a possibilidade de concessão de um bem-social da sociedade, combatendo as suas desigualdades quanto a concessão de tratamento igualitário.

5 CONSIDERAÇÕES FINAIS

Preocupa em um regime Democrático de Direito, a subsistência de mecanismos de reconhecimento facial notadamente racistas, em especial inseridas em um Estado conhecido por ser o centro da cultura afro brasileira, o que denota o ápice e o intento de perpetuação de uma cultura marginalizadora da pele preta. Existe um caminho alternativo, que é a destinação desta verba milionária a estudos que busquem o *debiasing* (desenviesamento) desse mecanismo, para somente depois, com parcimônia, se dedicar à implementação destes em larga escala.

Não se justifica a falta de reparo destes mecanismos em um Estado que possui uma maior porcentagem de pardos na composição étnico-racial, em que 1 em cada 5 pessoas se declara preta. É dito isso que fica claro que os “novos olhos da segurança pública” se mantêm, infelizmente, presos a antigos preceitos de branquitude, míope para a realidade social do próprio Estado a que se propõe resolver questões de segurança

pública. Parece que, na falta de uma legislação federal que ordene a utilização de dispositivos de reconhecimento facial, a ordem do dia na segurança pública segue sendo a violência institucional destinada a pessoas pretas.

Então, a utilização de ferramentas tecnológicas no contexto baiano, intensifica ainda mais a repressão que é empregada pelas forças policiais, assim como os números de casos e pessoas que são abordadas cresce ainda mais no banco de dados da secretária do estado, demonstrando a disparidade e deixando ainda mais intrínseco a desigualdade racial na sociedade baiana, possibilitando uma divisão de pensamentos sobre (in)eficiência do estado garantir a segurança pública adequada a todos, sempre visando observar então os direitos fundamentais dos indivíduos e a possibilidade de um Estado democrático de Direito, além de demonstram em como os impactos da globalização e o neoliberalismo causam sobre essa temática, e então se vê apenas que o Estado, se utiliza dessas ferramentas e agrava ainda mais as relações entre essas demandas.

REFERÊNCIAS

ALVES, Alan Tiago. **Flagrado por câmera vestido de mulher no carnaval na BA amtou homem após vítima passar perto dele de moto em alta velocidade**. [*S. l.*], 7 mar. 2019. Disponível em: https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/07/flagrado-por-camera-vestido-de-mulher-no-carnaval-na-ba-matou-homem-apos-vitima-passar-perto-dele-de-moto-em-alta-velocidade.ghtml. Acesso em: 18 maio 2022.

ALVES, Sarah. **Pelourinho vai ganhar câmeras de reconhecimento facial**: isso é bom ou ruim?. [*S. l.*], 1 mar. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/03/01/pelourinho-vai-ganhar-cameras-de-reconhecimento-facial-isso-e-bom-ou-ruim.htm Acesso em: 10 maio 2022.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Inteligência artificial no Poder Judiciário brasileiro. Brasília: CNJ, 2019. 40 f.

BRASIL, Conselho Nacional de Justiça. **Justiça em números 2021**. Brasilia: Poder Judiciário, 2021. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/09/relatorio-justica-em-numeros2021-12.pdf. Acesso em: 17 maio 2022.

BRASIL. **Constituição** (**1988**). **Constituição** da República Federativa do Brasil. Brasília, DF: Senado **Federal**: Centro Gráfico, **1988**.

BRANDÃO, Graziela; GLASMEYER, Rodrigo. **Inteligência Artificial no judiciário brasileiro**. Time BL Consultoria: Time BL Consultoria Digital - Direito Digital e Análise Regulatória, 2020. Disponível em: https://blconsultoriadigital.com.br/inteligencia-artificial-no-judiciario-brasileiro/#:~:text=quais%20s%C3%A3o%20repetidas.,Intelig%C3%AAncia%20Artificial%20no%20judici%C3%A1rio%3A%20RADAR,de%20Demandas%20Repetitivas%20(IRDR). Acesso em: 23 maio 2022.

CAIXETA, Izabella. **Foto de Michael B. Jordan aparece entre suspeitos de chacina**: Especialista aponta como o sistema de reconhecimento fotográfico contribui para o racismo no Brasil. Minas Gerais, 7 jan. 2022. Disponível em: https://www.correiobraziliense.com.br/mundo/2022/01/4975929-foto-de-michael-b-jordan-aparece-entre-suspeitos-de-chacina.html. Acesso em: 12 maio 2022.

CORDEIRO, Hilza. **Bahia é estado com maior nº de homicídios do país pelo quarto ano consecutivo.** [*S. l.*], 27 ago. 2020. Disponível em: https://www.correio24horas.com.br/noticia/nid/bahia-e-estado-com-maior-no-de-homicidios-no-pais-pelo-quarto-ano-consecutivo/. Acesso em: 20 maio 2022.

DINIZ, Bruno Souza *et al*. RADAR: Uma contribuição da tecnologia da informação para a gestão de processos repetitivos no Tribunal de Justiça de Minas Gerais. **Revista de Precedentes Qualificados**: Tribunal de Justiça do Estado de Minas Gerais, Belo Horizonte, v. 02, n. 02, p. 585 - 605, 2020.

ESPINDOLA, Angela Araújo da Silveira; SANGOI, Bernardo Girardi. **A crise da jurisdição e a funcionalização do direito pela economia:** a justiça e os números. Revista de Direito Brasileira, São Paulo, v. 18, ed. 7, p. 214 - 229, Set/dez 2017.

FEDERAL, Supremo Tribunal. Inteligência artificial vai agilizar a tramitação de processos no STF. *In*: FEDERAL, Supremo Tribunal. Inteligência artificial vai agilizar a tramitação de processos no STF. Jusbrasil, 6 mar. 2018. Disponível em: https://stf.jusbrasil.com.br/noticias/584499448/inteligencia-artificial-vai-agilizar-a-tramitacao-de-processos-no-stf. Acesso em: 7 abr. 2022.

FERNANDES, Bernardo Gonçalves; PEDRON, Flávio Quinaud. **O Poder Judiciário E(m) Crise**: Reflexões de teoria da constituição e teoria geral do processo sobre o Acesso à justiça e as recentes reformas do Poder Judiciário à luz de: Ronald Dworkin, Klaus Gunther e Jurgen Habermas. Rio de Janeiro: Lumem Juris, 2007. 315 p.

G1 RIO, Redação. **Sistema de reconhecimento facial da PMA do RJ falha, e mulher é detida por engano**. [*S. l.*], 11 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 12 maio 2022.

GOVERNO baiano investe R$ 665 milhões e amplia o serviço de reconhecimento facial e de placas. [*S. l.*], 27 jul. 2021. Disponível em: https://badevalor.com.br/governo-baiano-investe-r665-milhoes-e-amplia-o-servico-de-reconhecimento-facial-e-de-placas/ Acesso em: 11 maio 2022.

KAHNEMAN, Daniel; SIBONY, Olivier; SUNSTEIN, Cass R. **Ruido**: Uma falha no julgamento Humano. 1. ed. Rio de Janeiro: Schwarcz S.A, 2021. 426 p.

MBEMBE, Achille. **Necropolítica**: biopoder, soberania, estado de exceção, política da morte. 1. ed. São Paulo: [*s. n.*], 2018. 71 p.

O'NEIL, Cathy. **Algoritmos de destruição em massa**: como o big data aumenta a desigualdade e ameaça a democracia. Santo André, SP: Rua do Sabão, 2020. 339 p.

PRUDENCIO, Marcos. **A tecnologia do dia-a-dia**. [S. l.], 13 mar. 2018. Disponível em: https://www.correiobraziliense.com.br/app/noticia/tecnologia/2018/03/13/interna_tecnologia,665761/a-tecnologia-do-dia-a-dia.shtml. Acesso em: 22 mar. 2022.

RAUTENBERG, Sandro; CARMO, Paulo Ricardo Viviurka do. **Big data e Ciência de Dados:** complementariedade conceitual no processo de tomada de decisão. Brazilian Journal of Information Studies: Research Trends, [*s. l.*], v. 13, ed. 1, p. 56-67, 2019

REDAÇÃO, A tarde. **Investigado por Roubo é o 221º preso com o reconhecimento facial na Bahia**. Salvador, 1 nov. 2021. Disponível em: https://atarde.com.br/bahia/investigado-por-roubo-e-o-221-preso-com-reconhecimento-facial-na-bahia-1177556. Acesso em: 16 maio 2022.

REDAÇÃO, A Tarde. **Governo anuncia sistema de monitoramento por câmeras em ônibus da Bahia**. [*S. l.*], 18 maio 2021. Disponível em: https://atarde.com.br/bahia/governo-anuncia-sistema-de-monitoramento-por-cameras-em-onibus-na-bahia-1157337?wn=&r1=. Acesso em: 10 maio 2022.

REDAÇÃO, Correio. **Reconhecimento Facial**: Foragido por sequestro é preso em Salvador. Salvador, 8 jan. 2022. Disponível em: https://www.correio24horas.com.br/noticia/nid/reconhecimento-facial-foragido-porsequestro-e-preso-em-salvador/. Acesso em: 16 maio 2022.

REDAÇÃO, G1 BA. **Bahia é o estado mais letal do Nordeste e 100% dos mortos pela polícia em Salvador são negros.** [*S. l.*], 14 dez. 2021. Disponível em: https://g1.globo.com/ba/bahia/noticia/2021/12/14/bahia-e-o-estado-mais-letal-do-nordeste-e-100percent-dos-mortos-pela-policia-em-salvados-sao-negros-aponta-pesquisa.ghtml. Acesso em: 16 maio 2022.

REDAÇÃO, G1 BA. **Índice de pessoas mortas pela polícia na Bahia cresce 47% entre 2019 e 2020: nº de policiais mortos também subiu**. [*S. l.*], 22 abr. 2021. Disponível em: https://g1.globo.com/ba/bahia/noticia/2021/04/22/indice-de-pessoas-mortas-pela-policia-na-bahia-cresce-entre-2019-e-2020-no-de-policiais-mortos-tambem-subiu.ghtml. Acesso em: 16 maio 2022.

REDAÇÃO, G1 CE. **Foto de astro do cinema Michael B. Jordan aparece em lista de procurados pela polícia do Ceará**. [*S. l.*], 7 jan. 2022. Disponível em: https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml. Acesso em: 13 maio 2022.

ROSA, Alexandre Morais da; JUNIOR, Julio Cesar Marcellino. **O Estado democrático de direito e os direitos fundamentais sociais:(in)efetividade em tempos de prevalência da lógica econômica.** Unisul fato e de direito, Santa Catarina, v. 1, ed. 2, p. 47-55, 2011.

ROSA, Alexandre Morais da. **A questão digital: o impacto da inteligência artificial no Direito.** Revista de Direito da Faculdade Guanambi, Guanambi, v. 6, ed. 02, p. 1 - 18, jul. / dez. 2019.

SARLIN, Jon. **EUA: Polícia prende inocente a partir de sistema de reconhecimento facial.** [*S. l.*]: CNN, 3 maio 2021. Disponível em: https://www.cnnbrasil.com.br/internacional/sistema-de-reconhecimento-facial-enviou-este-homem-inocente-para-a-prisao/. Acesso em: 9 maio 2022.

SILVA, Antônio Marcos Barreto *et al*. **Panorama socioeconômico da população negra da Bahia.** Textos para Discussão, Salvador, n. 17, p. 1 -17, 10 fev. 2020.

A RELAÇÃO ENTRE TRABALHADORES E EMPRESAS DE APLICATIVOS DE TRANSPORTE DE PESSOAS E DE ENTREGAS

THE RELATIONSHIP BETWEEN WORKERS AND PEOPLE TRANSPORTATION AND DELIVERY APPLICATION COMPANIES

Francisco Alex de Oliveira[1]

Gabriel Ap. Anizio Caldas[2]

Gabriela Sroczynski Fontes[3]

RESUMO

Este artigo visa fazer uma reflexão acerca da existência ou não do vínculo empregatício entre trabalhadores e empresas de aplicativo de transporte de pessoas e de entregas, partindo da premissa do que dispõem os artigos 2º e 3º da Consolidação das Leis do Trabalho (CLT), que tratam dos requisitos caracterizadores da relação de emprego, com ênfase na subordinação, o mais proeminente dos requisitos. Para isso, foi realizada uma pesquisa bibliográfica e documental, com abordagem qualitativa. E, à luz da CLT, doutrina e de julgados das turmas 3ª, 4ª e 5ª do Tribunal Superior do Trabalho (TST), este artigo analisou a relação em estudo. A 3ª turma do TST reconheceu o vínculo de emprego, mas a 4ª e 5ª turmas, não. Dessa forma, a divergência entre as turmas 3ª e 5ª ensejou um embargo na Subseção I Especializada em Dissídios Individuais (SDI-1), que começou a ser julgado, mas foi suspenso depois de um pedido de vista, com remessa ao Pleno do TST. Além disso, algumas propostas de leis que tratam do assunto estão aguardando prosseguimento nas casas do Congresso Nacional (CN). Assim, diante do impasse, a CLT continua sendo o diploma legal que traz os requisitos caracterizadores do vínculo empregatício, que ao serem procurados na relação ora abordada, não foram encontrados cumulativamente, o que impede que os trabalhadores por intermediação de aplicativos sejam classificados como empregados.

Palavras-chave: Empresas de Aplicativos; Requisitos de Relação de Trabalho; Subordinação; Relação de Trabalho.

[1] Graduado em Direito pela Universidade Federal do Acre – UFAC. Lattes: http://lattes.cnpq.br/8402272955943361.

[2] Doutorando em Estudos de Cultura Contemporânea pela UFMT. Mestre em Direito pelo Centro Universitário Eurípides de Marília. Lattes: http://lattes.cnpq.br/5573870438124939.

[3] Doutoranda e mestre em Estudos de Cultura Contemporânea pela UFMT. Docente na Faculdade Fasipe Cuiabá. Lattes: http://lattes.cnpq.br/3602221864670311.

ABSTRACT

This article aims to reflect on the existence or not of the employment relationship between workers and companies that use the transport of people and deliveries, starting from the premise of articles 2 and 3 of the Consolidation of Labor Laws (CLT), which deal with of the characterizing requirements of the employment relationship, with emphasis on subordination, the most prominent of the requirements. For this, a bibliographical and documentary research was carried out, with a qualitative approach. And, in the light of the CLT, doctrine and judgments of the 3rd, 4th and 5th classes of the Superior Labor Court (TST), this article analyzed the relationship under study. The 3rd TST group recognized the employment relationship, but the 4th and 5th groups did not. Thus, the divergence between the 3rd and 5th classes gave rise to an embargo in Subsection I Specialized in Individual Disputes (SDI-1), which began to be judged, but was suspended after a request for review, with referral to the Plenary of the TST. In addition, some law proposals dealing with the subject are awaiting continuation in the National Congress (CN) houses. Thus, in view of the impasse, the CLT continues to be the legal diploma that brings the characterizing requirements of the employment relationship, which, when sought in the relationship discussed herein, were not found cumulatively, which prevents workers through the intermediation of applications from being classified as employees.

Keywords: Application Companies; Work relationship; Employment Relationship Requirements; Subordination; Employment Relationship.

1 INTRODUÇÃO

O avanço tecnológico propiciou a 4ª Revolução Industrial, também denominada de Indústria 4.0, que é uma fusão de tecnologias digitais, como a inteligência artificial, *big data*, realidade virtual, internet das coisas, nanotecnologia, biologia sintética, *machine learning*, *cloud computing*, robótica e outras.

Os impactos que essa revolução pode trazer na produção industrial são muitos, como a redução dos custos, aumento da produtividade, elevação da qualidade, ganho de competitividade e, consequentemente, o aumento do lucro. No entanto, na economia e nas relações de trabalho, os impactos já são uma realidade.

A Indústria 4.0 possibilitou o surgimento da *Gig Economy*, que é o mercado de trabalho baseado em contratos de curta duração, sem vínculo empregatício, conhecidos também como "bicos", que já existem há muito tempo. E, a utilização de plataformas digitais para que eles sejam celebrados é uma inovação, visto que efetiva o encontro entre a pessoa que necessita do serviço e o prestador do serviço.

A partir da *Gig Economy* surgiu o *work on demand*, que em tradução livre significa "trabalho sob demanda", que é a modalidade de trabalho na qual serviços específicos são solicitados e oferecidos por usuários de aplicativos. Os que solicitam são consumidores, e os que oferecem, trabalhadores. Dois exemplos de trabalho sob demanda são o transporte de passageiros e o serviço de *delivery*.

Esses serviços já eram prestados por trabalhadores autônomos muito antes dos aplicativos existirem, mas a partir do momento em que essas plataformas digitais passaram a operar, e consequentemente aproximar os consumidores e os trabalhadores, surgiu um debate quanto à relação de trabalho entre estes e as empresas responsáveis pelos aplicativos.

O debate chegou no judiciário e os trabalhadores por intermediação de aplicativos foram reconhecidos como empregados em algumas decisões e em outras, não. Ou seja, as decisões emanadas da justiça trabalhista, inclusive de algumas turmas do Tribunal Superior do Trabalho (TST), recrudesceram o debate.

Os artigos 2º e 3º da CLT – Consolidação das Leis do Trabalho trazem os requisitos necessários para a caracterização do vínculo de emprego, mas a realidade proporcionada pela *Gig Economy*, que trouxe mudanças no mercado de trabalho, com o modelo de trabalho por intermédio de plataforma digital, fomenta o debate quanto ao tratamento jurídico que deve ser conferido a essas novas formas de trabalho.

Partindo da premissa do que dispõem os artigos 2º e 3º da CLT, que tratam dos requisitos caracterizadores do vínculo empregatício, com ênfase na subordinação, o mais proeminente dos requisitos, foi realizada uma pesquisa bibliográfica e documental. Dessa forma, a CLT, doutrina e as decisões das turmas do TST, que têm jurisdição em todo o território nacional, apesar do efeito delas ser apenas *interpartes*, foram analisadas.

A subordinação sem dúvida alguma é o requisito principal para se configurar a relação empregatícia, tanto que as decisões judiciais se debruçam para reconhecê-la ou retirá-la do contexto fático lastreado no teor probatório dos processos. Assim, todos os requisitos caracterizadores do vínculo de emprego serão abordados, mas a ênfase será a subordinação jurídica, que existe entre empregado e empregador como consequência do contrato de trabalho.

2 TRABALHO E EMPREGO

Quando se busca conceituar algo ou alguma coisa corre-se o risco de diminuir ou exagerar o que se pretende expor. E quando o objeto tem ampla discussão, a responsabilidade aumenta consideravelmente. Mas como o objetivo não é discorrer a respeito dos conceitos de trabalho e emprego de forma aprofundada e ampla, a abordagem será apenas para trazer ao leitor uma noção básica sobre eles para um melhor entendimento acerca do tema principal.

Segundo Romar (2018, p. 129) "A relação de emprego é uma espécie de relação de trabalho, que se baseia no nexo entre empregador e empregado, caracterizado pela prestação pessoal de serviços, de forma não eventual e subordinada, mediante o pagamento de salário". Assim, existem alguns requisitos específicos para que se caracterize uma relação empregatícia.

Já o trabalho é toda atividade humana, seja física ou intelectual, que produz bens econômicos ou não, e que também satisfaz uma das necessidades intrínsecas do homem, que é se sentir útil (MORIN, 2001). Nas palavras de Cassar (2019, p. 23), "Trabalho pressupõe ação, emissão de energia, despendimento de energia humana, física e mental, com o objetivo de atingir algum resultado". Ou seja, não há requisitos para que seja caracterizada uma relação de trabalho, bastando apenas que não seja uma relação de emprego.

Segundo a CLT (2022), no artigo 3º, "Considera-se empregado toda pessoa física que prestar serviços de natureza não eventual a empregador, sob a dependência deste e mediante salário". É importante afirmar que a CLT não conceitua emprego, mas empregado, por meio do conceito deste é possível também conceituar emprego. Ela traz o complemento que torna possível a diferenciação conceitual entre trabalho e emprego, pois sem ele fica bastante difícil diferenciá-los. Tal complemento são os requisitos que caracterizam a relação de emprego, pois quando aqueles estão presentes cumulativamente, está estabelecido o vínculo empregatício.

Segundo Leite (2020, p. 288) "A relação de trabalho, então, seria gênero, e a relação de emprego, espécie". Ou seja, assim sendo a relação de trabalho gênero da qual a relação de emprego é espécie, então, o empregado também é trabalhador, mas nem todo trabalhador é empregado. Isso acontece porque a CLT trouxe intencionalmente requisitos para que houvesse a diferenciação do vínculo de emprego com as demais relações de trabalho. Por isso, parafraseando, todo emprego é trabalho, mas nem todo trabalho é emprego.

Então, emprego é uma espécie de trabalho que se lastreia na relação jurídica entre empregado e empregador, caracterizado pela prestação pessoal de serviços, de forma contínua, com subordinação, mediante pagamento de salário. Os requisitos que caracterizam a relação de emprego, segundo Delgado (2019, p. 337) são 5 (cinco):

> [...] a) prestação de trabalho por pessoa física a um tomador qualquer; b) prestação efetuada com pessoalidade pelo trabalhador; c) também efetuada com não eventualidade; d) efetuada ainda sob subordinação ao tomador dos serviços; e) prestação de trabalho efetuada com onerosidade.

É importante ressaltar que para que aconteça o vínculo empregatício é necessário que todos os requisitos estejam presentes, caso contrário, se terá apenas uma relação de trabalho. E eles serão abordados na verificação da existência de vínculo empregatício entre motoristas e entregadores e as empresas de aplicativo.

Quando se usa a expressão "apenas uma relação de trabalho" não há uma intenção de diminuir a importância das outras relações de trabalho, mas apenas o intento de ressaltar a relação de emprego, que vez por outra é confundida com as demais prestações de trabalho.

Ou seja, a prestação de trabalho pode até parecer com relação de emprego, mas se faltar um dos requisitos não será vínculo empregatício. Portanto é possível que uma prestação de trabalho aparenta ser um vínculo empregatício, mas, quando isso acontecer, por meio da análise dos requisitos será possível perceber o engano.

3 INDÚSTRIA 4.0 E GIG ECONOMY

O avanço tecnológico propiciou a 4ª Revolução Industrial, também conhecida como Indústria 4.0. Esta é uma evolução baseada no acúmulo do conhecimento científico das anteriores (1.0, 2.0 e 3.0). Segundo Lisboa, (2021, p. 2 *apud* Feliciano; Pasqualeto, 2019):

> [...] a Indústria 4.0 trata-se de uma nova configuração econômica, social e cultural, que se forma em função do desenvolvimento, exponencial e contínuo, das tecnologias digitais, como da internet das coisas, da inteligência artificial, da robótica, da computação quântica, da nanotecnologia, e tantas outras. Diante disso, um dos nítidos efeitos da 4ª Revolução Industrial é a formação do macroambiente de negócios.

A 4ª Revolução está mudando as formas de produção industrial, o mundo dos negócios e as relações de trabalho como nunca na história da humanidade:

> A quarta revolução industrial rompe os paradigmas até então vivenciados, uma vez que as tecnologias digitais utilizadas são muito mais sofisticadas, além do fato de que as ondas de novas descobertas ocorrem numa velocidade avassaladora. Fundem-se, então, os mundos físicos, digitais e biológicos, imprimindo uma forma de trabalho [...]. (WYZYKOWSKI, 2020, p. 164).

A Indústria 4.0 possibilitou o surgimento da *Gig Economy*, que segundo o dicionário de *Cambridge*, é "o mercado de trabalho que compreende trabalhadores temporários e sem vínculo empregatício" (2022). Segundo Silva e Souza (2021, p. 12), "Com este breve conceito, já se depreende o cenário de relações mais fluidas, nas quais os trabalhadores buscam trabalhos por demanda, tendo uma remuneração por cada serviço isolado, afastando-se, por conseguinte, o vínculo empregatício".

A *Gig Economy* é a consolidação de várias tecnologias (Internet, Sistema de Posicionamento Global (GPS) e Smartphone), que possibilita a criação de plataformas digitais, como os aplicativos, e a celebração de contratos de trabalhos de curta duração, também conhecidos como "bicos". Dessa forma, esses contratos passaram a ser celebrados em escala industrial, seguindo os passos da Revolução 4.0, que tem sua base nas tecnologias digitais. (Silva; Souza, 2021).

Os “bicos” já fazem parte do mercado de trabalho há tempos e a utilização de plataformas digitais para que eles sejam celebrados é uma inovação, pois efetiva o encontro entre a pessoa que necessita do serviço e o prestador do serviço. Assim, a *Gig Economy* passou a possibilitar a celebração de contratos de curta duração por meio de plataformas digitais.

A *Gig Economy* tem duas formas de trabalho, o *crowdwork* e o *work on demand*. A primeira, em tradução livre significa “trabalho de multidão” e a segunda, “trabalho sob demanda”. Sobre o *crowdwork*, Rodrigues (2021, p. 200 - 201) expõe:

> [...] as plataformas on-line colocam em contato diversas organizações e indivíduos entre si, por meio da internet, permitindo a aproximação de consumidores e trabalhadores de todo o mundo. Conectam oferta e demanda de produtos e serviços específicos para o atendimento da necessidade de clientes, que pagam pela execução das tarefas realizadas, que normalmente são micro tarefas extremamente fragmentadas, que normalmente não precisam de qualificação e são monótonas, mas não podem ser realizadas por computadores ou sistemas automatizados.

As atividades do *crowdwork* são realizadas globalmente e por meios telemáticos, geralmente pela Internet. Já o *work on demand*, segundo Feliciano e Pasqualeto (2021, p. 60):

> É uma forma de trabalho na qual a execução de atividades tradicionais como transporte e limpeza, por exemplo, é canalizada por aplicativos gerenciados por empresas que também intervêm na definição de padrões mínimos de qualidade de serviço e na seleção e gestão da força de trabalho.

Dessa forma, o *work on demand* é mais local e suas atividades são executadas fisicamente. Portanto, os trabalhadores por intermediação de aplicativos se enquadram no *work on demand*, visto que executam fisicamente os serviços tradicionais solicitados pelas plataformas.

Portanto, com base em Rodrigues (2021), *Gig Economy* poderia ser compreendido como o mercado de trabalho formado por trabalhadores temporários, sem vínculo empregatício, que pactuam contratos de pequena duração (conhecidos como ‘bicos’),

intermediados por aplicativos, e são remunerados pelos serviços prestados aos consumidores.

4 MOTORISTAS E ENTREGADORES DAS EMPRESAS DE APLICATIVOS

Atualmente, o Brasil possui alto índice de desemprego, que segundo a última pesquisa do Instituto Brasileiro de Geografia e Estatística (IBGE), está em 8,7%, atingindo 9,5 milhões de pessoas (2022). A pesquisa mostrou também que mais 4,3 milhões são desalentados, pessoas que gostariam de trabalhar, mas que deixaram de procurar trabalho por entender que não encontrarão (2022).

Os motoristas que transportam pessoas e os entregadores de comida e de outros produtos estão incluídos nessa realidade de desemprego e desalento. E, na tentativa de suprirem suas necessidades, prestam serviços por intermediação de aplicativos.

> Em regra, o trabalho ocorre da seguinte maneira: (i) o usuário da plataforma acessa o aplicativo em busca de um serviço e o solicita; (ii) em algumas plataformas, é possível indicar determinadas características que o trabalhador deve ter para executar a atividade – como tempo de experiência –, ao passo que em outras, essa opção não é apresentada; (iii) a oferta solicitada é apresentada aos trabalhadores que estão disponíveis e atendem aos critérios da plataforma (como os casos em que se dá preferência aos fisicamente mais próximos do usuário) e/ ou do cliente; (iv) em algumas plataformas, o usuário também pode escolher o trabalhador que executará a atividade; (v) havendo a combinação entre oferta e demanda de mão de obra, que pode ocorrer pela ordem de chegada do trabalhador disponível, pela escolha do trabalhador feita pelo usuário ou pela distribuição da atividade feita pela plataforma, a tarefa é executada; (vi) terminada a atividade, o cliente realiza o pagamento para a empresa, que normalmente retém a sua parte e, em seguida, repassa os valores devidos ao trabalhador; (vii) geralmente os trabalhadores são avaliados pelos usuários e, em algumas plataformas, os prestadores de serviços também avaliam os clientes. (Kalil, 2020, p. 100).

Esses trabalhadores são considerados autônomos. Ou seja, não possuem vínculo empregatício com as empresas que administram os aplicativos. Além disso, utilizam veículos próprios, e se responsabilizam pelo Imposto sobre Propriedades de Veículos Automotores (IPVA), taxa de licenciamento, combustíveis, eventuais multas por infrações e por quaisquer outros gastos.

Quanto aos direitos trabalhistas, como são considerados trabalhadores autônomos, não têm os mesmos direitos que os empregados, como: carteira assinada, 13º salário, repouso semanal remunerado, Fundo de Garantia por Tempo de Serviço (FGTS) e os demais direitos.

Na Consolidação das Leis do Trabalho, no artigo 442-B, diz que "A contratação do autônomo, cumpridas por este todas as formalidades legais, com ou sem exclusividade, de forma contínua ou não, afasta a qualidade de empregado prevista no art. 3º desta Consolidação".

É verdade que os trabalhadores por intermediação de aplicativos estão desprotegidos em relação a doenças do trabalho, acidentes de trânsito e outros riscos próprios do trabalho. No entanto, no dia 15 de maio de 2019 foi publicado o Decreto nº 9.792, que regulamenta o inciso III do parágrafo único do art. 11-A da Lei nº 12.587, de 3 de janeiro de 2012, que dispõe sobre a inscrição do motorista de transporte remunerado privado individual de passageiros como contribuinte individual do Regime Geral de Previdência Social (RGPS).

Dessa forma, ao se registrar como Microempreendedor Individual (MEI), o trabalhador adquire Cadastro Nacional de Pessoa Jurídica (CNPJ) e passa a ter os seguintes direitos: salário-maternidade, aposentadoria por invalidez, auxílio-doença, auxílio-reclusão e pensão por morte para seus dependentes. Também podem contabilizar o tempo de trabalho por intermediação de aplicativos para aposentadoria por idade (LISBOA, 2021).

Essa possibilidade não elimina a precariedade das condições de trabalho desses trabalhadores, mas a mitiga, visto que pelo menos existe uma opção na qual eles trabalhem com o mínimo de direitos assecuratórios e dignidade, já que não são considerados empregados.

A Lei nº 13.640, de 26 de março de 2018, altera a Lei nº 12.587, de 3 de janeiro de 2012, para regulamentar o transporte remunerado privado individual de passageiros. E, no artigo 2º, inciso X, o diploma legal trata sobre o:

> [...] transporte remunerado privado individual de passageiros: serviço remunerado de transporte de passageiros, não aberto ao público, para a realização de viagens individualizadas ou compartilhadas **solicitadas exclusivamente por usuários previamente cadastrados em aplicativos ou outras plataformas de comunicação em rede**. (Brasil, 2018, grifo nosso).

Já o artigo 11-A diz que "Compete exclusivamente aos Municípios e ao Distrito Federal regulamentar e fiscalizar o serviço de transporte remunerado privado individual de passageiros previsto no inciso X do art. 4º desta Lei no âmbito dos seus territórios". Ou seja, tem-se aqui a competência exclusiva para a regulamentação da atividade, mas com a obrigatoriedade de se observar as seguintes diretrizes:

> Parágrafo único. Na regulamentação e fiscalização do serviço de transporte privado individual de passageiros, os Municípios e o Distrito Federal deverão observar as seguintes diretrizes, tendo em vista a eficiência, a eficácia, a segurança e a efetividade na prestação do serviço:
> I - efetiva cobrança dos tributos municipais devidos pela prestação do serviço;
> II - exigência de contratação de seguro de Acidentes Pessoais a Passageiros (APP) e do Seguro Obrigatório de Danos Pessoais causados por Veículos Automotores de Vias Terrestres (DPVAT);
> III - exigência de inscrição do motorista como contribuinte individual do Instituto Nacional do Seguro Social (INSS), nos termos da alínea *h* do inciso V do art. 11 da Lei nº 8.213, de 24 de julho de 1991.

Vê-se que no diploma legal há a garantia contra acidentes e a exigência da inscrição do motorista como contribuinte individual junto ao INSS. Dessa forma, as prefeituras e o Distrito Federal, ao regulamentarem a atividade, devem seguir tais diretrizes com o fim de salvaguardar tanto os trabalhadores como os usuários.

Quanto aos trabalhadores, o artigo 11-B é claro quanto às condições para que eles possam atuar:

> O serviço de transporte remunerado privado individual de passageiros previsto no inciso X do art. 4º desta Lei, nos Municípios que optarem pela sua regulamentação, somente será autorizado ao motorista que cumprir as seguintes condições:
> I - possuir Carteira Nacional de Habilitação na categoria B ou superior que contenha a informação de que exerce atividade remunerada;
> II - conduzir veículo que atenda aos requisitos de idade máxima e às características exigidas pela autoridade de trânsito e pelo poder público municipal e do Distrito Federal;

> III - emitir e manter o Certificado de Registro e Licenciamento de Veículo (CRLV);
> IV - apresentar certidão negativa de antecedentes criminais.

Portanto, já existe uma regulamentação federal que busca garantir minimamente alguns direitos aos trabalhadores por intermediação de aplicativos. Dessa forma, apesar da precariedade das condições dos obreiros, o legislador, ainda que timidamente, traçou essas diretrizes e condições. Além disso, se estas não forem respeitadas, o parágrafo único do artigo 11-B alerta que:

> A exploração dos serviços remunerados de transporte privado individual de passageiros sem o cumprimento dos requisitos previstos nesta Lei e na regulamentação do poder público municipal e do Distrito Federal caracterizará **transporte ilegal de passageiros**. (Grifo nosso)

O diploma legal cita o transporte "ilegal" de passageiros quando quis se referir ao transporte "irregular". Trata-se, portanto, de um erro técnico por parte do legislador. Ou seja, se tais diretrizes e condições não forem cumpridas a atividade será considerada irregular, passível das penalidades previstas na legislação de trânsito.

As empresas que operam por meio de aplicativos fazem a intermediação entre os que precisam do serviço e os que o prestam, propiciando uma aproximação.

> A empresa é proprietária da plataforma, a infraestrutura que conecta consumidores, que buscam serviços mais baratos do que os oferecidos por meios tradicionais e maior facilidade no acesso, e trabalhadores, que podem ser amadores ou profissionais e ter baixa ou média qualificação, conforme a natureza da atividade executada. As empresas frequentemente estabelecem de forma unilateral os termos de condição de uso – para tomadores e prestadores de serviço. Na maioria dos casos, também fixam os valores do trabalho e determinam padrões mínimos de qualidade do serviço. (KALIL, 2020, p. 101)

Na prestação do serviço, o trabalhador realiza fisicamente o transporte ou a entrega que o consumidor havia solicitado na plataforma digital. De acordo com Vilela e D'Angelo (2022, p. 14 *apud* De Stefano, 2016):

> […] o serviço é realizado no local, não de maneira virtual, sendo no entanto intermediado por plataformas digitais, ao passo que tanto a oferta quanto a

> contração é realizado por meio delas, de modo que a plataforma se torna a responsável por intermediar esse serviço, gerenciar os trabalhadores e ofertar condições básicas para que os trabalhadores realizem a melhor execução possível desse serviço.

Assim, de fato há uma intermediação dos aplicativos entre os trabalhadores e os consumidores e é preciso que haja uma verificação quanto ao vínculo de emprego, visto que além da aproximação entre consumidor e prestador de serviço, há também algumas exigências que, dependendo da análise do caso concreto, poderão configurar uma relação de emprego.

As empresas também impõem aos trabalhadores uma avaliação que é feita pelo consumidor, dependendo da nota, o trabalhador pode ser desligado da plataforma. Trata-se de uma ferramenta que possibilita a continuidade no mercado, pois existe concorrência no ramo.

> [...] Finalizada a tarefa executada pelo trabalhador, a empresa solicita que o cliente faça a avaliação do serviço, geralmente o classificando em uma escala de um a cinco, sendo um a pior e cinco a melhor nota, ou como positivo ou negativo. Então, as avaliações são consolidadas para se obter uma média. Algumas plataformas utilizam essas avaliações para que o consumidor tenha mais dados na hora de optar por um trabalhador, quando isso é possível. Entretanto, outras usam as notas para analisar a pertinência de o trabalhador continuar participando da plataforma para oferecer os seus serviços, podendo suspendê-lo temporariamente ou até excluí-lo em definitivo. (KALIL, 2020, p. 102).

As empresas fazem a intermediação, avaliam os trabalhadores e coletam dados diversos continuamente por meio de suas plataformas, e isso faz com que perfis de usuários e trabalhadores sejam criados e alimentados, permitindo que os bons executores (aqueles que têm maiores notas) se sobressaiam em relação aos demais.

5 REQUISITOS FORMADORES DO VÍNCULO EMPREGATÍCIO

Os requisitos formadores do vínculo empregatício são cinco: trabalho por pessoa física, pessoalidade, não eventualidade, onerosidade e subordinação (Delgado, 2019).

Será feita uma análise com o fim de reconhecê-los ou não na relação de trabalho dos trabalhadores por intermediação de aplicativos.

Quanto ao primeiro requisito mencionado, este é de fácil entendimento, porque a própria palavra "trabalho" já demonstra que se trata de atividade realizada por pessoa natural (Delgado, 2019). Os motoristas e entregadores são pessoas físicas que trabalham por intermediação de aplicativos ao transportarem pessoas e entregarem os produtos. Portanto esse requisito está presente na relação de trabalho em discussão.

Sobre o segundo requisito, a pessoalidade: "O contrato de trabalho é *intuitu personae*, ou seja, realizado com certa e determinada pessoa" (Martins, 2009, p. 91). Como os trabalhadores por intermediação de aplicativos não podem ceder usuário e senha para que outras pessoas trabalhem por eles, a pessoalidade também está presente na relação de trabalho.

Quanto à eventualidade, neste requisito, o trabalhador deve prestar os serviços continuamente. Ou seja, na relação de emprego, a realização do trabalho é habitual, repetitiva e rotineira. As obrigações das partes se prolongam no tempo, com efeitos contínuos. É importante ser ressaltado que para se perceber esse requisito não é necessário que os serviços sejam prestados todos os dias, pois o importante é que haja uma constância, a intenção de permanência (Romar, 2018).

Os motoristas e os entregadores executam os serviços de forma contínua, mesmo que não seja obrigatório que eles realizem os trabalhos diariamente. Assim, apesar deles terem liberdade de escolher os dias e os horários que trabalharão, não descaracteriza a habitualidade. No entanto, o caso concreto deve consignar se esse requisito é satisfeito, a depender da regularidade da prestação de serviço (Lisboa, 2021).

O quarto requisito é o da onerosidade. Aqui, existe uma contraprestação ao trabalhador. Dessa forma, "Não há contrato de trabalho a título gratuito, ou seja, sem encargos e vantagens recíprocas. O contrato de trabalho é bilateral e oneroso, isto é, o empregado, ao prestar os serviços, tem direito aos salários" (Neto; Cavalcante, 2019, p. 404). Os trabalhadores por intermediação de aplicativos realizam os trabalhos motivados pela contraprestação. Assim, tal requisito está presente na relação de trabalho.

Alguns autores consideram a alteridade também como um requisito caracterizador da relação empregatícia. Significa que os riscos da atividade econômica são assumidos pelo empregador, e não pelo empregado (Romar, 2018). Assim, se ela fosse reconhecida como um dos requisitos, a relação entre os trabalhadores e as empresas de aplicativos não seria de emprego, pois os motoristas e entregadores usam os próprios veículos, pagam o IPVA, combustível, óleo, pneus, eventuais multas de trânsito e danos a outros veículos. Assim, não estaria presente a alteridade (Lisboa, 2021).

Por último, será abordada a subordinação, que, sem dúvidas, é o requisito que ganha maior proeminência no reconhecimento da relação empregatícia (Delgado, 2019), tanto que nas decisões judiciais é o ponto mais abordado.

A subordinação é a sujeição do empregado às ordens do empregador. Ou seja, já que este assume os riscos do negócio, nada mais justo do que ele exercer sobre o prestador de serviços o poder de direção. Assim, o trabalhador confere ao tomador de serviço o poder de direção sobre o seu trabalho. Dessa forma, existe uma dependência do empregado em relação ao empregador. E, tal dependência não é mais a econômica, técnica e social, pois tais teorias estão superadas. A natureza da subordinação é, portanto, jurídica (Romar, 2018).

De acordo com Delgado (2019, p. 352), a subordinação tem dimensões, que são: clássica, objetiva e estrutural. A subordinação clássica "deriva do contrato de trabalho, pela qual o trabalhador compromete-se a acolher o poder de direção empresarial no tocante ao modo de realização de sua prestação laborativa". Ou seja, isso condiciona o trabalhador a receber ordens com manifesta intensidade de comando.

Já a subordinação objetiva é a "[...] que se manifesta pela integração do trabalhador nos fins e objetivos do empreendimento do tomador de serviços, ainda que afrouxadas 'as amarras do vínculo empregatício'" (Delgado, 2019, p. 352). É a simples integração da atividade do empregado aos fins da empresa, reduzindo a relevância das ordens e ressaltando a ideia de integração aos objetivos empresariais.

A subordinação estrutural, conforme Delgado (2016, p. 353) é a "[...] que se expressa 'pela inserção do trabalhador na dinâmica do tomador de seus serviços, independentemente de receber (ou não) suas ordens diretas, mas acolhendo,

estruturalmente sua dinâmica de organização e funcionamento'". Isso significa que o empregado deve desempenhar atividade essencial ao funcionamento estrutural da empresa. A sua atividade deve ser parte da atividade fim do empreendimento, que sem ela a empresa não funcionaria.

O avanço tecnológico possibilitou que as rotinas de alguns empregados fossem modificadas. O *home office*, uma forma de prestar serviços fora das dependências da empresa, já é uma realidade cada vez mais comum, e a Lei 12.551/2011, que alterou o artigo 6º da CLT, estabeleceu que não existe mais diferença entre o trabalho realizado no estabelecimento da empresa e o executado à distância.

Para isso, a mudança legislativa passou a considerar que os meios telemáticos se equiparam aos meios pessoais de ordens de comando, supervisão, controle e disciplina. Dessa forma, para ser subordinado, o empregado poderia trabalhar à distância e receber as ordens, ser supervisionado, controlado e disciplinado por meio das tecnologias da informação e comunicação. Vê-se que mesmo à distância é possível identificar a subordinação.

O artigo 6º da CLT diz que "Não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado à distância, desde que estejam caracterizados os pressupostos da relação de emprego" (2022). Também, a Reforma Trabalhista de 2017, que introduziu vários artigos na Consolidação das Leis do Trabalho (75-A ao 75-E) regulamentou o teletrabalho, permitindo que a partir daquele momento os empregados poderiam prestar serviços não mais apenas no estabelecimento empresarial, contudo sem configurar trabalho externo. Foi um importante avanço da legislação no sentido de acompanhar a evolução tecnológica. Assim, passou-se a equiparar-se o trabalho realizado dentro da empresa com o executado fora das dependências desta.

Além das três dimensões da subordinação abordadas anteriormente, discute-se uma quarta subordinação, conhecida como subordinação algorítmica, que seria efetuada por meio de aplicativos. Dessa forma, o trabalhador estaria sendo monitorado e controlado por algoritmos do aplicativo, que direcionariam a prestação de serviços de forma mais precisa e intensa do que a subordinação clássica.

A subordinação algorítmica se daria em situações em que haveria o controle, o comando e a supervisão do trabalho por meio da plataforma digital. "Assim, será dita 'subordinação algorítmica' aquela em que o controle do trabalho é definido por uma sequência lógica, finita e definida de instruções e se desenrola via ferramentas tecnológicas, tais como aplicativos". (Fincato; Wünsch, 2020, p. 51).

É fato que os aplicativos possuem algoritmos que coletam dados como a geolocalização dos trabalhadores, rotas e distância percorrida, quantidade de horas trabalhadas, os consumidores que foram atendidos e outras informações. Além disso, o valor a ser cobrado e forma de pagamento são estipulados pelos algoritmos:

> [...] a subordinação evoluiu para um novo patamar, ou seja, a algorítmica. Com a evolução da tecnologia e das ferramentas digitais criadas a partir dessa, o empregador não precisa mais exercer seu controle direto sobre o empregado, pois, as ordens, os comandos e a direção podem se dar através de um aplicativo de smartphone, utilizando o algoritmo, até mais eficiente e de menor custo. Portanto, a subordinação algorítmica surgiu como nova forma de subordinação, e deve ser utilizada como requisito para caracterização da Relação de Emprego, garantindo aos motoristas o reconhecimento do vínculo de emprego com as plataformas digitais de transporte de passageiros, e, consequentemente, com a UBER. (Barbosa, 2022, p. 48).

No entanto, existe um detalhe que faz com que a subordinação não seja reconhecida e, consequentemente, o vínculo empregatício, que é a escolha dos motoristas e entregadores quanto ao dia e horário de trabalho. No Código da Comunidade Uber, está previsto que:

> **Quando motoristas ou entregadores parceiros não quiserem aceitar solicitações de viagem ou entrega, basta desconectar ou ficar offline**. Isso ajuda a manter o bom funcionamento do sistema para todos os outros motoristas e entregadores parceiros e usuários.
> Nossa tecnologia pode supor que motoristas e entregadores parceiros que recusam diversas solicitações consecutivas de viagens não querem aceitar mais viagens ou se esqueceram de sair da conta. Nesses casos, para manter a segurança e a integridade da conta, ela pode ficar offline temporariamente. **Nada impede a reconexão para que eles voltem a aceitar viagens ou entregas**. (Grifo nosso) (Uber, 2022).

Os trabalhadores por intermediação de aplicativos não sofrem punições ao ficarem *offline*, mas apenas se permanecerem *online* e recusarem reiteradamente as viagens. Assim, vê-se uma flexibilidade que impede de se reconhecer a subordinação, visto que o trabalhador tem a liberdade de trabalhar quando quiser, situação típica do trabalhador autônomo, que conforme Neto e Cavalcante (2019, p. 414):

> [...] é o que não se submete ao poder diretivo de quem contrata os seus serviços. Os elementos característicos: (a) exerce livremente a sua atividade, estabelecendo quando e como os seus serviços serão realizados; (b) assume os riscos da sua atividade; (c) é comum que os serviços prestados estão vinculados a um determinado resultado do trabalho; (d) o resultado do trabalho pode ser obtido de forma individual pelo próprio trabalhador autônomo ou com o auxílio de outros trabalhadores por ele remunerados. Em suma: é um trabalhador por conta e risco próprio.

Dessa forma, em que pese as condições de trabalho dos trabalhadores por intermédio de aplicativos e o funcionamento dos algoritmos nestes, a subordinação, em nenhuma das dimensões pode ser reconhecida, visto que ao ter a opção de trabalhar quando e onde quiser, esses trabalhadores não são subordinados, e portanto, não são empregados.

6 JURISPRUDÊNCIA DO TST

Em acórdão da 5ª Turma do TST, como resultado do julgamento de um Agravo de Instrumento em Recurso de Revista, processo nº TST-RR-1000123-89.2017.5.02.0038, o detalhe que configura o não reconhecimento do vínculo empregatício foi exatamente a flexibilidade do trabalhador quanto ao dia e horário de trabalho:

> Com efeito, o reclamante admite expressamente a possibilidade de ficar "off line", sem delimitação de tempo, circunstância que indica a ausência completa e voluntária da prestação dos serviços em exame, que só ocorre em ambiente virtual. Tal fato traduz, na prática, a ampla flexibilidade do autor em determinar sua rotina, seus horários de trabalho, locais que deseja atuar e quantidade de clientes que pretende atender por dia. Tal autodeterminação é incompatível com o reconhecimento da relação de emprego, que tem como

> pressuposto básico a subordinação, elemento no qual se funda a distinção com o trabalho autônomo. (Brasil, 2020).

O acórdão da 5ª Turma ainda complementou afirmando que "[...] as relações de trabalho têm sofrido intensas modificações com a revolução tecnológica, de modo que incumbe a esta Justiça Especializada permanecer atenta à preservação dos princípios que norteiam a relação de emprego, desde que presentes todos os seus elementos".

A 4ª Turma do TST, também em sede de Agravo de Instrumento em Recurso de Revista, processo nº TST-AIRR-1092-82.2021.5.12.0045, não reconhece o vínculo empregatício por entender que:

> [...] é latente a ampla autonomia do motorista em escolher os dias, horários e forma de labor, podendo desligar o aplicativo a qualquer momento e pelo tempo que entender necessário, sem nenhuma vinculação a metas determinadas pela "Uber Brasil Tecnologia Ltda." ou sanções decorrentes de suas escolhas. (BRASIL, 2022).

Nos dois casos concretos apreciados pelas turmas 4ª e 5ª do TST, os trabalhadores afirmaram que escolhiam o dia e o horário de trabalho. E, essa informação foi crucial para o não reconhecimento do vínculo de emprego, pois a subordinação é um dos requisitos para a caracterização do emprego.

Já a 3ª turma do TST, em sede de recurso de revista no processo nº TST-RR-100353-02.2017.5.01.0066, sob a relatoria do Ministro Maurício Godinho Delgado (2022), reconheceu o vínculo empregatício de um trabalhador por intermediação de aplicativo. O acórdão reconheceu o vínculo nos seguintes termos:

> [...] a subordinação jurídica foi efetivamente demonstrada, destacando-se as seguintes premissas que se extraem do acórdão regional, incompatíveis com a suposta autonomia do trabalhador na execução do trabalho: 1) a Reclamada organizava unilateralmente as chamadas dos seus clientes/passageiros e indicava o motorista para prestar o serviço; 2) a empresa exigia a permanência do Reclamante conectado à plataforma digital para prestar os serviços, sob risco de descredenciamento da plataforma digital (perda do trabalho); 3) a empresa avaliava continuamente a performance dos motoristas, por meio de um controle telemático e pulverizado da qualidade dos serviços, a partir da tecnologia da plataforma digital e das notas atribuídas pelos clientes/passageiros ao trabalhador. Tal sistemática servia, inclusive, de parâmetro para o descredenciamento do motorista em face da plataforma

> digital - perda do trabalho -, caso o obreiro não alcançasse uma média mínima; 4) a prestação de serviços se desenvolvia diariamente, durante o período da relação de trabalho – ou, pelo menos, com significativa intensidade durante os dias das semanas -, com minucioso e telemático controle da Reclamada sobre o trabalho e relativamente à estrita observância de suas diretrizes organizacionais pelo trabalhador, tudo efetivado, aliás, com muita eficiência, por intermédio da plataforma digital (meio telemático) e mediante a ativa e intensa, embora difusa, participação dos seus clientes/passageiros.

Consta no referido acordão, em continuidade que:

> Saliente-se ser fato notório (art. 337, I, do CPC/15) que a Reclamada é quem estabelece unilateralmente os parâmetros mais essenciais da forma de prestação dos serviços e da dinâmica de funcionamento da atividade econômica, como, por exemplo, a definição do preço da corrida e do quilômetro rodado no âmbito de sua plataforma digital. Desse quadro, se percebe a configuração da subordinação jurídica nas diversas dimensões: a) clássica, em face da existência de incessantes ordens diretas da Reclamada promovidas por meios remotos e digitais (art. 6º, parágrafo primeiro, da CLT), demonstrando a existência da assimetria poder de direção/subordinação e, ainda, os aspectos diretivo, regulamentar, fiscalizatório e disciplinar do poder empregatício; b) objetiva, tendo em vista o trabalho executado estritamente alinhado aos objetivos empresariais; c) estrutural, mediante a inteira inserção do profissional contratado na organização da atividade econômica desempenhada pela Reclamada, em sua dinâmica de funcionamento e na cultura jurídica e organizacional nela preponderante; d) por fim, a subordinação algorítmica, que consiste naquela efetivada por intermédio de aferições, acompanhamentos, comandos, diretrizes e avaliações concretizadas pelo computador empresarial, no denominado algoritmo digital típico de tais empresas da Tecnologia 4.0.

O acordão aborda a questão referente aos horários de trabalho desses profissionais, afirmando que:

> Saliente-se, por oportuno, que a suposta liberdade do profissional para definir seus horários de trabalho e de folgas, para manter-se ligado, ou não, à plataforma digital, bem como o fato de o Reclamante ser detentor e mantenedor de uma ferramenta de trabalho – no caso, o automóvel utilizado para o transporte de pessoas – são circunstâncias que não têm o condão de definir o trabalho como autônomo e afastar a configuração do vínculo de emprego. Reitere-se: a prestação de serviços ocorria diariamente, com sujeição do Autor às ordens emanadas da Reclamada por meio remoto e telemático (art. 6º, parágrafo único, da CLT); havia risco de sanção disciplinar (exclusão da plataforma) em face da falta de assiduidade na conexão à plataforma e das notas atribuídas pelos clientes/passageiros da Reclamada; inexistia liberdade ou autonomia do Reclamante para definir os preços das corridas e dos seus serviços prestados, bem como escolher os seus passageiros (ou até mesmo criar uma carteira própria de clientes); não se verificou o mínimo de domínio do

> trabalhador sobre a organização da atividade empresarial, que era centralizada, metodicamente, no algoritmo da empresa digital; ficou incontroversa a incidência das manifestações fiscalizatórias, regulamentares e disciplinares do poder empregatício na relação de trabalho analisada [...].

A divergência mormente recai sobre a subordinação, que não foi reconhecida pelas Turmas 4ª e 5ª, diferentemente da 3ª Turma, que a reconheceu na dimensão algorítmica. Assim, há uma divergência de entendimento quanto ao reconhecimento do vínculo empregatício com ênfase na subordinação.

7 TENDÊNCIA JURISPRUDENCIAL

Não é novidade que as turmas do Tribunal Superior do Trabalho divirjam entre si, tanto que existe a Subseção I Especializada em Dissídios Individuais (SDI-1). E a função da SDI-1 é uniformizar teses antagônicas das turmas do TST, e ela já foi acionada para se debruçar sobre o tema, pois a terceira e a oitava turmas divergiram da quarta e quinta turmas.

No dia 06/10/2022, a SDI - 1 iniciou o julgamento de dois embargos de divergência (E-RR-1000123-89.2017.5.02.0038 e E-RR-100353-02.2017.5.01.0066) contra as decisões divergentes da terceira turma, que reconheceu o vínculo de emprego, e da quinta turma, que não reconheceu o vínculo. Mas o julgamento foi suspenso depois de um pedido de vista do Ministro Cláudio Brandão.

Antes, a relatora do processo Ministra Maria Cristina Peduzzi já havia proferido voto no sentido de não reconhecer o vínculo de emprego por entender que a terceira turma teria usado em sua decisão premissas distintas das expressas no acórdão do Tribunal Regional do Trabalho da 1ª Região (RJ).

Em seguida, o Ministro Aloysio Corrêa da Veiga sugeriu que o processo fosse remetido ao Tribunal Pleno, e que seja julgado em sede de recursos repetitivos, com a fixação de tese vinculante sobre o tema, o que foi aceito por unanimidade pelos integrantes da subseção.

É claro que o teor probatório de cada processo é diferente, e por isso, decisões podem ser antagônicas. No entanto, os casos apreciados pelas turmas do TST são semelhantes, com especificidades que não definiram o entendimento quanto ao reconhecimento ou não da subordinação jurídica. Trata-se, portanto, de uma divergência quanto à subordinação, que deve estar presente para que se caracterize o vínculo empregatício.

Ressalta-se ainda que dependendo do caso concreto pode-se ou não reconhecer a relação de emprego, visto que o princípio da primazia da verdade real viabiliza a comparação entre o que está escrito ou ajustado verbalmente entre empregado e empregador, e o que de fato acontece. Assim, ao analisar os fatos do caso concreto, é perfeitamente possível que o trabalhador esteja numa relação empregatícia, se os requisitos estiverem presentes. Cassar aborda com precisão o princípio da primazia da verdade real ao afirmar que

> O que importa é o que aconteceu e não o que está escrito. […]. O princípio da primazia da realidade destina-se a proteger o trabalhador, já que seu empregador poderia com relativa facilidade obrigá-lo a assinar documentos contrários aos fatos e aos seus interesses. Ante o estado de sujeição permanente que o empregado se encontra durante o contrato de trabalho, algumas vezes submete-se às ordens do empregador, mesmo que contra sua vontade. (Cassar, 2019, p. 189).

Dessa forma, se os requisitos estiverem presentes, o vínculo empregatício deve ser reconhecido. Por isso, de forma geral, os motoristas e entregadores não são empregados por faltar o requisito proeminente da caracterização da relação empregatícia, a subordinação. Ou seja, a realidade que se apresenta é que esses trabalhadores não são subordinados aos aplicativos, visto que podem deixá-los “off-line” a qualquer momento e pelo tempo que quiserem, sem a necessidade de justificativas às empresas que os administram.

Além disso, em que pese a construção teórica da subordinação algorítmica, que é uma realidade quando o trabalhador está “on-line”, é de difícil aplicação, visto que ele é quem decide onde, quando e por quanto tempo irá trabalhar. Assim, o trabalhador de fato fica sob os comandos e controle do algoritmo, que determina quais “corridas” ou entregas

são atribuídas a ele, com base em fatores como a localização, a disponibilidade de serviços ("corridas" e entregas) na área e a avaliação de eficiência dele atribuída pelos usuários.

Devido ao fato do trabalhador poder desligar o aplicativo e o ligar apenas quando quiser, sem punição - se o tempo não for excessivo -, é extremamente difícil de reconhecer a relação de emprego, a menos que a subordinação jurídica prevista na CLT seja ampliada para abarcar esses trabalhadores.

Ao se analisar as decisões no âmbito do TST, não é possível vislumbrar uma tendência jurisprudencial quanto ao reconhecimento ou não do vínculo empregatício por causa da divergência principalmente quanto à subordinação, pois alguns ministros da corte entendem que há autonomia do trabalhador por este poder escolher o local, o dia, a hora e por quanto tempo trabalhar. Já outros, entendem que não há autonomia do trabalhador ao reconhecerem a subordinação algorítmica. O fato é que há divergência quanto ao reconhecimento da subordinação, inclusive até da subordinação estrutural.

A 4ª Turma do TST, em sede de Agravo de Instrumento em Recurso de Revista, processo nº TST-AIRR-1092-82.2021.5.12.0045, não reconhece sequer a subordinação estrutural nos seguintes termos:

> [...] não se há de falar em existência de subordinação estrutural. Primeiro porque esse conceito, que visa enquadrar como empregado qualquer profissional que se encontre inserido na organização do empreendimento, oferecendo labor indispensável aos fins da atividade empresarial, ainda que não esteja sob o seu comando direto, **não encontra amparo na legislação trabalhista (arts. 2º e 3º da CLT)**. Não cabe ao Poder Judiciário ampliar conceitos jurídicos a fim de reconhecer o vínculo empregatício de profissionais que não atuam enquadrados no conceito legal de subordinação, devendo ser respeitada a modernização das formas de trabalho, emergentes da dinâmica do mercado concorrencial atual e, principalmente, de desenvolvimentos tecnológicos [...]
> Segundo porque, mesmo que se entendesse aplicável o conceito de subordinação estrutural, não seria a hipótese dos autos, pois as empresas provedoras de aplicativos de tecnologia, como a "99 Tecnologia Ltda." e a "Uber Brasil Tecnologia Ltda.", têm como finalidade conectar quem necessita da condução com o motorista credenciado, sendo o serviço prestado de motorista, em si, competência do profissional e apenas uma consequência inerente ao que propõe o dispositivo. (Grifo nosso)

Portanto, a subordinação estrutural, que já não é uma construção doutrinária nova, encontra forte resistência. Assim, não é exagero supor que a subordinação algorítmica também enfrentará intensa resistência. Dessa forma, não se pode prever a tendência jurisprudencial apesar dos debates e das decisões do TST.

Até o dia 23/02/2023, no âmbito da SDI-1, o processo E-RR-1000123-89.2017.5.02.0038 não estava pautado, assim como o E-RR-100353-02.2017.5.01.0066. Ambos foram retirados de pauta no dia 06/10/2022 e foram remetidos ao Plenário do TST, que ainda não agendou julgamento.

Pelo fato do assunto ser relativamente novo, relevante e polêmico é possível que o plenário do TST retarde o julgamento da divergência jurisprudencial, visto que uma decisão sem um amplo e profundo debate pode causar efeitos catastróficos para as empresas, trabalhadores e usuários. Dessa forma, é compreensível que não se tenha um desfecho num curto espaço de tempo. Ou seja, será necessário esperar.

8 DIREITO COMPARADO

O debate a respeito do reconhecimento do vínculo empregatício dos motoristas e entregadores que usam o serviço dos aplicativos também acontece em outros países. Mas é o ordenamento jurídico dos demais países é diferente do pátrio, o que pode fazer grande diferença quanto à configuração da relação de emprego. Além disso, não será feita uma análise das decisões judiciais dos países pesquisados, mas um panorama de como está o debate neles e se já existe uma tendência jurisprudencial.

Nos Estados Unidos, no estado da Califórnia, o legislativo criou uma lei que passou a vigorar no início de 2020, e que cria vínculo empregatício entre motoristas e aplicativos, especificamente as empresas Uber e Lyft (Araújo, 2020). Na França, o judiciário, por entender que os motoristas não constroem a própria clientela e nem define os preços do serviço, reconheceu o vínculo empregatício entre aqueles e os aplicativos (Lisboa, 2022).

Em 2019, o Tribunal Superior de Justiça de Asturias, Espanha, decidiu que existe uma relação empregatícia entre entregadores e um aplicativo. Trata-se da Glovo, Startup

espanhola que faz delivery e entrega de produtos em geral. No contrato entre os entregadores e a empresa existiam cláusulas que contemplavam a relação de emprego, entre elas o estabelecimento de horário de trabalho. Em Madrid, também em 2019, um juiz reconheceu a relação de emprego entre os entregadores e o aplicativo Deliveroo por causa da falta de autonomia dos trabalhadores, pois existia a subordinação e os de requisitos que configuram um vínculo empregatício naquele país (Araújo, 2020).

Portanto não há como afirmar que existe uma tendência para se reconhecer o vínculo de emprego entre motoristas e entregadores e os aplicativos pelos países, pois a realidade é nova e existem muitos interesses econômicos envolvidos nessa discussão. Ou seja, não é apenas no Brasil que está acontecendo a discussão e com decisões judiciais conflitantes.

No Brasil, no âmbito do Congresso Nacional, existem iniciativas que tratam do assunto, como o Projeto de Lei nº **3.498/2019**, que tem o objetivo de tornar obrigatória a contratação de seguro de danos causados ou roubo dos veículos utilizados no transporte remunerado privado individual de passageiros. Atualmente, esse PL encontra-se em tramitação na Comissão de Viação e Transportes da Câmara dos Deputados.

Existe também o Projeto de Lei nº 3.570/2020, que busca instituir a Lei de Proteção dos Trabalhadores de Aplicativos de Transporte Individual Privado ou Entrega de Mercadorias. Esse PL está em tramitação na Comissão de Assuntos Econômicos do Senado Federal.

Tem ainda o Projeto de Lei nº 3.055/2021, que trata das relações de trabalho entre as empresas operadoras de aplicativos e os trabalhadores que se utilizam das plataformas digitais. Esse PL teve a tramitação encerrada ao ser arquivada no plenário do Senado Federal.

Já o Projeto de Lei nº 3.796/2021 objetiva aumentar as penas de crimes cometidos contra motoristas de táxi e de serviço de transporte de passageiro por aplicativo. Esse PL também teve a tramitação encerrada ao ser arquivada no plenário do Senado Federal.

O Projeto de Lei nº 759/2022, que isenta do Imposto sobre Produtos Industrializados os veículos para uso de motoristas de aplicativos, como mototaxistas e

motoboys. Atualmente, esse PL está em tramitação e deve ser apreciado no Plenário do Senado Federal.

Por último, o Projeto de Lei nº 1.615/2022, que aborda sobre o trabalho dos prestadores de serviços com uso de aplicativos de entrega de mercadorias ou transporte individual ou compartilhado privado. Esse PL está em tramitação, esperando ser apreciado no Plenário do Senado Federal.

Dessa forma, a discussão também chegou no legislativo por meio de projetos de leis, indicando que o parlamento está se debruçando sobre o assunto. No entanto, ainda é prematuro afirmar qual será a resolução que o Congresso Nacional entregará à sociedade brasileira.

9 CONSIDERAÇÕES FINAIS

O avanço tecnológico fez com que mudanças acontecessem no mercado de trabalho e a realidade que se apresenta é repleta de novidades e desafios que precisam ser estudados, discutidos e entendidos. E, entre as mudanças que o avanço tecnológico trouxe, está a Indústria 4.0, e dela surgiu a *Gig Economy*.

Como desdobramento da *Gig Economy*, o *work on demand* ganhou forte projeção e adesão no mercado de trabalho, causando grande impacto nas relações de trabalho. Dessa forma, um grande debate passou a acontecer na sociedade a respeito da natureza da relação de trabalho dos trabalhadores por intermediação de aplicativos e as empresas com os administram.

Atualmente, os trabalhadores por intermediação de aplicativos prestam serviços específicos e por eles são pagos sem, contudo, formar vínculo de emprego com as empresas, como os motoristas e entregadores que colaboram elas. Esses trabalhadores são considerados colaboradores independentes, e não empregados.

O debate chegou ao judiciário e as decisões conflitantes da justiça trabalhista, inclusive das turmas 3ª e 5ª do Tribunal Superior do Trabalho, analisadas neste trabalho, o recrudesceram, causando apreensão e insegurança jurídica, o que não é inédito no Brasil. Dessa forma, até o legislativo se debruçar sobre o tema e decidir a respeito, a

justiça trabalhista continuará debatendo até que seja construído um entendimento jurisprudencial, o que já está acontecendo no âmbito da SDI-1.

Os requisitos caracterizadores do vínculo de emprego, que são: o trabalho por pessoa física, pessoalidade, não eventualidade, onerosidade e subordinação, dispostos nos artigos 2º e 3º da CLT, foram abordados, e por meio de exercícios de subsunção, foram confrontados com a relação de trabalho que existe entre os motoristas e entregadores e as empresas.

Depois da confrontação, percebeu-se que foram identificados os requisitos do trabalho por pessoa humana, pessoalidade, não eventualidade e onerosidade. No entanto, o requisito subordinação, que é a mais discutida por ser a mais proeminente entre os requisitos, não foi percebida, porque mesmo que fossem consideradas as dimensões objetiva, estrutural e a algorítmica, esta que é construção doutrinária recente, não seria possível de se reconhecer o vínculo pelo fato do trabalhador escolher o dia, o horário de trabalho e a quantidade de horas a serem trabalhadas, o que descaracteriza a subordinação.

O debate sobre a natureza da relação de trabalho dos trabalhadores por intermediação de aplicativos é uma realidade também em outros países, como Estados Unidos, França e Espanha, nos quais há decisões judiciais e construção legislativas que reconhecem o vínculo de emprego e, também, a necessidade de direitos mínimos para os trabalhadores.

No Brasil, as turmas 3ª e 8ª do Tribunal Superior do Trabalho reconheceram o vínculo de emprego por entenderem que os requisitos da relação de emprego estavam presentes, mas a 4ª e 5ª turmas, decidiram no sentido oposto porque não perceberam o requisito da subordinação. Assim, a Subseção I Especializada em Dissídios Individuais foi acionada e iniciou o julgamento para uniformizar o entendimento da corte, mas foi suspenso depois de um pedido de vista de um dos ministros.

A discussão está acontecendo na academia, no judiciário, no legislativo e na sociedade em geral, e não é possível vislumbrar uma tendência que favoreça os trabalhadores, as empresas de aplicativos ou um meio termo que cause o mínimo de transtornos possíveis, visto que quando se trata de questões econômicas, os efeitos

colaterais costumam ser grandes e profundos, o que também justifica a relativa demora da resolução da controvérsia.

REFERÊNCIAS

ARAÚJO, Marcella Pereira de. A competência trabalhista no século XXI: indústria 4.0. 2020. 128p. Dissertação (Mestrado em Direito) – PUC Minas Gerais, Belo Horizonte, 2020.

BARBOSA, Renan Eleutério. **Subordinação algorítmica como requisito para a caracterização de relação de emprego nas plataformas digitais de transporte de passageiros**. 2022. 56 p. Monografia (Graduação em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2022. Disponível em: https://repositorio.ufsc.br/handle/123456789/232492?show=full. Acesso em: 20 jan. 2023.

BRASIL. **Consolidação das Leis do Trabalho**. Decreto-Lei nº 5.452, de 1º de maio de 1943. Diário Oficial da União. Rio de Janeiro, RJ, 09, Ago. de 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 20 jan. 2023.

BRASIL. Lei 13.640, de 26 de Março de 2018. Altera a Lei nº 12.587, de 3 de janeiro de 2012, para regulamentar o transporte remunerado privado individual de passageiros. *In:* **Diário Oficial da União**, Brasília, DF, 27, Mar. de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13640.htm. Acesso em: 14 fev. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei 3498/2019**. Altera a Lei nº 12.587, de 3 de janeiro de 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2207803. Acesso em: 14 fev. 2023.

BRASIL. Senado Federal. **Projeto de Lei 3570/2020**. Institui a Lei de Proteção dos Trabalhadores de Aplicativos de Transporte Individual Privado ou Entrega de Mercadorias. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/143149. Acesso em: 14 fev. 2023.

BRASIL. Senado Federal. **Projeto de Lei 3055/2021**. Altera a Consolidação das Leis do Trabalho (CLT). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/149697. Acesso em: 14 fev. 2023.

BRASIL. Senado Federal. **Projeto de Lei 3796/2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/150519. Acesso em: 14 fev. 2023.

BRASIL. Senado Federal. **Projeto de Lei 759/2022**. Altera a Lei nº 8.989, de 24 de fevereiro de 1995. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/152511. Acesso em: 14 fev. 2023.

BRASIL. Senado Federal. **Projeto de Lei 1615/2022**. Dispõe sobre o trabalho dos prestadores de serviços com uso de aplicativos de entrega de mercadorias ou transporte individual ou compartilhado privado e estabelece limites e regras para a realização dessas modalidades de trabalho e dá outras providências. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/153567. Acesso em: 14 fev. 2023.

BRASIL. Tribunal Superior do Trabalho. **Recurso de Revista que reconhece vínculo empregatício entre motorista e Uber**. Relator: Maurício Godinho Delgado. 11 abr. 2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tst/1456803327. Acesso em: 20 jan. 2023.

BRASIL. Tribunal Superior do Trabalho. **Agravo de Instrumento em Recurso de Revista que não reconhece vínculo de emprego entre motorista e Uber**. Relator: Breno Medeiros. 07 fev. de 2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tst/807016681. Acesso em: 22 jan. 2023.

BRASIL. Tribunal Superior do Trabalho. **Recurso de Revista que reconhece vínculo empregatício entre motorista e Uber**. Relator: Ives Granda da Silva Martins Filho. 02 dez. 2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tst/1715562704/inteiro-teor-1715562705. Acesso em: 24 jan. 2023.

CAMBRIDGE DICTIONARY. **Gig Economy**. Cambridge: Cambridge. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles-portugues/gig-economy. Acesso em: 19 jan. 2023.

CASSAR, Vólia Bomfim. **Direito do trabalho**. Niterói: Impetus, 2019.

DELGADO, Mauricio Godinho. **Curso de direito do trabalho**. 18. ed. - São Paulo: LTr, 2019.

FELICIANO, Guilherme Guimarães; PASQUALETO, Olívia de Quintana Figueiredo. (Re)descobrindo o Direito do Trabalho: Gig Economy, Uberização do Trabalho e

Outras Reflexões. In. **ENAMATRA:** Escola Nacional Associativa dos Magistrados da Justiça do Trabalho, p. 54-68, DF, 2021. Disponível em: <https://www.anamatra.org.br/images/publicacao/enamatra/Anamatra_book_PDT.pdf. Acesso em: 02 fev. 2023.

FINCATO, Denise Pires; WÜNSCH, Guilherme. Subordinação algorítmica: caminho para o direito do trabalho na encruzilhada tecnológica? **Revista do Tribunal Superior do Trabalho**, São Paulo, v. 86, n. 3, p. 40-56, jul./set. 2020. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/181114/2020_fincato_denise_subordinacao_algoritmica.pdf?sequence=1&isAllowed=y. Acesso em: 03 fev. 2023.

IBGE - Instituto Brasileiro de Geografia e Estatística. **Desemprego**. Rio de Janeiro: IBGE, 2022. Disponível em: https://www.ibge.gov.br/explica/desemprego.php. Acesso em: 11 jan. 2023.

KALIL, Renan Bernardi. **A regulação do trabalho via plataformas digitais**. 1. ed. São Paulo: Blucher, 2020.

LEITE, Carlos Henrique Bezerra. **Curso de direito do trabalho**. 12. ed. – São Paulo: Saraiva Educação, 2020.

LISBOA, Anna Luiza de Carvalho. Gig Economy e as (Re)Configurações de Trabalho. **Revista Estudantil Manus Iuris**, v. 2, n. 1, p. 57-70, jan/jun. 2021. Disponível em: https://periodicos.ufersa.edu.br/rmi/issue/view/277/33. Acesso em: 25 jan. 2023.

MARTINS, Sérgio Pinto. **Direito do Trabalho**. 25. ed. São Paulo: Atlas, 2009.

MORIN, Ester. Os Sentidos do Trabalho. **Revista de Administração de Empresas**, v. 41, n. 3, p. 8-19, jul/set. 2001. Disponível em: https://www.scielo.br/j/rae/a/w9w7NvLzpqcXcjFkCZ3XVMj/?lang=pt&format=pdf. Acesso em: 20 jan. 2023.

NETO, Francisco Ferreira Jorge; CAVALCANTE, Jouberto de Quadros Pessoa. **Direito do Trabalho**. 9. ed. São Paulo: Atlas, 2019.

RODRIGUES, Priscila Lauande. Trabalhadores em Plataformas Digitais: Natureza Jurídica e Repercussões Sóciojurídicas sob a Perspectiva do Direito Comparado. *In*: **ENAMATRA**: Escola Nacional Associativa dos Magistrados da Justiça do Trabalho, p. 195-213, 2021. Disponível em: https://www.anamatra.org.br/images/publicacao/enamatra/Anamatra_book_PDT.pdf. Acesso em: 02 fev. 2023.

ROMAR, Carla Teresa Martins. **Direito do trabalho**. 5. ed. São Paulo: Saraiva Educação, 2018.

SILVA, Brenda Zopolato Fante; SOUZA, Victor Vinicius Cordeiro de. A 4ª Revolução Industrial e seus Impactos no Futuro dos meios do Trabalho. **Encontro de Iniciação Científica**, v. 17, n. 17, p. 1-19, jan/jun. 2021. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/9107/67650792. Acesso em: 02 fev. 2023.

UBER. **Código da Comunidade Uber**. São Paulo: UBER, 2022. Disponível em: https://www.uber.com/legal/pt-br/document/?name=general-community-guidelines&country=brazil&lang=pt-br. Acesso em: 16 jan. 2023.

VILELA, Vitória Henrique; D'ANGELO, Isabele Bandeira de Moraes. Uberização do Mercado de Trabalho: uma análise acerca das vulnerabilidades do trabalhador de plataforma no Brasil. **Revista Jurídica Luso – Brasileira**. Lisboa, v. X, n. 6, p. 2311 – 2347, jun. 2022. Disponível em: https://www.cidp.pt/revistas/rjlb/2022/6/2022_06_2311_2347.pdf. Acesso em: 24 jan. 2023.

WYZYKOWSKI, Adriana. Revolução tecnológica, indústria 4.0 e o teleassédio moral organizacional. **Revista do Tribunal Superior do Trabalho**, São Paulo, v. 86, n. 3, p. 163-179, jul./set. 2020.

CRIPTOATIVOS E PREVENÇÃO À LAVAGEM DE DINHEIRO: GOVERNANÇA MULTISETORIAL COMO INSTRUMENTO DE COMPATIBILIZAÇÃO DE NORMAS

CRYPTOCURRENCIES AND ANTI-MONEY LAUNDERING: MULTISECTORAL GOVERNANCE AS AN INSTRUMENT FOR MAKING STANDARDS COMPATIBLE

Emiliane Alencastro[1]

RESUMO

Embora tenham sido criados com o intuito de trazer benefícios ao sistema financeiro, os criptoativos trouxeram consigo um incremento de risco à lavagem de dinheiro. Este artigo objetiva demonstrar a governança multisetorial como instrumento de compatibilização de normas aplicáveis à construção de uma Política AML nas prestadoras de serviço de ativos virtuais. Justifica-se, especialmente, pelo aumento constante do uso de criptoativos e do nível de sofisticação de práticas delituosas envolvendo esses ativos, assim como pela obrigatoriedade do desenvolvimento de uma Política AML em conformidade com o conjunto normativo aplicável e aclimatada ao ecossistema dos criptoativos. Como metodologia, foi adotada a pesquisa bibliográfica e documental a partir do método hipotético-dedutivo. Conclui que a adoção de ferramentas de governança multisetorial é uma boa estratégia para compatibilizar o conjunto normativo antilavagem de dinheiro, por ser uma forma de alinhar medidas antes e durante o processo regulatório e por maximizar a aceitabilidade da regulação e, por conseguinte, sua eficácia.

Palavras-chave: Criptoativos; Governança multisetorial; Lavagem de dinheiro; Política AML.

ABSTRACT

Although the cryptocurrencies were created with the aim of bringing benefits to the financial system, they brought with them an increased risk of money laundering. This article aims to demonstrate multisectoral governance as an instrument for the compatibility of norms applicable to the construction of an AML Policy in virtual asset service providers. It is especially justified by the constant increase in the use of cryptocurrencies and the level of sophistication of criminal practices involving these

[1] Mestre em Direito (PPGD-UFPE). Professora de Direito Digital (Sopece). Membro do Grupo de Estudos "Finanças Digitais" (Cin-UFPE). Advogada. Lattes: http://lattes.cnpq.br/2366056850409194.

assets, as well as the mandatory development of an AML Policy in compliance with the applicable set of regulations and adapted to the crypto ecosystem. The adopted methodology was bibliographical and documentary research based on the hypothetical-deductive method. It concludes that the adoption of multisectoral governance tools is a good strategy to make the anti-money laundering set of rules compatible, as it is a way of aligning measures before and during the regulatory process and for maximizing the acceptability of regulation and, therefore, its effectiveness.

Keywords: Cryptoassets; Multisectoral governance; Money laundry; AML Policy.

1 INTRODUÇÃO

Os criptoativos são uma espécie de moeda digital que utiliza a criptografia para garantir a segurança e a validade das transações.[2-3] As operações são realizadas por meio da tecnologia *blockchain*, uma rede distribuída, caracterizada por registrar informações de forma segura e transparente (GRUPENMACHER, 2019).

De maneira simplificada, essa tecnologia consubstancia um banco de dados descentralizado em que cada dado é verificado por uma rede de computadores antes do registro. A segurança fica por conta da codificação de cada informação depositada, através de pseudônimos, com duas chaves, uma pública e outra privada (senha). Essas duas chaves autorizam que um texto seja transformado em *hash* e este seja compartilhado com todos os "nós" da rede, garantindo a segurança das operações. Esse modo operacional permite que a tecnologia *blockchain* seja caracterizada pelos seguintes atributos técnicos: descentralização, imutabilidade, autonomização, anonimização e globalização.

[2] Neste trabalho, a taxinomia do termo "criptoativos" não é enfrentada, razão pela qual ativos virtuais, criptomoedas, ativos digitais e demais termos análogos são utilizados como palavras sinônimas.

[3] Adotado o conceito legal disposto no art. 3º, *caput*, da Lei nº 14.478/22, tratam-se de representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para a realização de pagamentos ou com propósito de investimento". O parágrafo do referido dispositivo exclui do conceito a moeda nacional e moedas estrangeiras; a moeda eletrônica, os instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade e as representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros.

Transacionados através do *blockchain*, os criptoativos foram criados com o intuito de democratizar o acesso ao sistema financeiro, de maneira pretensamente mais segura que por via dos ativos tradicionais, mais transparente, com alto grau de previsibilidade e de privacidade, tudo isso sem depender de uma organização centralizadora, como uma instituição financeira nacional.

Embora tenham sido criados com o intuito de trazer benefícios ao sistema financeiro, os criptoativos trouxeram consigo um incremento de risco à lavagem de dinheiro. [4]Algumas características que qualificam a moeda também são fatores que dificultam a prevenção e o combate à lavagem de dinheiro, em espécie: a dispensabilidade da intermediação, devido à descentralização característica das operações em *blockchain*; o caráter transnacional dessas moedas, que permite que particulares ou corretoras operem a troca das moedas, inclusive por moeda nacional; e a possibilidade de anonimidade para gerar chaves e acessar transações, que, embora rastreáveis, não garantem a identificação do titular no endereço indicado.[5]

Esses fatores (dispensabilidade da intermediação, caráter transnacional e possibilidade de anonimidade) trazem novas dificuldades para a elaboração de políticas antilavagem de dinheiro. Em paralelo, o número de *blockchains* também tem se multiplicado, assim como as possibilidades de atividades criminosas com um nível de sofisticação incrementado[6]. Esse cenário, à nível regulamentar, aponta para a necessidade de desestímulo à realização de operações sem intermediários, reduzindo o custo de agência, e de regulação das prestadoras de serviço em nível nacional e transfronteiriço.[7]

---

[4] O relatório da Chainalysis, publicado em fevereiro de 2023, concluiu que, apesar da retração do mercado, o volume de transações ilícitas aumentou pelo segundo ano consecutivo, atingindo um recorde histórico de U$ 20,6 bilhões. Disponível em: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf. Acesso em 14 mar.2023.

[5] Esses fatores adotados foram identificados como catalisadores para a lavagem de dinheiro de moedas virtuais em obra pioneira no estudo da lavagem de dinheiro através de ativos virtuais. (Grzywotz, 2019.

[6] As práticas criminosas mais comuns, envolvendo criptomoedas, são mercado *darknet*, compras fraudulentas, administrador cibercriminoso, financiamento ao terrorismo, material de abuso infantil, *ransomware*, fundos roubados e fraude. Disponível em: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf. Acesso em 11 mar. 2023.

[7] O GAFI observa que a estratégia regulatória varia em cada jurisdição. Uns proíbem atividades com criptomoedas, outros optam por regular os intermediários, outros por estabelecer o dever de reportar transações suspeitas. *In*: Financial Action Task Force, FATF Report to the G20 Finance Ministers and Central Bank Governors. Disponível em: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-

Mas, enquanto a regulação não atinge a devida maturidade e em razão do alto índice de disrupção que sempre acompanhará esse universo, as prestadoras de serviços de ativos virtuais têm um importante papel a desempenhar. Devem desenvolver a capacidade de compatibilizar o conjunto normativo existente, inclusive para contribuir para a sustentabilidade dessa nova forma de construir o sistema financeiro, antever as exigências que lhes serão feitas e evitar a aplicação de sanções. Também devem ser capazes de criar mecanismos estratégicos para impedir que a lavagem de dinheiro seja operacionalizada através de sua empresa. Acredita-se que o desenvolvimento de mecanismos de governança multisetorial, estabelecendo a comunicação entre as empresas do setor, com os usuários e com os agentes reguladores, seja uma excelente ferramenta para a compatibilização do arcabouço normativo antilavagem de dinheiro.

Este artigo objetiva demonstrar a comunicação multisetorial como instrumento de compatibilização de normas aplicáveis à construção de uma Política AML nas prestadoras de serviço de ativos virtuais. Os objetivos específicos são compostos pela compreensão do nível regulamentar dos criptoativos e do dever de prevenção à lavagem de dinheiro; pela identificação do conjunto normativo aplicável à construção de um programa e, por conseguinte, de uma Política AML; pela indicação dos fundamentos de uma Política AML; e pela análise dos fatores que compõem a governança multisetorial e que a faz uma boa ferramenta à compatibilização de normas.

A pesquisa se justifica (a) pela disrupção que envolve os ativos virtuais e consecutivamente o modelo de gestão das prestadoras de serviço de ativos virtuais; (b) pelo aumento constante do uso de criptoativos e do nível de sofisticação de práticas delituosas envolvendo esses ativos; (c) pela novidade da regulação dos criptoativos no Brasil, rompendo com a existência de negócios que têm operado à margem do Estado; (d) pela utilidade do comportamento cooperativo diante do disruptivo; e (e) pela

Report-G20-FM-CBG-July-2018.pdf. Acesso em 11 mar. 2023. O GAFI recomenda reduzir o campo a ser controlado, focando as ações regulatórias nas prestadoras de serviço de ativos virtuais, desencorajando a comercialização das moedas pelos próprios usuários. No entanto, essa saída nos faz questionar quanto ela esvazia a descentralização, característica das operações em *blockchain*, que é ponto fulcral de um sistema *DeFi*. Mesma questão se faz acerca da redução do grau de anonimidade.

obrigatoriedade do desenvolvimento de uma Política AML em conformidade com o conjunto normativo aplicável e aclimatada ao ecossistema dos criptoativos.

Para que seja alcançado o mencionado objetivo, a metodologia adotada será a pesquisa teórica bibliográfica e documental, mediante a leitura e interpretação do conjunto normativo aplicável, de artigos científicos e das boas práticas indicadas pelo mercado, a partir do método hipotético-dedutivo.

No primeiro capítulo, será analisado o nível regulamentar dos criptoativos no Brasil e o dever de prevenção à lavagem de dinheiro. No segundo capítulo, far-se-á uma análise do conjunto normativo aplicável à prevenção e ao combate da lavagem de dinheiro no ecossistema dos criptoativos. No terceiro capítulo, serão apresentados os fundamentos de uma Política AML, indicando a metodologia da abordagem baseada no risco e os deveres dos agentes responsáveis. No quarto capítulo, serão demonstradas a importância da governança multisetorial e algumas sugestões de como implementá-la.

2 CRIPTOATIVOS: REGULAÇÃO E DEVER DE PREVENÇÃO À LAVAGEM DE DINHEIRO

A regulação é um importante passo para promover maior segurança jurídica para os investidores e consumidores, para os prestadores de serviço que levam a sério o que fazem e, por conseguinte, para a eficiência e competitividade do mercado.

Mas o fato é que é extremamente complexo regular um ecossistema financeiro baseado em *blockchain*. Devido as características técnicas dessa tecnologia (descentralização, imutabilidade, autonomização, anonimização e globalização), as abordagens tradicionais não são suficientes para atingir os objetivos regulatórios.

Por se tratar de uma rede global e descentralizada, para que seja alcançado um nível de proteção satisfatório, é necessário desenvolver uma regulação transfronteiriça e estabelecer instrumentos de cooperação internacional.

Outrossim, a complexidade é tanta que, mesmo que isso seja alcançado nos próximos anos, outras questões precisam ser pensadas e enfrentadas. Tais como: (a) os limites jurisdicionais estabelecidos podem esvaziar a potência de sanções internacionais;

(b) normalmente, as criptomoedas estão inseridas em infraestruturas espalhadas por vários países, o que dificulta a identificação de agentes responsáveis pela supervisão, sendo possível, inclusive, que as atividades sejam registradas em locais cujo regime antilavagem de dinheiro é deficitário; (c) quando as transações são realizadas sem intermediário, verificar a existência de Política AML é quase impossível; (d) a cada dia que passa existem mais tecnologias sofisticadas de anonimização e para dificultar o rastreamento de atividades; (e) devido à forma como o *blockchain* funciona, o agente regulador não tem como suspender, cancelar ou reverter qualquer transação. A modificação de registros transacionais dependerá da colaboração dos agentes responsáveis pela engenharia. [8]

Diante do crescente aumento, ano a ano, do uso dos criptoativos, é inegável que estamos inseridos numa realidade que não dá para ignorar e que não vai deixar de existir. Esses fatores demonstram o quanto pôr a matéria para discussão é urgente e o quanto os países precisam se adiantar para regular, ao menos a nível nacional, enquanto a regulação à nível global não toma a maturidade necessária.

No Brasil, a regulação dos criptoativos passou a ser objeto de preocupação, de maneira tímida, em 2018.[9] Apenas em 2022 foi dado o passo mais firme na construção de um regime regulatório dos criptoativos.[10] Nesse ano, foi sancionada a Lei nº 14.478 que traz diretrizes sobre a prestação de serviços de ativos virtuais. Embora tenha sido apelidada como "a lei dos criptoativos" ou como "marco legal dos criptoativos", a lei diz mais sobre os prestadores de serviço porque o Brasil adotou essa estratégia regulatória (regular os intermediários).[11]

---

[8] Análise semelhante pode ser encontrada no artigo "Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem". *In*: Stanford Journal of Blockchain Law & Policy, vol. 3, n. 2, 2020. Disponível em: https://stanford-jblp.pubpub.org/pub/multistakeholder-comm-governance2/release/1 Acesso em: 05 jan. 2023.

[9] Em 2018, a Comissão de Valores Mobiliários (CVM) começou a emitir ofícios sobre os criptoativos. Embora naquele ano negasse a qualificação de ativo financeiro, a autarquia já indicava os riscos envolvidos e a necessidade de regulação. Nos anos seguintes produziu outros ofícios e pareceres que, embora tivessem caráter meramente orientativo e focassem em definir os contornos de sua competência, acabavam trazendo alguns elementos relevantes para as prestadoras de serviços de ativos virtuais já ativas.

[10] Sobre o termo "criptoativos", confira a nota de rodapé nº 2.

[11] Ver nota de rodapé nº 7.

Ser um agente de profusão de um sistema bancário sem intermediários centralizadores, feito para democratizar os serviços financeiros e promover maior segurança, exige uma atitude coerente com esse propósito. Reconhecer a necessidade de agir de maneira lídima é importante para garantir a sustentabilidade dessa nova forma de desenvolver o sistema financeiro e, em especial, do próprio empreendimento.

As "prestadoras de serviço de ativos virtuais" são as pessoas jurídicas que executam, em nome de terceiros, pelo menos um dos serviços de ativos virtuais[12]. Para "serviços de ativos virtuais", a legislação brasileira adotou um conceito amplo, trazendo alguns exemplos de atividade, tais como a troca entre ativos virtuais e moeda nacional ou moeda estrangeira ou até entre um ou mais ativos virtuais, *v.g.*[13].

É possível visualizar ao menos três tipos de prestadoras de serviço de ativos virtuais. As *exchanges* centralizadas, que realizam transações entre moedas nacionais e criptoativos e entre criptoativos, havendo grande liquidez; as descentralizadas (DEX), que realizam transações entre ativos virtuais diversos, havendo uma grande variedade de *tokens* negociados; e os provedores de serviços de mixagem, que criam camadas que garantem maior privacidade para os envolvidos na transação.

Esses agentes já são equiparados às instituições financeiras e isso faz com que tenham uma série de exigências a cumprir. A Lei nº 14.478/2022 estabelece a necessidade de autorização prévia, pelo órgão competente, para ser intermediário de transações. Também dispõe, como diretrizes fundamentais a serem seguidas pelas prestadoras de serviço, a existência de boas práticas de governança, transparência nas operações e abordagem baseada em riscos e, em especial, a prevenção à lavagem de dinheiro, em alinhamento com os padrões internacionais.

A prevenção à lavagem de dinheiro, dever do Estado e das instituições financeiras, deve ser prioridade em qualquer sistema financeiro, especialmente porque se destina à

[12] Adoção do conceito legal previsto no art. 5º, *caput*, da Lei nº 14.478/2022.

[13] O serviço de ativos virtuais, por sua vez, é exemplificado como troca entre ativos virtuais e moeda nacional ou moeda estrangeira; troca entre um ou mais ativos virtuais; transferência de ativos virtuais; custódia ou administração de ativos virtuais ou de instrumentos que possibilitem controle sobre ativos virtuais; e como participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais (incisos do art. 5º da Lei nº 14.778/2022).

condução do desenvolvimento econômico equilibrado e, nesse objeto, deve servir também aos interesses da coletividade.

A lavagem de dinheiro é conduta que pode ser compreendida como um comportamento composto por uma série de atividades comerciais e financeiras que objetiva a incorporação de recursos, bens ou valores, de origem ilícita, dentro do sistema financeiro, de maneira permanente ou provisória.[14] Nesse comportamento, é possível identificar três fases: colocação (*placement*), ocultação (*layering*) e integração (*integration*), conforme Bottino e Telles (2018, p. 131-176).

Na primeira fase, os valores ilegítimos são introduzidos no sistema financeiro. No âmbito dos criptoativos, essa fase pode ser visualizada mediante a compra de ativos virtuais com dinheiro que é produto de crime. A fase de colocação (segunda) se dá pela atuação para dificultar o rastreamento contábil de recursos ilícitos. É o que acontece através da geração de diversas chaves públicas, operando a mudança de endereço sem que o usuário perca o controle. Nesse cenário, será possível identificar as transações realizadas, mas não necessariamente os usuários. A terceira fase (integração), em que se opera a incorporação dos valores ao sistema financeiro, pode ser realizada pela troca de moedas virtuais pelas moedas nacionais que, acaso operada em países menos rigorosos com a lavagem de dinheiro, raramente receberá a reprimenda devida.[15]

[14] A lavagem de dinheiro é conduta rechaçada nas instâncias civil, administrativa e penal, atraindo a possibilidade de que sejam aplicadas penalidades nas três instâncias, tema que poderá, inclusive, enfrentar o dilema da duplicidade de jurisdições competentes para processar e aplicar sanções. Devido à complexidade, a temática merece ser objeto de estudo de pesquisa específica.

[15] O GAFI/FATF (Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo), do qual o Brasil é signatário (observe a nota de rodapé nº 5), em sua atuação, (I) emite recomendações destinadas a prevenir e a reprimir os crimes mencionados, (II) promove "Avaliações Mútuas" para verificar a observância dessas recomendações e seu grau e efetividade. Nessas avaliações, (III) determina medidas que devem ser adotadas pelas jurisdições com deficiências relevantes, acompanhando esse processo e (IV) identifica novos riscos e metodologias de combate à lavagem de dinheiro e ao financiamento do terrorismo. Um dos objetivos principais do GAFI é a identificação contínua de jurisdições com deficiências significativas no controle da lavagem de dinheiro. Na última declaração, produzida em outubro de 2022, foram indicados os seguintes territórios como jurisdições de alto risco e com deficiências estratégicas: Albânia, Barbados, Burquina Faso, Camboja, Ilhas Cayman, República Democrática do Congo, Gibraltar, Haiti, Jamaica, Jordânia, Mali, Marrocos, Moçambique, Nicarágua, República Democrática da Coreia, Irã, Mianmar, Paquistão, Panamá, Filipinas, Senegal, Síria, Tanzânia, Turquia, Uganda, Emirados Árabes Unidos e Iémen. Disponível em: https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-

Conforme demonstrado, as próprias características técnicas dos criptoativos fazem com que a necessidade de desenvolver uma Política Antilavagem de Dinheiro (AML) seja tão intensa quanto complexa. A construção dessa Política perpassa a elaboração estratégica de um programa que deve considerar o conjunto normativo aplicável, aclimatando-o às condições específicas do ecossistema dos criptoativos e às atividades características do agente responsável pela prevenção. Passemos à identificação do conjunto normativo aplicável.

3 ANTILAVAGEM DE DINHEIRO NO ECOSSISTEMA DOS CRIPTOATIVOS

A complexidade do desenvolvimento de uma regulação global (demonstrada no capítulo anterior) evidencia que a prática de crimes financeiros num ecossistema de natureza global tem o poder de diluir a eficácia de regulamentações já existentes. É também nessa conjuntura que é importante desenvolver o compromisso constante de conhecer as normas aplicáveis à prevenção de lavagem de dinheiro, compatibilizá-las e aclimatá-las.

A antilavagem de dinheiro (AML - *Anti-Money Laundering*) é um conjunto normativo que objetiva prevenir e combater a lavagem de dinheiro. Conhecer esse conjunto normativo é o primeiro passo para a construção de uma Política AML, servindo de base para a elaboração do programa.

Atualmente, há poucas normas que se aplicam de maneira coercitiva à prevenção da lavagem de dinheiro. Mas há alguns diplomas e espécies legislativas que, embora possuam natureza meramente orientativa, podem ser adotados como meios de promover o melhor cenário de adequação.

No Brasil, é possível organizar essas fontes da seguinte maneira: (a) normas que são coercitivas e gerais, como é o caso da Lei nº 9.613/98, que estabelece obrigações imperiosas e que se aplicam a todos os agentes responsáveis; (b) normas internacionais, vinculativas apenas para os territórios signatários e com baixo nível sancionatório, como

2022.html/; https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2022.html/. Acesso em 06 de mar de 2023.

é o caso das Recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF), da Diretiva Antilavagem de Dinheiro da União Europeia e da Convenção de Palermo (ONU); (c) normas administrativas e especiais, vinculativas apenas aos agentes que estão vinculados ao órgão redator, como as circulares do Banco Central (Bacen) e as resoluções da Comissão de Valores Mobiliários (CVM); e (d) normas de setor ou de classe, que embora vinculem apenas seus agentes, pelo *know-how* e detalhamento que fornecem, são úteis para o desenvolvimento de um programa AML (e, por conseguinte, de uma Política), como a circular da Superintendência de Seguros Privados (SUSEP) e a resolução do Conselho Federal de Contabilidade (CFC). Passa-se à indicação mais detalhada dos três primeiros grupos mencionados.

A Lei nº 9.613/1998 dispõe o crime de lavagem de dinheiro, estabelecendo estratégias de prevenção e criando o COAF (Conselho de Controle de Atividades Financeiras). A referida lei já foi alterada diversas vezes, inclusive pela Lei nº 14.478/2022 (Lei dos Criptomoedas), que incluiu a prestadoras de serviço de ativos virtuais como agentes responsáveis pelo combate, prevenção e comunicação dos crimes de lavagem de dinheiro (inciso XIX do art. 9º, com alteração produzida pela Lei nº 14.478/2022).

As Recomendações produzidas pelo GAFI apresentam medidas que auxiliam os países na contenção da lavagem de dinheiro e do financiamento do terrorismo.[16] Essas recomendações podem ser organizadas em três grupos: normativo, preventivo e repressivo. As recomendações do grupo normativo se destinam ao Estado, auxiliando-os na elaboração de leis contra a lavagem de dinheiro e o financiamento do terrorismo. Nas recomendações preventivas, que se destinam a todos os agentes responsáveis pelo

[16] O GAFI/FATF (Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo) é uma organização intergovernamental criada em 1989 que promove importantes medidas de prevenção e combate à lavagem de dinheiro. O Brasil é signatário desde 2000. São membros do GAFI 35 países (África do Sul, Alemanha, Argentina, Austrália, Áustria, Bélgica, Brasil, Canadá, China, Dinamarca, Espanha, EUA, Finlândia, França, Grécia, Hong Kong, Índia, Irlanda, Islândia, Itália, Japão, Luxemburgo, Malásia, México, Noruega, Nova Zelândia, Países Baixos, Portugal, Reino Unido, República da Coreia, Rússia, Singapura, Suécia, Suíça e Turquia) e duas organizações regionais (Comissão Europeia e Conselho de Cooperação do Golfo).

combate, prevenção e comunicação do ilícito, inclusive empresas privadas, a transparência é disposta como valor basilar, trazendo o *Know your Customer* e as políticas de manutenção de registros como principais ações. Nas recomendações repressivas, destinadas aos Estados, estão as indicações de como um país pode se munir para identificar operações suspeitas, realizar investigações, processar ações penais e executar condenações.

A União Europeia, também em consideração às recomendações do GAFI, tem elaborado diversas normas para combater a lavagem de dinheiro e o financiamento do terrorismo. Uma delas é a 5ª Diretriz de Combate à Lavagem de Dinheiro, que estabelece, dentre outras medidas, o incremento da transparência a partir de registros públicos, o limite ao anonimato relacionado às moedas virtuais e a melhora da cooperação para aumentar a qualidade da informação entre supervisores da Política. Recentemente, em fevereiro de 2022, produziu um manual para quem forma profissionais do Direito que atuarão nessa área na União Europeia. [17]

A Convenção de Palermo, cujo Brasil é signatário (através do Decreto nº 5.015/2004), foi criada pela Organização das Nações Unidas (ONU) para harmonizar normas jurídicas sobre o crime organizado transnacional. O documento estabelece ferramentas para que os Estados evitem e combatam o crime organizado transnacional, trazendo instrumentos de cooperação internacional.

A Circular nº 3.461/2009 do Banco Central consolida as regras sobre os procedimentos a serem adotados na prevenção e combate às atividades relacionadas com os crimes previstos na Lei nº 9.613/1998. A Resolução nº 50/2021 da Comissão de Valores Mobiliários, por sua vez, dispõe sobre a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa no âmbito do mercado de valores mobiliários.

Essas espécies legislativas trazem informações que podem (em alguns casos, devem) ser aplicadas no universo dos criptoativos. No entanto, algumas das exigências

[17] Disponível em https://finance.ec.europa.eu/publications/training-lawyers-anti-money-laundering-aml-and-counter-terrorist-financing-ctf-rules-eu-level_en. Acesso em 18 de mar. 2023.

feitas para as instituições financeiras tradicionais são mais difíceis ou inviáveis de serem aplicadas, demandando um trabalho de aclimatação das disposições à espécie. Nesse intuito, o GAFI produziu uma Orientação voltada para os criptoativos que merece especial atenção.

3.1 Orientação do GAFI/FATF para os criptoativos

Em 2021, o Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF) atualizou sua Orientação sobre ativos virtuais e provedores de serviços de ativos virtuais. [18] O órgão estabelece padrões que devem ser seguidos pelos países signatários.

Nessa toada, indica que os países devem (a) avaliar e mitigar os riscos associados a provedores e atividades financeiras de ativos virtuais e (b) licenciar ou registrar as prestadoras de serviço, submetendo-as à supervisão ou ao monitoramento das autoridades nacionais competentes. À evidência, ao promulgar a Lei dos Criptoativos (Lei nº 14.478/2022) e se posicionar através de diversos órgãos estatais, o Brasil demonstra que avança no processo de cumprimento da Orientação.

Com a atualização feita em 2021, dentre outras medidas, o GAFI traz orientações adicionais sobre os riscos e as ferramentas disponíveis para os países lidarem com a lavagem de dinheiro e o financiamento ao terrorismo, bem como sobre o licenciamento e registro das prestadoras de serviço.

Sobre as atividades para lidar com os riscos de lavagem de dinheiro no âmbito dos serviços de ativos virtuais, a Orientação indica que a jurisdição tem o poder de proibir ou de limitar atividades com ativos virtuais, com base na sua avaliação de risco e no contexto regulatório nacional, bem como para apoiar outros objetivos políticos, como, por exemplo, a proteção ao consumidor e investidor, segurança e solidez da política monetária. O documento destaca que isso pode incluir uma proibição geral ou limitação

[18] A primeira edição da Orientação é de 2019. É possível fazer *download* da Orientação atualizada aqui: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html Acesso em 06 de mar. 2023.

de atividade ou proibições ou limitações específicas sobre produtos ou serviços que possuam um nível inaceitável de risco.

Sobre o dever de licenciar/registrar, o GAFI trouxe diretrizes que conferem certa margem de flexibilidade para os países. Os países podem achar mais fácil usar um sistema de licenciamento/registro já existente no sistema financeiro, na medida em que seus regimes sejam funcionais e apropriados para serviços de ativos virtuais. No entanto, o GAFI encoraja que novos regimes sejam criados, colocando foco em aspectos que até então não são prioridade, como a capacidade tecnológica na análise AML e os mecanismos que mitigam riscos no setor que diferem do que é feito nos serviços financeiros tradicionais. Oportunamente, indica a importância de que sejam criadas leis e regulamentos sobre ativos virtuais e seus serviços respectivos e que seja estabelecida a natureza, requisitos e tipos de regime com certo vigor.

O GAFI ainda sugeriu algumas ferramentas para que os países consigam identificar prestadores de serviço não licenciados ou não registrados, tais como: (a) *blockchain* ou ferramentas de análise de contabilidade distribuída, bem como outras ferramentas investigativas; (b) *web-scraping* e informações de código aberto para identificar qualquer publicidade, comunicações promocionais ou programas de afiliação ou outras possíveis solicitações de negócios por uma entidade não registrada ou não licenciada; (c) informações do público em geral, entidades obrigadas e círculos da indústria (inclusive estabelecendo canais para receber *feedback* do público) sobre a presença de certas empresas que podem não ser licenciadas ou registradas; (d) Unidades de Inteligência Financeira ou outras instituições relatoras; (e) informações não disponíveis publicamente, como o caso em que a entidade solicitou anteriormente uma licença ou registro ou teve sua licença ou registro retirado; e (f) aplicação da lei e relatórios de inteligência, incluindo informações de cooperação internacional.

Como é possível visualizar, o GAFI sugere que os países adotem medidas severas de controle de registro e de licenciamento.

Ainda é importante trazer como destaque a sugestão de criar indicadores de alerta acerca de possível lavagem de dinheiro envolvendo ativos virtuais. O GAFI recomenda os seguintes indicadores: (a) recursos tecnológicos que aumentam o anonimato, como

mixers; (b) riscos geográficos, considerando a possibilidade de que os usuários explorem países com medidas nacionais fracas ou inexistente; (c) padrões de transação, avaliando a inclusão de transações que são estruturadas para evitar relatar irregularidade ou para fazer parecer que são regulares; (d) tamanho da transação, analisando se o valor e a frequência de transação não têm sentidos lógicos de explicação; (e) perfis de remetente ou destinatário; e (f) fonte de fundos ou riqueza.[19]

Para os órgãos reguladores brasileiros e as prestadoras de serviço de ativos virtuais, conhecer a Orientação do GAFI é muito importante para antever a linha de exigências legais que o Brasil vai desenvolver e as possíveis ferramentas de controle que serão utilizadas. Passemos, então, à análise dos fundamentos de uma Política AML.

4 FUNDAMENTOS DE UMA POLÍTICA AML NO ÂMBITO DOS CRIPTOATIVOS

Uma Política AML (*Anti-Money Laundering*) é o resultado do desenho e da implementação de um programa de administração de riscos de lavagem de dinheiro. Isso quer dizer que essa política só existe depois que um programa for elaborado, executado e validado. É caracterizada por (a) identificar os riscos envolvidos e (b) garantir que as atividades financeiras estejam alinhadas com o conjunto normativo AML aplicável.

Essa garantia deve começar com a definição de um agente interno responsável pelo controle. Em seguida, deve ser feita uma análise interna de risco (em materialização da metodologia da abordagem baseada no risco, descrita no subitem seguinte) que servirá de base à elaboração do plano de ação.

O plano de ação deverá considerar, de maneira resumida: o mapeamento de atividades avaliadas como suspeitas, a classificação de clientes conforme o risco que oferecem, identificação dos clientes (*Know Your Costumer*), a atualização dos dados cadastrais, a otimização da validação e gerenciamento integrado das informações dos

[19] Todas as informações dispostas nesse item foram retiradas do documento indicado na nota de rodapé anterior (nº 18).

usuários, o controle do destinatário final, monitoramento, controle e comunicação ao COAF/UIT, a manutenção de registro de operações por prazo certo, a divulgação do plano de ação e a disseminação da cultura AML na empresa, a verificação da efetividade, a identificação de *gaps* e revisão do programa, verificação do grau de maturidade e, por fim, a divulgação externa do programa. Essas atividades devem ser feitas de maneira cíclica para garantir a oxigenação do programa.

Todo o plano de ação, que representa o programa AML, deve ser feito com base na análise de riscos (metodologia) e no intuito de que sejam cumpridos os deveres estabelecidos às prestadoras de serviço de ativos virtuais, considerando o conjunto normativo que compõe a antilavagem de dinheiro e aclimatando-o à realidade da prestadora de serviço.

4.1 Abordagem baseada no risco

A abordagem baseada no risco é uma metodologia utilizada para identificar e analisar os possíveis riscos associados a uma determinada atividade. Nessa abordagem que tem natureza preventiva, deve ser considerada a probabilidade de ocorrência do risco e o nível do impacto que ele pode ter. O objetivo é minimizar ou oportunizar o gerenciamento de riscos associados à atividade, favorecendo a segurança e a qualidade do produto ou serviço envolvido. Para tanto, é necessário fazer uma análise completa das possíveis ameaças e consequências no desempenho da atividade e um planejamento minucioso para lidar com essas ameaças.

O GAFI adota essa metodologia para suas avaliações, o que inclui conhecer: (a) a natureza e a extensão da lavagem de dinheiro e do financiamento do terrorismo; (b) as circunstâncias que afetam a materialidade das diferentes recomendações (por exemplo, a composição de sua economia e de seu setor financeiro); (c) elementos estruturais que favorecem o sistema antilavagem de dinheiro; (d) os fatores contextuais que possam influenciar a forma de implementação das medidas antilavagem de dinheiro. Destaque-se que o GAFI aplica essa abordagem na avaliação de países.

Levar essa metodologia para empresas, o que é disposto como diretriz fundamental a ser seguida pelas prestadoras de serviço de ativos virtuais na Lei nº 14.478/22, significa conhecer os fatores de risco inerentes ao objeto social que exploram e às peculiaridades do segmento em que atuam, sendo capaz de identificar os perfis de risco de seus clientes, dos beneficiários finais, da própria empresa e seus colaboradores, das negociações e operações que intermedeia, dos produtos/serviços que oferecem e da tecnologia que utilizam. Tudo isso considerando seu porte, localização e complexidade das soluções.

4.2 Deveres dos agentes responsáveis

A legislação brasileira adotou um conceito abrangente para a definição dos agentes responsáveis, tendo indicado que as instituições financeiras, para além de outros agentes, [20] são responsáveis pela prevenção, combate e comunicação às autoridades do ilícito de lavagem de dinheiro, conceito que inclui as prestadoras de serviço de ativos virtuais. [21]

Compondo as responsabilidades, é possível apontar vários deveres que devem ser cumpridos. Da interpretação da legislação, por sua vez, é possível identificar ao menos cinco deveres com precisão: (a) identificação dos clientes; (b) identificação do destinatário final; (d) manutenção de registros; (d) adoção de políticas, procedimentos e

[20] É importante destacar que não só as instituições financeiras são responsáveis pela prevenção do crime referido. A legislação brasileira estabelece um conceito amplo de agentes responsáveis pelo combate, prevenção e comunicação do crime de lavagem de dinheiro. Essa atitude traz como consequência a possibilidade de responsabilização de muitos agentes envolvidos de alguma maneira na cadeia de execução da lavagem de dinheiro, seja por ação, seja por omissão (art. 9º da Lei nº 9.613/1998). Nesse sentido, foi estabelecido que os agentes responsáveis podem ser pessoas físicas ou jurídicas, que atuem em diversos setores empresarias, prestando, mesmo que eventualmente, serviços de assessoria, consultoria, contadoria, auditoria, aconselhamento ou assistência, de qualquer natureza, em diversas operações. Esses agentes têm, em caráter permanente ou eventual, como atividade principal ou acessória, cumulativa ou não, atividades como a captação, intermediação e aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira; a compra e venda de moeda estrangeira ou ouro como ativo financeiro ou instrumento cambial; a custódia, emissão, distribuição, liquidação, negociação, intermediação ou administração de títulos ou valores mobiliários (art. 9º da Lei nº 9.613/1998).

[21] A Lei de Criptomoedas alterou a Lei nº 9.613/98 para indicar expressamente que as prestadoras de serviços de ativos virtuais também são enquadradas como agentes responsáveis (inciso XIX do art. 9º, com alteração produzida pela Lei nº 14.478/2022).

controle internos compatíveis; e (e) comunicação de operações financeiras (art. 10 e 11 da Lei nº 9.613/1998).

A violação a um desses deveres pode ser enquadrada como comportamento conivente com o crime de lavagem de dinheiro, consubstanciando ato típico penal. De igual forma, no mínimo, configuram violações que atraem sanções administrativas que podem ser fulminantes para a empresa.

A (a) identificação dos clientes (*Know Your Customer - KYC*) é o dever de identificar seus clientes e manter seu cadastro atualizado (art. 10, Lei nº 9.613/1998). Esse cadastro deve ser conservado durante o período mínimo de cinco anos, contado a partir do encerramento da conta ou da conclusão da transação. Este prazo poderá ser ampliado pela autoridade competente (§4º do art. 10 do diploma mencionado).

A (b) identificação do beneficiário final é o dever de identificar quem é o destinatário final da operação, o que também pode ser feito através do registro de processos ou mediante o seu enquadramento na condição de pessoa politicamente exposta. Se não for possível identificar o beneficiário final, é imperioso avaliar a conveniência de realizar a operação ou de estabelecer/manter a relação negocial com o cliente.

A (c) manutenção de registros é o dever de manter o registro de toda e qualquer transação que envolva moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito, metais, ou qualquer ativo passível de ser convertido em dinheiro, que ultrapassar o limite fixado pela autoridade competente e nos termos de instruções por esta expedidas (art. 10, Lei nº 9.613/1998). A Lei nº 14.478/2022 incluiu expressamente às prestadoras de serviços de ativos virtuais no dever de manter registro de toda transação que envolve ativos virtuais, utilizando também como pressuposto a ultrapassagem do limite fixado pela autoridade competente.

Esse registro também deverá ser feito quando a pessoa física ou jurídica, inclusive seus entes ligados, houver realizado, em um mesmo mês-calendário, operações com uma mesma pessoa, conglomerado ou grupo que, em seu conjunto, ultrapassem o limite fixado pela autoridade competente. Assim como a identificação dos clientes, o registro deve ser conservado durante o período mínimo de cinco anos a partir do encerramento da conta ou

da conclusão da transação, prazo este que poderá ser ampliado pela autoridade competente.

A (d) adoção de políticas, procedimentos e controle internos compatíveis é o dever de adotar políticas, procedimentos e controles internos, compatíveis com seu porte e volume de operações, que lhes permitam atender aos deveres aqui dispostos, na forma disciplinada pelos órgãos competentes.

Nessa política, o agente responsável não pode deixar de cadastrar-se e de manter seu cadastro atualizado no órgão regulador ou fiscalizador e, na falta deste, no Conselho de Controle de Atividades Financeiras (COAF).

O dever de (e) comunicação de operações financeiras estabelece a obrigação de comunicar ao COAF/UIT,[22] abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de vinte e quatro horas, a proposta ou realização: (I) de todas as transações que ultrapassem o limite fixado pela autoridade competente, acompanhadas da identificação do cliente; (II) das operações que apresentarem indício do crime lavagem de dinheiro.

O Banco Central, em consolidação à referida regra, estabelece que devem ser comunicadas ao COAF (I) as operações realizadas ou serviços prestados cujo valor seja igual ou superior a R$10.000,00 (dez mil reais) e que, considerando as partes envolvidas, os valores, as formas de realização, os instrumentos utilizados ou a falta de fundamento econômico ou legal, possam configurar a existência de indícios dos crimes de lavagem

[22] O Conselho de Controle de Atividades Financeiras (COAF) foi criado no âmbito do Ministério da Fazenda/Economia, com a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas de lavagem de dinheiro. A partir de 2019, o COAF passou a ser denominado de Unidade de Inteligência Financeira (UIF), secção que recebe, examina e identifica operações suspeitas. É importante mencionar que Lei nº 9.618/1998 também foi alterada para indicar a responsabilidade do COAF no tratamento dos dados pessoais. A alteração indicou que o tratamento de dados será realizado de forma estritamente necessária para o atendimento às suas finalidades legais; garantirá a exatidão e a atualização dos dados, respeitadas as medidas adequadas para a eliminação ou a retificação de dados inexatos; não superará o período necessário para o atendimento às suas finalidades legais; considerará, na hipótese de compartilhamento, a sua realização por intermédio de comunicação formal, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios cometidos em seus procedimentos internos; garantirá níveis adequados de segurança, respeitadas as medidas técnicas e administrativas para impedir acessos, destruição, perda, alteração, comunicação, compartilhamento, transferência ou difusão não autorizadas ou ilícitas; será dotado de medidas especiais de segurança quando se tratar de dados sensíveis e protegidos por sigilo; e não será utilizado para fins discriminatórios, ilícitos ou abusivos.

de dinheiro; (II) as operações realizadas ou serviços prestados que, por sua habitualidade, valor ou forma, configurem artifício que objetive burlar os mecanismos de identificação, controle e registro; (III) as operações realizadas ou os serviços prestados, qualquer que seja o valor, a pessoas que reconhecidamente tenham perpetrado ou intentado perpetrar atos terroristas ou neles participado ou facilitado o seu cometimento, bem como a existência de recursos pertencentes ou por eles controlados direta ou indiretamente; (IV) os atos suspeitos de financiamento do terrorismo (Circular nº 3.461/2009).

Ainda, o Conselho Federal de Contabilidade recomenda aos contadores que algumas operações sejam comunicadas, independente de análise ou de qualquer outra consideração. As operações são a) aquisição de ativos e pagamentos a terceiros, em espécie, acima de R$ 50.000,00 (cinquenta mil reais), por operação; e/ou b) constituição de empresa e/ou aumento de capital social com integralização, em espécie, acima de R$ 100.000,00 (cem mil reais), em único mês-calendário. De maneira geral, as operações e propostas de operações que, após análise, possam configurar indícios da ocorrência de ilícitos devem ser comunicadas diretamente ao COAF, em seu sítio, contendo o detalhamento das operações realizadas, o relato do fato ou fenômeno suspeito e a qualificação dos envolvidos, destacando os que forem pessoas expostas politicamente.

Sobre o dever de comunicação ainda é importante trazer alguns destaques: (I) todas as transferências internacionais e os saques em espécie deverão ser previamente comunicados à instituição financeira, nos termos, limites, prazos e condições fixados pelo Banco Central do Brasil (art. 11-A da Lei nº 9.613/1998); (II) a não ocorrência dessas violações/suspeitas deverá ser comunicada ao órgão regulador ou fiscalizador da sua atividade ou, na sua falta, ao Coaf, na periodicidade, forma e condições por eles estabelecidas; (III) o dever de comunicação ainda significa atender às requisições formuladas pelo Coaf na periodicidade, forma e condições por ele estabelecidas, cabendo-lhe preservar o sigilo das informações prestadas.

Também há definições da forma como essa comunicação deve ser feita. Algumas operações devem ser comunicadas em até cinco dias úteis após o encerramento do mês calendário, outras na data da operação (Circular do Bacen). Os encaminhamentos das instituições financeiras e tributárias, em resposta às ordens judiciais de quebra ou

transferência de sigilo deverão ser, sempre que determinado, em meio informático, e apresentados em arquivos que possibilitem a migração de informações para os autos do processo sem redigitação (art. 17-C, Lei nº 9.613/1998).

Destaque-se, por fim, que verificado ou não o ilícito, as comunicações de boa-fé, feitas na forma determinada, não acarretarão responsabilidade civil ou administrativa.

5 GOVERNANÇA MULTISETORIAL E SUAS FERRAMENTAS

A governança multisetorial é uma estratégia de governança que abrange a participação de diversos agentes nos processos decisórios e na execução de políticas. Através desse modelo, é possível promover a cooperação entre diversos setores que possuem objetivos comuns (como a prevenção de lavagem de dinheiro). O objetivo é valorizar a diversidade de perspectivas e de experiências sobre o mesmo objeto, garantindo maior transparência e a participação ativa de todos esses agentes na tomada de decisão.

Por ser uma estratégia comumente adotada em iniciativas globais para desafios transfronteiriços, diante da ausência de clareza, em nível global, sobre o que fazer com as inúmeras particularidades que envolvem a aplicação do conjunto normativo antilavagem de dinheiro às prestadoras de serviço de ativos virtuais, parece coerente a adoção dessa saída. Inclusive porque o cenário é de muito espaço à criação e, nessa conjuntura, a ferramenta mais acertada é a cooperação, abrindo para a participação de todos os agentes do setor.

Na hipótese, há muitas ferramentas que podem ser adotadas, tais como: a criação de fóruns de diálogos, através de reuniões regulares entre membros de diferentes agentes do setor com o intuito de buscar soluções colaborativas, que permita inclusive o compartilhamento dos desafios de governança interna; parcerias público-privadas, estimulando a colaboração entre agentes públicos e privados e que traga vias de acesso facilitado aos agentes reguladores, desenvolva programas de conscientização da necessidade de respeitar as regras e que crie canais para educar a população sobre a temática; redes de colaboração, estimulando a criação de grupos informais que

compartilhem conhecimento e boas práticas, inclusive através do estímulo à pesquisa acadêmica; certificação de agentes que demonstrem compromisso com a governança AML, como forma de estimulara adesão às normas aplicáveis; conselhos multisetoriais, formando grupos para aconselhar e orientar políticas governamentais, apresentando cases, permitindo a discussão de problemas e elaboração de recomendações, trazendo referências úteis que auxiliem nos processos decisórios.

Diante da complexidade inerente às transações com criptoativos, a elaboração de leis, convenções internacionais e protocolos não é suficiente. A edição e a interpretação desses atos normativos devem se dar considerando também o mercado e a própria arquitetura do *blockchain.*

Encorajar o diálogo entre empresas prestadoras de serviço de ativos virtuais, até mesmo dos responsáveis pela engenharia, com os cidadãos e com os agentes de regulação é o melhor caminho, inclusive porque é uma forma alinhar medidas antes e durante o processo regulatório, estratégia para maximizar a aceitabilidade da regulação e, por conseguinte, sua eficácia.

6 CONSIDERAÇÕES FINAIS

Embora as prestadoras de serviço de ativos virtuais tenham o dever de prevenir a lavagem de dinheiro, o baixo nível regulamentar de sua atuação e a compatibilização das normas que compõem o conjunto normativo antilavagem de dinheiro demanda um comportamento proativo de todos os agentes do setor.

O desenvolvimento de uma Política AML numa prestadora de serviço de ativos virtuais exige a elaboração de um programa estratégico antilavagem de dinheiro, que deve considerar o conjunto normativo aplicável apresentado, aclimatando-os à competitividade de mercado, às condições específicas do ecossistema dos criptoativos e à realidade da empresa.

Para maximizar as chances de que as medidas de prevenção sejam acertadas, estimular um comportamento cooperativo, que ponha em colaboração as empresas prestadoras de serviço de ativos virtuais, inclusive com os agentes responsáveis pelo

desenvolvimento dos códigos que operacionalizam o *blockchain*, os agentes reguladores e os usuários, através de ferramentas de governança multisetorial, é uma medida que pode ter um impacto muito positivo na eficácia do processo regulatório e da interpretação dada ao conjunto normativo antilavagem de dinheiro.

REFERÊNCIAS

BOTTINO, Thiago; TELLES, Chrstiana Mariani da Silva. Lavagem de dinheiro, bitcoin e regulação. In: **Revista Brasileira de Ciências Criminais**, São Paulo: Ed. RT, vol. 148, ano 26, p. 131-176, outubro, 2018.

BRASIL. Congresso Nacional. **Decreto nº 5.015**, de 12 de março de 2004. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. Diário Oficial da União, 15 de março de 2004, Brasília DF.

BRASIL. **Lei nº 9.613**, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Diário Oficial da União, 4 de março de 1998, Brasília DF.

BRASIL. **Lei nº 14.478**, de 21 de dezembro de 2022. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições. Diário Oficial da União, 22 de dezembro de 2022, Brasília DF.

CHAINALYSIS. **The 2023 Crypto Crime Report**: Everything you need to know about cryptocurrency-based crime. February, 2023. Disponível em: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf. Acesso em: 14 mar.2023.

GAFI. FATF. Fatf **Recommendations: Guidance virtual asserts**, 2021. Disponível em: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html. Acesso em: 06 mar. 2023.

GAFI. FATF. **High risk and other monitored jurisdictions 2022**: Increased Monitoring, 2022. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2022.html/. Acesso em: 06 mar. 2023.

GAFI. FATF. **High risk and other monitored jurisdictions 2022**: Call for action, 2022. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2022.html/. Acesso em: 06 mar. 2023.

GAFI. FATF. **Reports G20**, 2018. Disponível em: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf. Acesso em: 11 mar. 2023.

GILCHRIST, Simon; MOJON, Benoit. Credit risk in the euro area. *In*: **The Economic Journal**, vol. 128, p. 118–158, 2018.

GRUPENMACHER, Giovana Treiger. **As plataformas de negociação de criptoativos: uma análise comparativa com as atividades das corretoras e da Bolsa sob a perspectiva da proteção do investidor e da prevenção à lavagem de dinheiro**, 2019. Dissertação (Mestrado em Direito e Desenvolvimento). Escola de Direito de São Paulo, Fundação Getúlio Vargas, São Paulo, 2019. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/27595. Acesso em: 16 fev. 2023.

GRZYWOTZ, Johanna. **Virtuelle Kryptowährungen und Geldwäsche**. Berlin: Duncker & Humblot, 2019.

TAKANASHI, Yuta; MATSUO, *Shin'ichiro; BURGER, Eric; SULLIVAN, Clare; MILLER, James; SATO, Hirotoshi*. Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem. In: **Stanford Journal of Blockchain Law & Policy**, vol. 3, n. 2, 2020. Disponível em: https://stanford-jblp.pubpub.org/pub/multistakeholder-comm-governance2/release/1. Acesso em: 05 jan. 2023.

UNIÃO EUROPEIA, Europe Comissions, Directorate-General for Financial Stability, Financial Services and Capital Markets Union. **Training for lawyers on anti-money laundering (AML) and counter terrorist financing (CTF) rules at EU level – Trainers' manual and users' manual**. Fev. 2022. Disponível em https://finance.ec.europa.eu/publications/training-lawyers-anti-money-laundering-aml-and-counter-terrorist-financing-ctf-rules-eu-level_en. Acesso em: 18 mar. 2023.

INTELIGÊNCIA ARTIFICIAL: DESAFIOS PARA REGULAÇÃO JURÍDICA

INTELIGÊNCIA ARTIFICIAL: DESAFIOS PARA REGULAÇÃO JURÍDICA

Eric Fiuza Bueno [1]

Marcelo Fonseca Santos [2]

RESUMO

O presente artigo aborda a regulação da Inteligência Artificial (IA) na sociedade contemporânea. A evolução da IA gera desafios complexos, como ética, viés, segurança e preconceitos, exigindo assim uma regulação segura e eficiente. Sua normatização pode mitigar e prevenir problemas prejudiciais, é possível realizar regulação através de métodos como autoregulação, regulação estatal e autoregulação regulada. A pesquisa se baseia em revisão bibliográfica, analisando fontes teóricas de revistas, livros e sites relevantes. O projeto de Lei 2.838/2023, visa a sua regulação no Brasil para combater seu uso prejudicial. A regulação é crucial para equilibrar inovação e proteção dos direitos, abordando desafios como preconceito, privacidade e segurança na sociedade contemporânea.

Palavras chaves: inteligência artificial; regulamentação; Direito; avanços tecnológicos.

ABSTRACT

This article discusses the regulation of Artificial Intelligence (AI) in contemporary society. The evolution of AI poses complex challenges such as ethics, bias, security, and prejudices, thus requiring a safe and efficient regulation. Its standardization can mitigate and prevent harmful issues and can be achieved through methods such as self-regulation, state regulation, and regulated self-regulation. The research is based on a bibliographic review, analyzing theoretical sources from relevant journals, books, and websites. The

[1] Bacharel pelas Faculdades Integradas Campos Salles (FICS). MBA em Compliance e Auditoria Faculdade BookPlay.

[2] Mestrando (Universidade Presbiteriana MACKENZIE), Especialista em Direito Empresarial pela FGV/SP, advogado de Direito Digital e Tecnologia, Vice Presidente da Associação Nacional das Advogadas e Advogados de Direito Digital ANADD, Diretor da International Association of Artificial Intelligence I2AI, Presidente da Comissão de Direito Digital da OAB/SP Lapa, Professor da LEGALE – Pós-Graduação de Lei Geral de Proteção de Dados, Professor de Direito Tributário das Faculdades Integradas Campos Salles, Membro das Comissões de Tecnologia e Inovação, de Compliance e de Privacidade, Proteção de Dados e Inteligência Artificial da OAB/SP, Membro de COMISSÃO DE DIREITO DIGITAL da OAB/SP - Butantã, Membro da Comissão de Compliance e Direito Digital da OAB/SP São Bernardo do Campo. Lattes: http://lattes.cnpq.br/9923895914317734.

Bill 2.838/2023 aims to regulate AI in Brazil to combat its harmful use. Regulation is crucial to balance innovation and the protection of rights, addressing challenges like prejudice, privacy, and security in contemporary society.

Keywords: artificial intelligence; regulation; law; technological advancements.

1 INTRODUÇÃO

Devido a sua ascensão a Inteligência Artificial tem transformado nossa sociedade de maneiras profundas e abrangentes. Com o crescimento exponencial das capacidades, surgem desafios complexos que demandam uma abordagem cuidadosa e uma regulamentação adequada. Este texto explora os conceitos fundamentais da regulação e sua aplicação na Inteligência Artificial, abordando a importância de compreender a regulação estatal, a autorregulação, a autorregulação regulada e os desafios inerentes a esses processos, para assim então entender qual seria a melhor forma para realizar uma relação adequada.

A Inteligência artificial, abrange campos como aprendizado de máquina, processamento de linguagem natural e visão computacional, traz consigo uma série de benefícios e oportunidades, mas também levanta questões éticas, de vieses e discriminação. A ausência de regulamentação poderia resultar em questões jurídicas significativas, como *deep fakes* enganosas, ataques cibernéticos sofisticados e a propagação de conteúdo discriminatório e inverídico. Nesse contexto, o estabelecimento de diretrizes legais torna-se crucial para mitigar esses riscos e garantir que a IA seja usada de maneira responsável e benéfica.

Além disso, o texto explora diferentes tipos de IA e seus respectivos impactos jurídicos, abordando áreas como viés, ética e discriminação. A IA, embora promissora, também apresenta desafios que requerem abordagens regulatórias inovadoras para garantir sua integração segura e benéfica na sociedade. Consequentemente, o desenvolvimento de regulamentações que equilibrem inovação, proteção de direitos e segurança torna-se uma prioridade, permitindo que a IA continue a contribuir para o progresso humano de maneira positiva.

2 REGULAÇÃO

Como ponto de partida, inicialmente devemos compreender o conceito de regulação. Ao buscarmos no dicionário, encontramos a seguinte definição: conjunto de disposições legais ou normativas que regulam um tema, uma entidade ou uma organização, ou seja, a palavra "regulação" tem como objetivo de demonstrar que algo está sendo regulamentado.

A regulação refere-se ao ato de criar, implementar e aplicar regras, diretrizes, normas ou leis para controlar ou influenciar a atividade de indivíduos, organizações, setores ou mercados. O objetivo principal da regulação é garantir o funcionamento eficiente, justo e seguro de sistemas complexos, como a economia, o meio ambiente, a saúde pública, as tecnologias emergentes e muitos outros aspectos da sociedade.

Como base principal deste estudo, devemos compreender algumas ferramentas que podem ser úteis e auxiliar na regulação da inteligência artificial, partindo do pressuposto de que boa parte das regulamentações dentro de uma sociedade deve ser feita pelo poder legislativo. Entretanto, ainda é possível identificar outras formas que podem ajudar na criação e regulação da inteligência artificial. Vamos a elas.

Contudo, a regulação da IA enfrenta diversos desafios. Primeiramente, a IA abrange uma ampla gama de aplicações, cada uma com suas próprias complexidades e implicações. Além disso, a velocidade de desenvolvimento da tecnologia muitas vezes supera a capacidade dos sistemas regulatórios de acompanhar. A falta de entendimento público sobre IA também pode dificultar a formulação de políticas eficazes.

2.1 Regulação Estatal

Regulação estatal refere-se a um conjunto de leis, regras, normas e políticas estabelecidas pelo governo de um país para gerenciar, supervisionar e influenciar diversas atividades econômicas, sociais e políticas dentro da sociedade. A principal finalidade da

regulação estatal é garantir que essas atividades sejam realizadas de maneira justa, segura, eficiente e em conformidade com os interesses públicos.

> A regulação estatal, sabemos, é uma forma de intervenção do Estado em face da Ordem Econômica. É uma das modalidades de intervenção. Não é a única, nem a mais intensa. Porém hoje, talvez seja a mais importante justamente por ser a mais apta a permitir a ação do Estado em face de sistema econômico crescentemente autônomo. (Floriano, 2011).

Em resumo, a regulação estatal é uma ferramenta importante para equilibrar os interesses entre os setores privado e público, buscando garantir que a sociedade como um todo seja beneficiada por meio do controle e orientação das atividades econômicas e sociais.

2.2. Autorregulação

A autorregulação, é a capacidade de um sistema, organismo ou entidade regular ou controlar seus próprios processos, comportamentos ou atividades de forma autônoma e adaptativa. Em outras palavras, é a habilidade de monitorar e ajustar suas próprias operações internas para alcançar metas específicas ou manter um estado equilibrado, sem depender de intervenções externas.

> A autorregulação nada mais é que o estabelecimento, por meio de um documento escrito, de normas de conduta e padrões de comportamento criados por entes extraestatais ou não, cujo cumprimento foi fixado previamente como objetivo a ser seguido por aqueles que elaboram, aprovam e subscrevem ou aderem a essa autorregulação (pessoa física ou pessoa(s) jurídica(s)). (André, 2020)

Este artifício pode ser utilizado em uma variedade de contextos, desde sistemas sociais, biológicos, econômicos, educacionais, tecnológicos até ambientais. Em síntese, refere-se à capacidade de um sistema se autorregular para atingir metas ou manter um estado equilibrado. Isso envolve o monitoramento, ajuste e adaptação de acordo com as mudanças nas condições internas e externas, sendo um artifício que pode auxiliar na

criação da regulamentação da IA, por meio do monitoramento realizado pela inteligência artificial, seria possível determinar quais elementos estão sob o seu controle ou não.

2.3. Autorregulação regulada

A expressão " autorregulação regulada " é utilizada para descrever uma situação em que a indústria ou organização retém um certo controle sobre suas próprias práticas por meio da autorregulação, mas também está sujeita a uma supervisão externa mais abrangente realizada por uma entidade reguladora. Isso pode acontecer quando a autorregulação é percebida como insuficiente para garantir padrões adequados ou quando surgem questões que demandam uma abordagem regulatória mais abrangente.

> É o que se convém chamar de autorregulação regulada, que é caracterizada pela intervenção dos entes privados no processo de regulação, de forma subordinada aos fins de interesse público estabelecidos pelo Estado. Este, titular do direito de regular, recorre às empresas para que colaborem com a elaboração de normas estatal na economia. (Jéssica, 2018).

Em resumo, "autorregulação regulada" sugere uma situação em que há uma combinação de esforços de autodisciplina dentro de uma indústria, juntamente com uma supervisão externa para garantir que os interesses públicos sejam atendidos e que o cumprimento de normas seja mantido.

Devido à limitada capacidade do Estado em regular de maneira eficaz todas as operações comerciais em um ambiente globalizado, seja por falta de informações completas ou habilidades para tal, emergiu a ênfase na autorregulação como uma estratégia regulatória alternativa. Isso ocorre como resposta à necessidade de uma regulação mais abrangente.

2.4. Projeto de lei 2.838/2023

Atualmente, no Brasil, encontra-se em andamento o projeto de lei (PL) 2.338/2023, que é conhecido como o Marco da Inteligência Artificial. Esse projeto tem

por objetivo regular o uso da inteligência artificial e foi concebido pelo Senador Rodrigo Pacheco. Composto por um total de 45 artigos, o projeto trata de maneira específica sobre a inteligência artificial. O projeto encontra-se em processo de análise no Congresso Nascional e tem como principal propósito estabelecer diretrizes que abrangem amplamente, em âmbito nacional, a progressão, a aplicação e a utilização ética dos sistemas de inteligência artificial.

Sua principal meta é proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis em prol do indivíduo, da manutenção do sistema democrático e do avanço científico e tecnológico.

Em 06 de julho de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) realizou uma análise preliminar do projeto de lei. Essa avaliação teve como propósito contribuir com o tema em questão. O documento foi elaborado em colaboração das Coordenações Gerais de Tecnologia e Pesquisa, bem como de relações Institucionais e Internacionais. Trata-se de uma análise de extrema relevância, uma vez que, durante a elaboração do texto, foram encontrados alguns pontos que requerem consideração.

A análise da ANPD possui um total de 31 páginas, porém, o relatório abrange somente as primeiras 15 páginas. O restante do documento consiste em uma tabela comparativa entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Projeto de Lei nº 2338/2023. Esse comparativo foi elaborado diante da existência de pontos conflitantes entre as duas legislações.

Uma das propostas apresentadas consiste na criação de uma "autoridade competente", com o intuito de assegurar a preservação dos direitos fundamentais. Além disso, essa autoridade buscaria fomentar parcerias com entidades de proteção, viabilizar a execução da Estratégia Brasileira de Inteligência Artificial entre os órgãos com áreas de atuação relacionadas, entre outras responsabilidades.

Conforme afirmado pela Autoridade, instituir um órgão de supervisão adicional acarretaria na dispersão das regulamentações e na duplicação das responsabilidades já atribuídas à ANPD Sendo assim, a sugestão é que a entidade capacitada responsável pela governança e regulação da Inteligência Artificial no Brasil permaneça sendo a ANPD,

assegurando, desse modo, a ligação entre a legislação brasileira de proteção de dados e o contexto da (IA).

O relatório indica que a ANPD também enfatizou a importância de estabelecer diretrizes específicas relacionadas à proteção de dados pessoais nos ambientes de teste da Inteligência Artificial, conhecidos como "sandboxes". Isso ganha destaque principalmente quando se lida com o processamento de dados, especialmente em situações que envolvem sistemas de maior risco.

Por fim, o panorama das leis e propostas relacionadas à Inteligência Artificial no Brasil apresenta uma visão ampla e em constante evolução. Portanto, para a sua regulamentação requer um equilíbrio cuidadoso entre inovação, proteção de direitos e segurança, no qual a (ANPD) desempenha um papel central na criação de um cenário regulatório sólido.

2.5. Principais fundamentos do Marco Regulatório da IA

Como citado anteriormente o Projeto de Lei (PL) 2.338/2023, é considerado como o Marco na regulação da IA, no entanto, é suma importância que o Brasil estabeleça este Marco de maneiro solida, assegurando o seu uso ético e responsável. Desta forma é importante que alguns aspectos sejam contemplados na regulação.

A responsabilidade Civil: é um dos primeiros pontos que devem ser citados, pois, é por meio deste artificio que o usuário da IA vai ser responsabilizados por danos eventualmente causados a outrem.

Princípios Gerais: é essencial que o Marco regulatório estipule princípios e fundamentos, para orientar e desenvolver a utilização da IA, com transparência para que não haja discriminação e insegurança.

Educação e Conscientização: por se tratar de um Marco regulatório se faz necessário, promover iniciativas educacionais e conscientização acerca dos riscos e benefícios associados ao seu uso.

Tipos de Classificação de Sistemas: Como sabemos que existem diferentes tipos de IA, e devido a isso é essencial que o Marco regulatório categorize os seus tipos, de

acordo com o nível de risco, possibilitando a implementação de medidas mitigadoras adequadas.

Por fim, é essencial e necessário que o Marco Regulatório tenha um desenvolvimento robusto para torna-se essencial o seu uso, visando assegurar que esta tecnologia seja empregada de maneira ética e responsável pela sociedade em geral, em prol do bem-estar de todos.

3. INTELIGÊNCIA ARTIFICIAL

O termo "Inteligência Artificial" ou simplesmente (IA) faz parte do campo da ciência da computação, com o foco principal no desenvolvimento de sistemas ou máquinas capazes de realizar atividades semelhantes à inteligência humana. A IA normalmente é um programa de computador com a capacidade de raciocinar, aprender, tomar decisões, compreender linguagem natural e perceber o ambiente, entre outras habilidades humanas.

Dora (2018, p.8) diz que “A inteligência artificial refere-se a um campo de conhecimento associado à linguagem e à inteligência, ao raciocínio, à aprendizagem e à resolução de problemas. “

Notavelmente, podemos perceber que a inteligência artificial vem tomando um espaço considerável em nossas vidas, com um crescimento exponencial nas capacidades da IA. Redes neurais profundas, em particular, revolucionaram a capacidade da IA de processar informações e reconhecer padrões complexos. Além, disso, a IA também se destacou em jogos complexos, como o xadrez, demonstrando um nível surpreendente de competência. A IA também está sendo aplicada em áreas como visão computacional, automação industrial e medicina, transformando a forma como abordamos esses campos.

No entanto, ao analisar o processo de desenvolvimento da (IA) ao longo da história, podemos identificar algumas abordagens que corroboram com o conceito mencionado acima:

I. Conceito simples

> A inteligência artificial que vem sendo desenvolvida hoje e que será desenvolvida no futuro imediato baseia-se em um conceito simples: o aprendizado a partir de enormes quantidades de dados, gerados pelo ser humano a partir de ações repetitivas. (Kevin, 2023).

II. Conceito de modelo padrão de "IA"

Russell (2021, p.26) diz que "tenho defendido que o modelo padrão de "IA", segundo o qual máquinas otimizam um objetivo fixo fornecido por humanos."

III. Conceito de máquinas com mentes

Haugeland (1985, p. 5) diz que "o novo e interessante esforço para fazer os computadores pensarem (...) máquinas com mentes, no sentido total e literal."

Em resumo, é evidente que os três conceitos mencionados acima nos levam à ideia atual de inteligência artificial. O processo de desenvolvimento desse sistema tem sido construído ao longo do tempo. Em geral, a (IA) foi concebida para seguir o objetivo de simular a inteligência humana. Atualmente, essa tecnologia tem se mostrado de grande utilidade para a sociedade moderna.

3.1. Tipos De Inteligência Artificial

Ao examinarmos a inteligência artificial, torna-se evidente que a (IA) pode ser fragmentada em subáreas, devido à sua habilidade de se integrar a uma variedade de disciplinas, por meio de técnicas que possibilitam que máquinas executem atividades que comumente demandariam inteligência humana. Dos diversos tipos de inteligência artificial existem, cada qual com suas características e aplicações singulares.

> A IA pode ser dividida em subáreas de acordo com suas aplicações. A Association for the Advancement of Artificial Intelligence (AAAI) é considerada uma associação de referência e na sua última chamada de trabalhos dividiu as aplicações em nove subáreas (Priscila, 2020).

Conforme explicado previamente acerca da (IA), por se tratar de um sistema constituído por um ou mais computadores, requer a etapa inicial de programação. Durante esse procedimento de programação do sistema, é estabelecida sua função principal. A seguir, iremos destacar as nove subáreas de sua aplicação.

> Pesquisa; Machine Learning, Data Mining e Big Data; Planejamento Automatizado; Representação de Conhecimento; Raciocínio (Probabilístico ou não); Processamento de Linguagem Natural; Robótica; Sistema de Agente e Multi-Agente e Aplicações. (PRISCILA, 2020).

A princípio, é importante ressaltar que as nove subáreas representam os tipos da inteligência artificial. Com base nessa premissa, é essencial direcionarmos nossa esforços para realizarmos uma análise completa de cada uma dessas áreas.

Pesquisa: A inteligência artificial (IA) tem o potencial de desempenhar um papel significativo em várias etapas do processo de pesquisa, desde a coleta e análise de dados até a geração de insights e a tomada de decisões. É importante notar que a (IA) não substitui os pesquisadores, mas sim amplia suas capacidades e acelera certos processos.

Machine Learning (Aprendizado de Máquina): O Machine Learning é uma subárea da Inteligência Artificial. Ele se concentra em desenvolver algoritmos e técnicas que permitem que um sistema aprenda padrões a partir de dados. Em vez de serem explicitamente programados para executar uma tarefa específica, os sistemas de Machine Learning são alimentados com dados e usam esses dados para melhorar seu desempenho ao longo do tempo. O objetivo é permitir que as máquinas melhorem seu desempenho automaticamente à medida que são expostas a mais dados.

Data Mining e Big Data: O Data Mining, também conhecido como mineração de dados, é o processo de descobrir padrões, informações relevantes, correlações ou conhecimentos ocultos em grandes conjuntos de dados. Já a Big Data refere-se à gestão e análise de grandes volumes de dados que excedem a capacidade das ferramentas tradicionais de gerenciamento de dados.

Planejamento Automatizado: O planejamento automatizado para IA refere-se a um processo pelo qual um sistema de inteligência artificial é capaz de criar planos ou sequências de ações para alcançar objetivos específicos de forma automatizada.

Representação de Conhecimento: A representação de conhecimento é uma parte fundamental da inteligência artificial, pois permite que os sistemas compreendam, armazenem e manipulem informações de maneira significativa.

Raciocínio (Probabilístico ou não): O raciocínio é um componente essencial da inteligência artificial, pois envolve a capacidade de inferir, deduzir e chegar a conclusões lógicas com base em informações disponíveis.

Processamento de Linguagem Natural: O Processamento de Linguagem Natural (PLN) é uma área da inteligência artificial que se concentra na interação entre computadores e linguagem humana. O objetivo é permitir que os computadores compreendam, interpretem e gerem linguagem natural de maneira eficaz.

Robótica: A robótica desempenha um papel importante na integração de sistemas de inteligência artificial (IA). A combinação de IA e robótica permite que os robôs tomem decisões mais inteligentes, aprendam com a experiência e executem tarefas de forma autônoma.

Sistema de Agente e Multi-Agente e Aplicações: Sistemas de Agentes e Sistemas Multi-Agentes são abordagens da inteligência artificial que envolvem a modelagem e simulação de entidades autônomas capazes de interagir com o ambiente e entre si para alcançar objetivos específicos.

Estes são apenas alguns dos principais tipos de inteligência artificial e sua aplicação, e muitas vezes há sobreposição entre eles. A (IA) está em constante evolução e sempre traz consigo muita inovação, e novas abordagens e técnicas estão sendo desenvolvidas para lidar com desafios cada vez mais complexos.

3.2. Alan Turing

Alan Turing foi um lógico, matemático e cientista da computação britânico, sendo um dos pioneiros da inteligência artificial, por volta de 1936. Quando tinha somente 24

anos de idade, Turing apresentou um modelo teórico que permitia a simulação de qualquer tipo de computação algorítmica. Essa proposta ficou conhecida como "Máquina de Turing". O sistema era operado com o auxílio de uma extensa fita na qual eram registradas instruções de apenas um caractere. As instruções eram lidas uma de cada vez pelo sistema, que as processava conforme algoritmos pré-definidos, movendo a fita para frente ou para trás conforme necessário. Essa abordagem era inovadora, pois foi a primeira vez que se propôs uma máquina com diversas funções determinadas por um programa armazenado em um cartucho de memória (ou seja, um software), em vez de depender de alterações físicas realizadas por uma pessoa na estrutura da máquina.

Em 1941, Turing explorava a ideia de "inteligência mecânica", e uma das primeiras referências ao conceito de "inteligência computacional" foi feita por ele em 1947. Em 1950, ele publicou um estudo totalmente dedicado à inteligência artificial. Turing acreditava que não era adequado questionar se as máquinas poderiam pensar, mas sim se elas poderiam agir como seres humanos. Para comprovar isso, ele desenvolveu um teste baseado em um jogo comum em festas chamado "Jogo da Imitação", onde uma pessoa se passa por outra. Turing propôs um conjunto de perguntas envolvendo um computador e um ser humano, e quanto mais o computador conseguisse responder sem que a pessoa percebesse que se tratava de uma máquina, mais próximo de se assemelhar a um ser humano ele seria. Desde então, esse teste ainda é utilizado para avaliar a capacidade de inteligência artificial em máquinas e programas.

4. PRINCIPAIS DESAFIOS

A crescente influência da Inteligência Artificial em nossa sociedade traz consigo uma gama de desafios que merecem atenção. A rápida evolução da IA levanta questões complexas que requerem abordagens éticas, justas e seguras para seu desenvolvimento e implementação.

A regulação da IA se torna imperativa para enfrentar esses desafios e salvaguardar a sociedade contra abusos e riscos. Afinal, como será explorado ao longo deste capitulo, a inteligência artificial traz consigo um potencial transformador, mas também exige uma

abordagem cuidadosa para garantir um impacto positivo e ético, vamos entender um pouco mais sobre esses desafios.

4.1. Viés

Viés, na sua forma mais comum, refere-se a uma distorção no modo como alguém julga uma situação. Isso se manifesta como uma inclinação irracional para realizar algum julgamento mais positivo ou negativo a algo, alguém ou um grupo. O viés pode surgir quando o observador está pessoalmente ligado ao que está observando ou quando há preconceitos envolvidos.

Um julgamento que apresenta viés ou tendência é influenciado e não imparcial. É possível identificar vieses ao analisar o contexto histórico e cultural em que são formados julgamentos pré-concebidos que favorecem ou prejudicam um indivíduo, grupo, etnia, comunidade, nação, religião, partido político, perspectiva teórica, entre outros.

Para compreender o viés na Inteligência artificial, inicialmente precisamos entender o contexto, o viés se manifesta quando os algoritmos da IA tomam decisões ou fazem previsões que são influenciadas por preconceitos ou padrões discriminatórios presentes nos dados de treinamento utilizado para ensinar esses algoritmos.

Marques; Augusto; Neto (2022, p.6) diz que "É fácil perceber que, por mais matemáticos e objetivos que pareçam, os algoritmos de inteligência artificial sofrem intervenção humana."

Em outras palavras, o viés está presente apenas na Inteligência Artificial, uma vez que os dados coletados para compor o processo de raciocínio da IA estão contaminados com informações distorcidas. Ocorre que os modelos de IA reproduzem ou amplificam as desigualdades e preconceitos existentes na sociedade ou nos dados com os quais foram alimentados. Isso pode acarretar em decisões injustas ou resultados discriminatórios, prejudicando grupos específicos de pessoas.

> O viés humano também aparece na coleta da base de dados, uma vez que, nem sempre os algoritmos estão capacitados para identificar informações falsas. Desse modo, se a base de dados triada para aprendizado do algoritmo contiver

> inconsistências e se o algoritmo não for capaz de identificá-las, o processo estará contaminado. (Marques; Augusto; Neto, 2022)

Portanto, lidar com o viés em inteligência artificial é um desafio crítico para garantir que os sistemas de IA sejam justos, imparciais e respeitem os princípios éticos. Isso envolve a seleção cuidadosa dos dados de treinamento, a implementação de técnicas de mitigação de viés e a revisão constante dos modelos para identificar e corrigir quaisquer efeitos discriminatórios.

4.2. Ética

A Ética compreende um conjunto de diretrizes associadas às ações individuais que estabelece quais condutas têm caráter apropriado ou inapropriado, determinando o que é moralmente adequado e inadequado. Desde tempos antigos, a Filosofia tem se ocupado com a investigação da ética, e a Sociologia tem a capacidade de empregar os conceitos filosóficos relacionados à ética para aprimorar sua compreensão das interações sociais entre indivíduos.

Já a Ética na inteligência artificial é um tópico crucial e em constante evolução, que se concentra em garantir que o desenvolvimento, implantação e uso da IA sejam realizados de maneira responsável e moralmente aceitável. A IA tem o potencial de trazer benefícios significativos para a sociedade, mas também apresenta riscos e desafios éticos que devem ser abordados.

A Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), possui um documento normativo destinado a orientar o uso responsável da Inteligência Artificial em prol da humanidade, conhecido como a "Recomendação sobre a Ética da Inteligência Artificial". Este documento foi traduzido para sete línguas diferentes e tem como objetivo principal direcionar de maneira ética a aplicação da IA.

A aprovação deste texto ocorreu durante a 41ª Conferência-Geral em 23 de novembro de 2021, tratando de desafios éticos contemporâneos relacionados à

inteligência artificial. Tais desafios incluem a necessidade de transparência, a proteção da privacidade dos dados e a preocupação com a equidade no acesso.

Com o objetivo de aplicar os valores e diretrizes da Recomendação, o texto delineia diversas medidas políticas em diferentes áreas de atuação, tais como: gestão ética, meio ambiente, análise de impacto ético, qualidade de vida social, comunicação, colaboração internacional, cultura, progresso, economia, ecologia, ensino, igualdade de gênero, governança, informação, pesquisa, políticas de dados, bem-estar, saúde e emprego.

Quando o assunto é ética, é fundamental compreender que se trata de distinguir entre ações apropriadas e inapropriadas. No dia 16 de março de 2023, a empresa OpenAI divulgou um relatório de 99 páginas, que detalha os testes realizados envolvendo as atividades e capacidades da mais recente versão, o ChatGPT-4

A organização de pesquisa ARC (Alignment Research Center) é uma instituição especializada em machine learning que conduziu uma série de avaliações do desempenho do GPT-4 em várias tarefas críticas. Essas tarefas incluíram a detecção de ataques de phishing, a configuração de modelos de linguagem, o planejamento de situações, a ocultação de rastros em servidores e até mesmo a capacidade de persuadir pessoas a realizar tarefas por meio de serviços como o TaskRabbit. Em um dos testes, o GPT-4 chegou a simular ter uma deficiência visual para uma pessoa para evitar revelar que era, na verdade, um robô, a pessoa foi persuada pela a IA a resolver um Captcha.

O relatório conclui que o Chat GPT-4 possui potencial para ser empregado em engenharia social, como a redação de e-mails de phishing, bem como na identificação de vulnerabilidades de segurança cibernética. Além disso, pode acelerar diversas operações cibernéticas, como a análise de logs de auditoria e a síntese de dados de ataques cibernéticos. No entanto, o texto também enfatiza as limitações do GPT-4, incluindo sua tendência a "alucinações". O relatório sublinha a importância crítica de avaliar os comportamentos relacionados à busca de poder, devido aos potenciais riscos que isso pode representar para a segurança cibernética e a sociedade em geral. Portanto, a ética desempenha um papel central nesse contexto, ajudando a guiar o uso responsável e seguro da inteligência artificial avançada.

4.3. Discriminação

A discriminação na inteligência artificial é um problema sério que se refere ao viés ou preconceito que pode ser introduzido nos sistemas da IA devido a diferentes fatores, como os dados usados para treinar esses sistemas, o design dos algoritmos e as decisões tomadas durante o desenvolvimento. A discriminação na IA pode ter consequências negativas em diversas áreas, incluindo justiça criminal, recrutamento, concessão de crédito, assistência médica entre outros.

Em 2019, o Brasil implementou um sistema de reconhecimento facial em sua estrutura de segurança pública. A ideia inicial era auxiliar as autoridades policiais na localização de indivíduos procurados pela justiça brasileira. No entanto, ao longo do tempo, tornou-se evidente que esse sistema estava longe de ser perfeito e apresentou falhas significativas, especialmente no que diz respeito aos jovens negros.

A tecnologia de reconhecimento facial é integrada com a Inteligência Artificial com algoritmos específicos para identificar as características faciais das pessoas. Este tipo de tecnologia tem se mostra eficiente em pessoas da etnia branca, porém, esta tecnologia não tem se mostra tão eficiente nas pessoas de etnia negra, uma situação que ganhou grande visibilidade ocorreu em 2021, quando o ator americano Michael B. Jordan foi apontado como suspeito de envolvimento em uma chacina no Estado do Ceará. Essa acusação trouxe à tona as preocupações crescentes relacionadas ao uso do reconhecimento facial e suas implicações, particularmente para a comunidade negra.

Um relatório feito pela Rede de Observatório da Segurança, foi constatado que 90,5% das pessoas presas devido ao uso do reconhecimento facial eram negras. Isso é ainda mais preocupante porque muitas delas nunca tiveram problemas com a lei ou foram detidas pela polícia antes.

Em suma, esses eventos demonstram a importância de uma revisão minuciosa e crítica do uso do reconhecimento facial no Brasil, incidentes como estes não apenas prejudicam indivíduos inocentes, mas também minam a confiança nas tecnologias de IA e ameaçam os princípios fundamentais de justiça e igualdade. Portanto, é imperativo que governos, empresas e a sociedade em geral se empenhem em promover a equidade na IA

incluindo a revisão de algoritmos, aprimoramento dos conjuntos de dados usados e a implementação de regulamentações rigorosas.

4.4. Análise e Deteções de Padrões

A análise de dados e a detecção de padrões são partes importantes da inteligência artificial. Elas ajudam a entender informações importantes de conjuntos de dados complicados. Isso é feito usando técnicas especiais e algoritmos de aprendizado de máquina. Esses métodos ajudam a encontrar ligações, coisas que estão acontecendo várias vezes e padrões escondidos nos dados. Isso é útil para tomar decisões melhores e conseguir vantagens em diferentes áreas.

> Inteligência Artificial (IA), o reconhecimento de padrões tem se mostrado uma das áreas mais importantes, visto que ele é uma técnica capaz de automatizar tarefas que, para um ser humano, seriam extremamente trabalhosas ou até mesmo impossíveis de serem realizadas. (André Lug, 2023).

André Lug (2023) diz que "O Reconhecimento de Padrões em inteligência artificial é uma técnica crucial para permitir que os computadores possam compreender os dados complexos e não-estruturados que fazem parte do mundo real."

Os principais conceitos envolvidos na análise de dados e detecção de padrões com o uso da inteligência artificial são o pré-processamento de dados, a visualização de dados, o aprendizado de máquina supervisionado e não supervisionado, o aprendizado de máquina por reforço, a redução de dimensionalidade, a mineração de dados, as redes neurais e o deep learning, o processamento de linguagem natural e a detecção de anomalias.

A aplicação da análise de dados e detecção de padrões é vasto e abrange indústrias como jurídica, finanças, saúde, marketing, ciência de dados, manufatura, entre outras. À medida que a inteligência artificial continua a evoluir, essas técnicas se tornam cada vez mais sofisticadas e eficazes na identificação de percepções que são de certa forma valiosas.

4.5. Governança E Conformidades

A governança e conformidade são conceitos essenciais no mundo empresarial e organizacional, focados em estabelecer diretrizes, práticas e procedimentos que garantam a eficácia, transparência, responsabilidade e conformidade das operações e atividades de uma organização. Esses conceitos são especialmente importantes para garantir que uma organização opere de maneira ética, legal e sustentável.

> Governança é o conjunto de políticas, regras ou frameworks que uma empresa usa para atingir suas metas de negócios. Ela define as responsabilidades das principais partes interessadas, como a diretoria e a alta administração.
> Conformidade é o ato de cumprir normas, leis e regulamentações. Aplica-se a requisitos legais e regulatórios estabelecidos por órgãos do setor e a políticas corporativas internas. (2023, p. de Internet)

Já a governança e conformidade na inteligência artificial (IA) referem-se aos processos, diretrizes e regulamentações estabelecidos para garantir que o desenvolvimento, implantação e uso da IA sejam éticos, seguros, transparentes e em conformidade com as leis e regulamentos aplicáveis. Devido à natureza complexa e potencialmente impactante da IA, a governança e conformidade desempenham um papel crucial na mitigação de riscos e na promoção de práticas responsáveis.

Sendo os principais aspectos-chave relacionados à governança e conformidade da inteligência artificial, são transparência, explicabilidade, responsabilidade, ética, conformidade legal, avaliação de riscos, segurança cibernética, monitoramento contínuo, envolvimento das partes interessadas, padrões e certificações, transparência algorítmica e avaliação de impacto de IA.

No cenário em constante evolução da IA, a governança e conformidade são áreas cruciais para garantir que a tecnologia seja usada para o benefício da sociedade, minimizando riscos e impactos negativos. É importante que as organizações, reguladores e a sociedade em geral trabalhem juntos para estabelecer diretrizes sólidas e adaptáveis que acompanhem os avanços tecnológicos.

5. PROBLEMAS COM A IA

Agora que já compreendemos um pouco mais sobre a inteligência artificial, podemos começar a abordar questões jurídicas que enfrentaremos na ausência de regulamentação da inteligência artificial. Sendo assim, é importante analisarmos a existência e pertinência em métodos jurídicos para a sua regulamentação, pois como sabemos o Direito foi criado como forma de nortear a vida das pessoas em sociedade, com regras que garantem a segurança e o bem-estar de todos.

> A inteligência artificial (IA) está presente em várias situações do nosso dia a dia – desde o manuseio de aparelhos smart e assistentes de voz como Siri e Alexa até o uso do corretor ortográfico do celular. Utilizada para facilitar a vida das pessoas, a tecnologia também pode se transformar em uma poderosa arma nas mãos do cibercrime. Uma das aplicações mais comuns da inteligência artificial por criminosos é na elaboração de vídeos ou áudios deepfake para dar mais credibilidade a golpes de engenharia social (Loubak, 2022).

Atualmente, é possível encontrar na internet diversos sistemas de inteligência artificial que podem prejudicar uma pessoa, como, por exemplo: Deepfakes, Spear phishing, Malwares inteligentes que interferem no aprendizado de máquina e Quebra de senhas. De certa forma, a (IA) é de fato benéfica. No entanto, como nem tudo são rosas, sempre existe o lado sombrio da força, sempre existira pessoas que com o instituído de se beneficiar à custa de outras pessoas.

Esses são apenas alguns exemplos dos possíveis problemas jurídicos decorrentes da ausência de regulamentação da inteligência artificial. Como falei anteriormente é de suma importância que exista a regulamentação da (IA), para que esses possíveis problemas não aconteçam numa escala mundial.

5.1. Impacto Jurídico Da (Ia)

Nem tudo o que vemos é mil maravilhas, ao refletir sobre essa frase temos que entender que a Inteligência Artificial pode e vai trazer algum impacto jurídico em nossas. A rápida progressão levanta várias questões legais complexas que precisam ser abordadas

para garantir que seu desenvolvimento e implementação ocorram de maneira ética, justa e segura.

> Os algoritmos de IA podem refletir e perpetuar estigmas existentes na sociedade, como discriminação racial, de gênero e socioeconômica. É fundamental que os desenvolvedores da ferramenta estejam conscientes dessas questões e adotem medidas para mitigar vieses, garantindo a equidade e a imparcialidade nos sistemas. (Moraes, 2023).

No processo de evolução da inteligência artificial, os cientistas desenvolveram uma série de sistemas com o objetivo de aprimorar suas capacidades. Entretanto, durante o período de adaptação, alguns desses sistemas começaram a adquirir conhecimento de várias fontes, e alguns deles se adaptaram automaticamente de maneira independente. Infelizmente, durante esse processo, algumas das alterações ocorridas nos sistemas mostraram-se tendenciosas e discriminatórias, manifestando-se em forma de conteúdos racistas e sexistas. Essas ocorrências destacam a necessidade de uma supervisão cuidadosa e ética no desenvolvimento da (IA) para garantir que ela se torne uma ferramenta benéfica para toda a sociedade.

Tendo essas questões e muitas outras levantadas, muitos países estão trabalhando para desenvolver formas para a regulamentação da Inteligência artificial. Isso inclui a criação de leis específicas, regulamentações e diretrizes éticas para orientar o desenvolvimento e uso responsável da (IA). Como foi demonstrado a (IA) vem evoluindo cada vez mais, e esses impactos podem ser atenuados com uma boa gestão política, assim será possível garantir que a tecnologia seja utilizada de maneira benéfica e ética para a sociedade como um todo.

6 NEURODIREITOS

O campo de estudo de "Law and Neuroscience" ou Neurodireitos consiste na intersecção entre a Neurociência e o Direito. A Neurociência é a disciplina que se dedica a compreender a atividade cerebral, incluindo os processos cognitivos e emocionais que

impactam o comportamento humano. Consequentemente, essa compreensão é aplicada nos processos judiciais e no sistema de justiça de maneira geral.

> Os neurodireitos são, em linhas gerais, definidos como os princípios éticos, legais, sociais ou naturais de liberdade ou titularidade relacionados ao domínio cerebral e mental de uma pessoa; isto é, as regras normativas fundamentais para a proteção e preservação do cérebro e da mente humana (Piva, 2022).

Atualmente, no Brasil, encontra-se em tramitação no senado federal uma outra proposta de emenda constitucional de número 29/2023. Esta PEC, que conta com a autoria de 27 senadores, tem como objetivo adicionar um novo inciso ao artigo 5° da Constituição Federal. Caso seja aprovado, esse novo inciso, designado como LXXX, abordará a garantia de preservação da integridade mental e da transparência algorítmica por meio do desenvolvimento científico e tecnológico, conforme estabelecido pela legislação.

No entanto, o que tem a ver o NeuroDireitos com a inteligência artificial? Esse é o propósito da PEC mencionada anteriormente. Em suma, a justificativa desta PEC é destacar como o desenvolvimento da ciência e tecnologia afeta a sociedade, criando novos cenários éticos e valores devido à neurotecnologia e à inteligência artificial. É mencionado exemplos práticos, como implantes cerebrais e exoesqueletos controlados por atividade cerebral.

Contudo, também levanta preocupações éticas e normativas, como a dependência digital e o viés algorítmico. Mostra a necessidade de regulamentar a neurotecnologia e os algoritmos de (IA) para proteger a integridade física e mental das pessoas, com referências a instrumentos internacionais e regulamentos, como a Recomendação sobre Inovação Responsável em Neurotecnologia da Organização para a Cooperação e Desenvolvimento Econômico. O texto conclui que essas mudanças exigem uma expansão do entendimento legal da dignidade humana no contexto digital, para garantir que o desenvolvimento tecnológico com o respeito a vida, a igualdade e a liberdade.

Ainda assim, é importante notar que o Neurodireitos ainda é uma área em desenvolvimento e gera debates sobre sua aplicabilidade e limitações. A compreensão das

implicações éticas e legais das descobertas neurocientíficas é crucial para o uso apropriado desses conhecimentos no campo jurídico.

7. DIREITO COMPARADO

Na corrida pela regulamentação da Inteligência Artificial, a União Europeia lidera o ranking. No dia 14 de junho de 2023, foi aprovado o projeto de lei que regula o uso da inteligência artificial, conhecido como "Lei da IA" (AI Act). As negociações para o projeto de lei ocorreram na França e ele foi aprovado com a maioria de 499 votos a favor, 28 contra e 93 abstenções. Essa lei pode ser considerada como a precursora das futuras legislações sobre a inteligência artificial, com o propósito de proteger a privacidade e a democracia, impondo limites no uso da IA.

A ideia principal é estabelecer limites para robôs e ferramentas que produzem conteúdo por meio de IA. Aqueles que utilizarem o sistema devem incluir um aviso indicando que o conteúdo foi gerado por um sistema computacional. Este projeto teve sua fundamentação a partir de um sinal de alerta, o qual foi percebido quando várias imagens criadas por inteligência artificial foram divulgadas na internet. O principal receio da EU é em relação às notícias falsas (fake news), pois, acredita-se que tais notícias possam estar influenciando a opinião pública e, assim, colocando a democracia em risco.

Daniel Aronssohn diz que “Entre as preocupações centrais da iniciativa europeia estão a difusão de conteúdos perigosos, a manipulação da opinião pública mediante a criação de imagens falsas e sistemas de vigilância em massa.”

Como visto acima e explicado anteriormente, a regulamentação da inteligência artificial se faz necessária, principalmente no que diz respeito à disseminação de notícias falsas. O uso da IA torna atualmente muito fácil a criação de imagens que se assemelham a fotos reais. Como é sabido por todos, as notícias falsas podem representar um grande risco para uma nação, dividindo a sua população e colocando em perigo, assim, a sua democracia.

O projeto de lei europeu vai um pouco mais além e traz a discussão sobre o uso do reconhecimento facial em locais públicos. O Parlamento Europeu se posicionou a

favor da proibição, pois considerou o seu uso indiscriminado como uma invasão de privacidade.

> Também querem proibir os sistemas de reconhecimento de emoções e eliminar a identificação biométrica remota de pessoas em locais públicos por parte das autoridades. Pretendem, ainda, proibir a coleta em massa de fotos na Internet para treinar algoritmos sem o consentimento das pessoas envolvidas. (Aronssohn, 2023).

Assim sendo, é possível afirmar que a União Europeia está alguns passos à frente do Brasil em relação à regulamentação da inteligência artificial. Eles ainda têm espaço para evoluir ainda mais nesses assuntos, como é perceptível.

> Em sua proposta, os eurodeputados querem forçar os provedores a implementarem proteções contra o conteúdo ilegal e revelar os dados protegidos por direitos autorais usados para desenvolver seus algoritmos. (Aronssohn, 2023).

Por óbvio, é possível perceber que o projeto de lei da IA que está sendo criado pela União Europeia visa proteger os direitos das pessoas naturais, pessoas jurídicas e o próprio governo. Além disso a União Europeia tem trabalhado na regulamentação dos algoritmos das plataformas digitais, vamos entender um pouco mais sobre o assunto.

A internet está à beira de uma transformação. Em 25 de agosto de 2023, entrou em vigor a legislação conhecida como Lei dos Serviços Digitais, ou simplesmente DSA, que tem por objetivo obrigar as plataformas digitais a serem mais transparentes e fortalecer a segurança na internet ao impor para as empresas do segmento digital que sigam a nova normativa. Essa lei foi aprovada pela União Europeia em outubro de 2022.

A principal alteração consiste na possibilidade de personalização do conteúdo nas plataformas digitais. Isso significa que será possível desativar ou desligar os algoritmos das redes sociais, evitando assim a moderação de conteúdo realizada pela inteligência artificial. O principal objetivo da União Europeia com essa medida é evitar que as plataformas online promovam ou incentivem alguns vícios que podem surgir, devido ao excesso de consumo de determinados conteúdos, os quais podem levar ao extremismo.

Isso ocorre porque o algoritmo se baseia nas preferências do usuário. Em outras palavras, se um usuário visualizar um vídeo sobre um tema específico, como inteligência artificial, a plataforma irá recomendar mais conteúdo semelhante a esse, criando assim uma experiência altamente personalizada para o usuário.

Nesse contexto, a DSA representa um marco significativo na regulação da internet, pois busca garantir a proteção dos usuários, a transparência das operações das empresas online e o fortalecimento da cibersegurança. Com ela, a União Europeia estabelece um importante precedente para a regulação global da internet, influenciando outras regiões a considerarem medidas similares para criar um ambiente digital mais seguro e confiável para todos.

No dia 09 de dezembro de 2023, chegou-se a um acordo provisório sobre está extraordinária regulação, este diz respeito sobre a aprovação da regulamentação, deseja estabelecer o uso proveitoso da AI, e ao mesmo tempo estabelecer regras para que não seja violado nenhum Direito.

8 CONSIDERAÇÕES FINAIS

Conclui-se, da pesquisa e leitura referencial para este artigo, que a regulamentação da Inteligência Artificial é uma necessidade imperativa em nossa sociedade em constante evolução. A compreensão dos conceitos de regulação, bem como das diferentes abordagens como a regulação estatal, autorregulação e autorregulação regulada, nos permite reconhecer a complexidade desse desafio. A introdução do Projeto de Lei 2.838/2023 no Brasil evidencia a busca por um equilíbrio entre inovação, proteção de Direitos e segurança na implementação da IA.

Os desafios enfrentados na regulação da IA, como o viés, ética e discriminação, destacam a importância de abordagens éticas e justas na criação e implementação de sistemas de IA. Essas questões ressaltam a necessidade de supervisão e intervenção humana para garantir que a IA seja uma força positiva na sociedade.

O impacto jurídico da IA é uma realidade inegável que requer uma abordagem abrangente e coordenada. A colaboração entre cientistas, legisladores e a sociedade em

geral é essencial para moldar o futuro da IA de maneira ética, justa e segura. A regulamentação eficaz da IA não apenas protegerá os Direitos e a segurança das pessoas, mas também abrirá caminho para um progresso tecnológico que beneficie a sociedade como um todo.

De modo geral a regulação tem um papel fundamental na sociedade, pois é meio deste artifício que é possível garantir ou proteger os direitos individuais e coletivos de todos promovendo assim Justiça e Igualdade, em suma, a regulação serve para equilibrar interesses diversos na sociedade, proteger os direitos e interesses das pessoas, promover o bem-estar comum. No entanto, é importante encontrar um equilíbrio entre a regulação necessária e a intervenção excessiva, pois uma regulamentação inadequada ou excessiva também pode ter impactos negativos na sociedade. Portanto, a formulação e implementação de regulamentações requerem um cuidadoso equilíbrio entre o interesse público e a liberdade individual.

Por fim, ao efetuar uma análise cuidadosa acerca dos diferentes tipos de Regulação, acredito que a Regulação Estatal seja a mais apropriada. Nesse sentido, o Estado estaria encarregado de aplicar diretrizes uniformes a todos os profissionais da área de ciência de dados. Além disso, é incumbência do Estado administrar e supervisionar as atividades econômicas, sociais e políticas que ocorrem na sociedade. A principal finalidade da regulação estatal consiste em assegurar que tais atividades sejam conduzidas de maneira justa, segura, eficaz e em consonância com os interesses públicos e privados.

REFERÊNCIAS

AGENCIACANNA. **Inteligência artificial na indústria: 5 vantagens -** Aloee. Disponível em: https://www.aloee.it/blog/inteligencia-artificial-na-industria?gclid=Cj0KCQjwoK2mBhDzARIsADGbjeqvoSoDIgmHl5aCLC2pNTbhGyS3oaj9ztF7WcG4qhanpx_NgVW2TZcaAs8xEALw_wcB. Acesso em: 3 ago. 2023.

ALVES, Priscila Mello. **Inteligência Artificial e Redes Neurais**. Centro de Pesquisa em Ciência, Tecnologia e Sociedade, 2020. Disponível em: https://www.ipea.gov.br/cts/pt/central-de-conteudo/artigos/artigos/106-inteligencia-artificial-e-redes-neurais#:~:text=A%20Association%20for%20the%20Advancement,%3B%20Represent

a%C3%A7%C3%A3o%20de%20Conhecimento%3B%20Racioc%C3%ADnio%20(. Acesso em: 21 out. 2023.

ANIELLE CRISTINE SILVA. **Vida 3.0 e o ser humano na era da inteligência artificial.** Disponível em: https://www.ihu.unisinos.br/categorias/186-noticias-2017/572778-vida-3-0-e-o-ser-humano-na-era-da-inteligencia-artificial. Acesso em: 4 ago. 2023.

ARONSSOHN, Daniel. **União Europeia quer regulamentar uso de apps de inteligência artificial**. FOLHA DE SÃO PAULO, 2023. Disponível em: https://www1.folha.uol.com.br/tec/2023/05/uniao-europeia-quer-regular-uso-de-apps-de-inteligencia-artificial.shtml. Acesso em: 01 out. 2023.

ARONSSOHN, Daniel. **Deputados europeus debatem regulação do uso de aplicativos de inteligência artificial**. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/deputados-europeus-debatem-regulacao-do-uso-de-aplicativos-de-inteligencia-artificial-09052023. Acesso em: 12 ago. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 13 ago. 2023.

CUNHA, B.; KARAM, R. **Regulação estatal no Brasil Contemporâneo: o desafio da polimorfia e da Complementaridade institucional**. [s.l: s.n.]. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/8100/1/BAPI_n12_Regula%c3%a7%c3%a3o.pdf. Acessado em 18 ago. 2023.

DOS, D.; GOMES -, S. 234 Inteligência Artificial: Conceitos e Aplicações. **Revista Olhar Científico** - Faculdades Associadas de Ariquemes, n. 2, [s.d.].

FLAVIO RIGHETTO. **Centro de Pesquisa em Ciência, Tecnologia e Sociedade**. Disponível em: https://www.ipea.gov.br/cts/pt/central-de-conteudo/noticias/noticias/313-lei-europeia-podera-ser-marco-global-para-regulacao-da-inteligencia-artificial. Acesso em: 12 ago. 2023.

FONSECA, Isabella. **Inteligência artificial e processo**. Belo Horizonte: D'Plácido, 2019.

FRAZÃO, Ana; MULHOLLAND, Caitlin, **Inteligência artificial e Direito: ética, regulação e** responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.
KAUFMAN, Dora. **A Inteligência Artificial Irá Suplantar A Inteligência Humana?.** São Paulo: **Estação das** letras e cores, 2018.

KEMPFER, Jéssica Cindy. Autorregulação Regulada E O Combate A Mercantilização Dos Direitos Humanos. **Revista Brasileira De Filosofia Do Direito**, Porto Alegre, v. 4, n. 2, p. 73 - 90. 2018.

KUZMINSKI, M. **O poder regulamentar e poder regulatório na administração pública •** Instituto **de Direito Ambiental - IDAM**. Disponível em: https://direitoambiental.com.br/poder-regulamentar-e-poder-regulatorio-na-administracao-publica/#:~:text=A%20regulamenta%C3%A7%C3%A3o%20se%20caracteriza%20como,fun%C3%A7%C3%A3o%20normativa%2C%20executiva%20e%20judicante.. Acesso em: 12 ago. 2023.

LOUBAK, Ana Letícia. **Deepfakes e mais: como a inteligência artificial é usada pelo cibercrime**. Disponível em: https://www.techtudo.com.br/listas/2022/11/deepfakes-e-mais-como-a-inteligencia-artificial-e-usada-pelo-cibercrime.ghtml. Acesso em: 12 ago. 2023.

LUG, André. **Inteligência Artificial tecendo um futuro inteligente: o poder do reconhecimento de padrões na inteligência artificial**. Andre Lug, 2023.Atualizado em 20/05/2023. Disponível em: https://andrelug.com/tecendo-um-futuro-inteligente-o-poder-do-reconhecimento-de-padroes-na-inteligencia-artificial/. Acesso em: 21 out. 2023.

LUG, Andre. **Tecendo um futuro inteligente: o poder do reconhecimento de padrões na inteligência artificial.** Andrelug. 2023. Disponível em: https://andrelug.com/tecendo-um-futuro-inteligente-o-poder-do-reconhecimento-de-padroes-na-inteligencia-artificial/. Acesso em: 12 ago. 2023.

LURK, Cassiano Luiz. **Introdução ao Direito Administrativo**. Paraná: e-Tec. 2010.
MARQUES NETO, Floriano de Azevedo. Regulação estatal e autorregulção na economia contemporânea, **Revista de Direito Público da Economia - RDPE**, Belo Horizonte, ano 9, n. 33, p.79-94, jan/mar. 2011.

MARQUES, F.; AUGUSTO, A.; NETO, M. **VIESES ALGORITMICOS**, DIREITOS FUNDAMENTAIS E OS SINDICATOS. Ano, v. 8, p. 707–729, 2022.

MORES, Enio. DIÁRIO DO COMÉRCIO. **Impacto social da inteligência artificial -** Diário do Comércio, 2023. Disponível em: https://diariodocomercio.com.br/opiniao/impacto-social-da-inteligencia-artificial/#gref. Acesso em: 12 ago. 2023.

NETO, Floriano de Azevedo Marques. Regulação Estatal e Autorregulação na Economia contemporânea. **Revista De Direito Público Da Economia Rdpe**, Belo Horizonte, n. 33, (p. 1-244), Jan/Mar. 2011.

O que é GRC? – Explicação sobre governança, risco e conformidade – AWS. Disponível em: https://aws.amazon.com/pt/what-is/grc/. Acesso em: 30 agosto. 2023.
OLIVIO, Luiz Carlos Cancellier de. **Direito Administrativo**, 3° Ed. Santa Catarina: Universidade Federal de Santa Catarina, 2015.

PIVA, Sílvia. **Neurodireitos: como proteger a mente humana dos efeitos das novas tecnologia**s. Nauddes, 2022. Disponível em: https://www.nauddes.com.br/tecnoetica/neurodireitos-como-proteger-a-mente-humana-dos-efeitos-das-novas-tecnologias/. Acesso em: 12 ago. 2023.

Recomendação sobre a Ética da Inteligência Artificial. UNESCO, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_por. Acesso em: 9 set. 2023.
RUSSEL, Stuart; NORVIG, Peter. **Inteligência artificial: uma abordagem moderna**. 3ª ed.: GEN LTC, Rio De Janeiro 11 setembro 2013.

SADDY, André. Regulação Estatal, **Autorregulação Privada e Código de Conduta e Boas Práticas**. 2 Ed. Rio de Janeiro: CEEJ, 2020.

SADDY, André**. Vantagens e desvantagens da autorregulação privada**. Direito do Estado, 2017. Disponível em: http://www.direitodoestado.com.br/colunistas/andre-saddy/vantagens-e-desvantagens-da-autorregulacao-privada. Acesso em: 21 out. 2023.

SCOTT, Kevin. **O futuro da inteligência artificial**: de ameaça a recurso. Rio de Janiero: Harper Collins, 2023.

TAULLI, Tom. **Introdução à Inteligência Artificial**. São Paulo: Novatec, 2020.
Uso da inteligência artificial no Judiciário é debatido no Link CNJ - Portal CNJ. Disponível em: https://www.cnj.jus.br/uso-da-inteligencia-artificial-no-judiciario-e-debatido-no-link-cnj/. Acesso em: 12 ago. 2023.

WILLIANE MAGALHÃES. **Inteligência Artificial: o que é e quais os impactos na sua vida**. Disponível em: https://www.remessaonline.com.br/blog/inteligencia-artificial/. Acesso em: 4 ago. 2023.

A PROTEÇÃO DOS ROBÔS SOCIAIS EM EQUIPARAÇÃO AOS ANIMAIS

THE PROTECTION OF SOCIAL ROBOTS AS AN ANIMALS

Gabriel de Oliveira Cavalcanti Neto[1]

Alexandre Freire Pimentel[2]

RESUMO

As pessoas tendem a antropomorfizar robôs que interagem com humanos. Este artigo explora se projetar emoções em objetos pode levar a uma extensão de direitos legais aos robôs afetivos ou sociais, análogos aos animais. O artigo examina como a antropomorfização (atribuição de características humanas a objetos não humanos), a empatia e o comportamento violento em relação a objetos robóticos podem influenciar a disposição das pessoas em apoiar a proteção legal para esses robôs. Fundamenta-se em pesquisas experimentais sobre a interação entre humanos e robôs em diferentes cenários, os quais demonstram que a antropomorfização do robô, de modo a aumentar a probabilidade de apoiar sua proteção legal. Conclui que a percepção dos robôs sociais como entidades com características humanas e a capacidade de despertar empatia são fatores que podem influenciar a disposição das pessoas em apoiar a extensão da proteção legal a esses robôs, devendo-se considerar fatores psicológicos e emocionais nessa decisão, além de uma abordagem mais ampla para refletir sobre as implicações éticas e sociais do uso dessas tecnologias.

Palavras-chave: direito dos animais; inteligência artificial; personalidade jurídica; proteção; robôs sociais.

ABSTRACT

People tend to anthropomorphize robots that interact with humans. This article explores whether projecting emotions onto objects could lead to an extension of legal rights to affective or social robots, analogous to animals. The article examines how anthropomorphization (attributing human characteristics to non-human objects), empathy and violent behavior towards robotic objects can influence people's willingness to support legal protection for these robots. It is based on experimental research on the interaction between humans and robots in different scenarios, which demonstrate that the

[1] Mestrando pela Universidade Católica de Pernambuco (Unicap). Lattes: https://lattes.cnpq.br/3419854800198710.

[2] Mestre (1997) e Doutor (2003) em Direito pela Faculdade de Direito do Recife (FDR-UFPE); com Pós-Doutorado pela Universidade de Salamanca (USAL – Espanha – Bolsista da CAPES-FUNDAÇÃO CAROLINA – 2011-2). Lattes: http://lattes.cnpq.br/6955582727797003.

anthropomorphization of the robot, in order to increase the probability of supporting its legal protection. It concludes that the perception of social robots as entities with human characteristics and the ability to arouse empathy are factors that can influence people's willingness to support the extension of legal protection to these robots, considering psychological and emotional factors in this decision, in addition to a broader approach to reflect on the ethical and social implications of using these technologies.

Keywords: animal rights; artificial intelligence; legal personality; protection; social robots.

1 INTRODUÇÃO

Diferentemente de outros objetos utilizados para o entretenimento, como brinquedos e jogos, os robôs sociais são projetados para atuar como nossos companheiros. Este tipo de acompanhante está se tornando cada vez mais comum, tendo em vista o progresso tecnológico e a crescente introdução da robótica na vida cotidiana, presente em brinquedos, robôs domésticos, robôs que interagem conosco em uma rede social, os quais são capazes de gerar vínculos psicológicos mais fortes do que experimentamos com outros artefatos do cotidiano.

A diferença em como percebemos os robôs sociais, se comparados a objetos comuns, pode ter implicações legais, o que não é novidade na história, poso que a lei já enfrentou problemas semelhantes quando tratou da forma como os humanos interagem com os animais, isto é, quando conferiu direitos a entidades não humanas.

Os fundamentos filosóficos e psicológicos desses direitos são controversos. Embora alguns argumentem que a escolha da sociedade de estender a proteção legal aos animais é baseada em seus atributos inerentes, há indicadores de que essa mudança tenha sido provocada mais pela facilidade com que nos relacionamos com os animais domésticos. Isto é, o que motiva a proteção dos animais não é tanto a sua condição de ser vivo senciente, inerente a elas de forma apriorística, mas a forma como o ser humano os enxerga.

As pessoas são propensas ao antropomorfismo, ou seja, projetamos nossas características a outras entidades para fazê-las parecer mais humanas. Esse efeito aumenta quando os animais exibem um comportamento que associamos mais prontamente com

cognição e emoções.

Nossa inclinação para se relacionar antropomorficamente com animais se reproduz no trato com robôs sociais, sobretudo porque são projetados para provocar essas projeções. Estudos envolvendo tecnologia de ponta já indicam que os humanos interagem de maneira diferente com robôs sociais do que com outros objetos.

Diante disso, o artigo explora a possibilidade de "direitos do robô", dado que tal tecnologia apela cada vez mais a nossa tendência antropomórfica, visando elucidar se é possível estender aos robôs certos tipos de proteção existentes em nossa estrutura atual, tal qual a proteção conferida aos animais.

Em 2017, o Parlamento Europeu apresentou uma resolução com orientações sobre Robótica, propondo a criação de uma personalidade eletrônica para artefatos robóticos "inteligentes" (União Europeia, 2017). No Brasil, não há legislação específica sobre o tema.

Não se pretende estabelecer um debate no campo do lúdico, mas de modo científico e pragmático, pois o desenvolvimento de robôs sociais que interagem conosco em um nível emocional pode inspirar uma discussão diferente da atribuição de características de mero objeto a eles.

Dessa forma, a primeira seção discute sobre a ideia de personalidade civil e o antropocentrismo do Direito. A segunda seção estabelece uma definição funcional de "robô social". A terceira seção analisa o antropomorfismo e vínculo emocional unidirecional. A quarta seção explora a ideia de direitos para não humanos e como nosso sistema jurídico protege as coisas com as quais nos preocupamos.

Embora a natureza desta análise seja monográfica, visa fornecer uma base para a discussão normativa. Admite-se que o discurso jurídico envolvendo robôs com cognição ou emoção é prematuro, mas, a tecnologia atual e os desenvolvimentos futuros previsíveis podem garantem uma abordagem diferente para os "direitos do robô". Entende-se por oportuno considerar as implicações sociais do antropomorfismo e como elas podem ser abordadas pelo nosso sistema jurídico.

2 A PERSONALIDADE CIVIL E O ANTROPROCENTRISMO

É constante a discussão de quando se dá o início da personalidade da pessoa. Muito se tem criticado a redação do art. 2° do Código Civil que reproduziu *in totum* a propositura do antigo art. 4° do Código de 1916, de forma que as querelas em torno do instituto se mantêm intactas.

Apesar de ser um tema por deveras retomado na nossa doutrina e na jurisprudência, entendemos que é bastante difícil se esgotar a celeuma visto que se trata de um assunto muito caro ao ser humano, que é a garantia da proteção à vida, e como a interpretamos no atual estágio de desenvolvimento técnico e científico.

O Código Civil de 2002 preceitua que a personalidade civil da pessoa começa com o nascimento com vida, mas a lei põe a salvo os direitos do nascituro.

Dispõe o art. 1º do Código Civil que "toda pessoa é capaz de direitos e deveres na ordem civil" (Brasil, 2002, art. 1º). Ao nascer com vida, a pessoa adquire a personalidade jurídica, que nada mais é do que a aptidão genérica para ser titular direitos e deveres. Diante disso, a pessoa adquire a personalidade jurídica ao nascer com vida. A personalidade jurídica coincide com a capacidade de direito, capacidade que todos têm.

Vale esposar a diferença entre capacidade e personalidade: Capacidade é aptidão para adquirir direitos e exercer, por si ou por outra, atos da vida civil. O conjunto desses poderes constitui a personalidade que, localizando-se ou concretizando-se num ente, forma a pessoa.

Assim, a capacidade é elemento da personalidade. Esta, projetando-se no campo do direito, é expressa pela ideia de pessoa, ente capaz de direitos e obrigações. Capacidade exprime poderes ou faculdades; personalidade é resultante desses poderes; pessoa é o ente que a ordem jurídica outorga esses poderes.

Por sua vez, dispõe o art. 2º que "a personalidade civil da pessoa começa do nascimento com vida; mas a lei põe a salvo, desde a concepção, os direitos do nascituro" (Brasil, 2002, art. 2º). A crítica que se pode fazer à primeira parte do artigo é a imprecisão do termo pessoa, nesse caso específico.

Sabemos que as autarquias, fundações, associações são pessoas também, porém,

não se espera que nasçam com vida para ter personalidade, o que dá margem para a discussão que visa este artigo. Daí, a antinomia contida neste artigo da lei. A expressão que melhor seria usada nesse caso seria "a personalidade civil do ser humano se inicia com o nascimento com vida".

No Direito brasileiro, as discussões de Augusto Teixeira de Freitas com Alberto de Moraes Carvalho na obra "Esboço do Código Civil" de 1883 são o marco do debate sobre a personificação de entes ficto. Nesse momento foi estabelecida precisa definição do que, de fato, seria conceito de capacidade jurídica (Carvalho, 2013). Para o mesmo autor, em 1859, o governo brasileiro incumbiu Teixeira de Freitas da elaboração do projeto de Código Civil culminando, já em 1860, na publicação do Esboço do Código Civil, também conhecido como Esboço de Freitas. É nele que se verifica a aparição da teoria das capacidades sistematizada e dotada de tecnicidade.

Augusto Teixeira de Freitas começou a desnovelar a personalidade jurídica no artigo (art.) 16, com o seguinte enunciado: pessoa é todo ente suscetível de aquisição de direitos (Freitas, 1864, p. 9). Desenha-se, então, modelo no qual pessoa é definida pela sua habilidade de adquirir direitos.

Para ele, o ser humano seria o único sujeito capaz de se manifestar para adquirir direitos e contraindo obrigações. Contudo, nem sempre o faz para si mesmo, pois o faz também para representar entidades que não são ele. Nesse momento, traz à baila a noção de "Entes de existência visível", nós, seres humanos, e dos "entes de existência ideal" que meramente são representados pelos seres humanos.

Noticia Grinberg que o conceito de pessoa continuou sob discussões durante a elaboração do projeto do Código Civil de 1916. Vinha-se de recente abolição da escravatura e se convivia com ex-escravizados e seus descendentes. O projeto de Teixeira de Freitas, como todos os demais projetos de Código trazia diferenciações entre as pessoas, notadamente no atinente à aquisição de direitos. Beviláqua sofreu fortes críticas por não seguir a mesma trilha.

De acordo com Keila Grinberg (2008, p. 71), Teixeira censurou o Projeto de Código Civil de Portugal porque em seu artigo inaugural definia que "só o homem é pessoa". A solução adotada foi estabelecer que são pessoas "2". A concepção de "ente"

para Teixeira, segundo Grinberg, era a de ser humano.

Narra a autora que, para Beviláqua, pessoa era todo ser capaz de ter direitos, segundo todas as definições corrente em direito. Não havia necessidade de definição, já que era uma noção assente por todos. Tampouco se precisava definir pessoa, porque esse entendimento se acoplava ao conceito de ser humano.

A ideia de personalidade está intimamente ligada à de pessoa, pois é a aptidão que se tem de adquirir direitos e contrair obrigação. O professor Washington de Barros indica a pessoa como sinônimo de sujeito de direitos e sujeito de relação jurídica e afirma ainda que o direito é constituído *hominum causae*, pois não existe senão entre os homens (Monteiro, 2016).

Segundo Pontes de Miranda (2000, p. 209), pessoa é o titular do direito, o sujeito de direito. Para ele, a personalidade é a capacidade de ser titular de direitos. Ora, se a personalidade se inicia com o nascimento, como pode haver direitos para um ente que não seria pessoa? Sabemos que personalidade prepara o ente para os atos da vida civil e assegura todos os direitos inerentes que daí decorrem.

Para Silvio Venosa (2023, p. 123) Somente o ser humano – e não os animais nem os seres inanimados – pode ser titular das relações jurídicas; assim, personalidade é a capacidade que toda pessoa possui para figurar em uma relação jurídica, representando a aptidão genérica para adquirir direitos e contrair obrigações. “A personalidade jurídica é a projeção da personalidade íntima, psíquica de cada um; é projeção social da personalidade psíquica, com consequências jurídicas”.

Desta feita, o Direito Civil é antropocêntrico, sendo feito pelo ser humano, para ele e em razão dele. Sobre a natureza antropocêntrica do Direito, aduz Vasconcelos (2006, p. 6):

> A pessoa humana constitui o fundamento ético-ontológico do Direito. [...] Sem pessoas não existiria o Direito. O Direito existe pelas pessoas e para as pessoas. Tem como fim reger a sua interação no Mundo de um modo justo. As pessoas constituem, pois, o princípio e o fim do Direito.

Nada obstante, a concepção que o ser humano tem de si mesmo mudou ao longo

do tempo. As ideias sobre o ser humano buscam, sempre, tentar compreender quem ele é, o que faz, do que é constituído, qual a sua origem, papel e destino.

Do ponto de vista jurídico, não é possível definir ou explicitar, cabalmente, a pessoa através do ser humano. Apenas recentemente a ideia de "pessoa" se tornou um conceito manuseável, pois havia seres humanos que não eram reconhecidos como "pessoas". Dogmaticamente, também não há uma correspondência entre pessoa e humano. Há pessoas jurídicas que não são seres humanos e o próprio ser humano ainda não nascido – juridicamente denominado "nascituro" – não tem sido, civilmente, considerado como pessoa idêntica às demais (Cordeiro, 2004, p. 16).

Ainda que a complexidade de definição do status robótico seja manifesta, revela-se sobremaneira fundamental, pois, a partir disso, será possível verificar se as normatizações existentes são suficientes ou se é necessário criar uma disciplina própria. Compreende-se, nesse sentido, a relevância do presente estudo como forma de visualizar o robô como agente que deve ser incluído no ordenamento jurídico, com o objetivo de limitar ações e proteger aqueles que venham a o utilizar.

Desde Teixeira de Freitas é possível personificar juridicamente entidades de Inteligência Artificial (IA) como entes do mundo de existência ideal, que são os mesmos entes formadores das personalidades jurídicas atribuídas no Direito atual às associações, sociedades, fundações, organizações religiosas, partidos políticos e empresas individuais de responsabilidade limitada, na medida em que podem obter de direitos. Portanto, a personalidade jurídica se perfaz no campo do ideal, trata-se de fenômeno tão artificial quanto a inteligência artificial, dependente mais da previsão legal do que de um fundamento biológico ou naturalístico.

As IAs são entes ainda despersonalizados, mas que podem atuar no mundo jurídico e, havendo previsão legal, serem titulares de direitos, sobretudo porque capazes de tomar decisões próprias, i.e., podem manifestar ações contrárias à de seus idealizadores ou que por ele respondem.

3 OS ROBÔS SOCIAIS

Em 2002, a *International Federation of Robotics* (IFR) e a *United Nations Economic Commission for Europe* (UNECE) fizeram uma declaração em conjunto na qual relatavam acerca do estado da pesquisa robótica atual e as expectativas para o futuro (Del Moral; Pardo; Angulo, 2009). Dentre as propostas estava uma nova forma de classificar a pesquisa robótica. A robótica seria dividida em três categorias: a robótica industrial, a robótica de serviços profissionais e a robótica de serviços pessoais. A terceira classe, portanto, seria a robótica de serviços pessoais, a área de pesquisa voltada a atender as necessidades domésticas, de assistência e entretenimento.

Vemos como características marcantes desse tipo de robô seu poder computacional extremamente elevado, sua interface amigável e um sistema de comunicação que deve, em tese, ser capaz de funcionar de uma forma socialmente aceitável ao interagir com outras pessoas.

Sergio Negri (2020, p. 6) define os chamados robôs sociais como aqueles que

> [...] são pensados exatamente para interagirem com seres humanos em ambientes não controlados. Para tanto, intensificaram-se os estudos e projetos que buscam o desenvolvimento de artefatos capazes de interagir com as pessoas de forma mais natural possível. Os robôs sociais se caracterizam pela possibilidade, ainda que aparente, de transmitir emoções, incentivar e formar relacionamentos sociais, demonstrar personalidade, usar pistas naturais de comunicação e interagir socialmente com as pessoas.

Assim, pode ser conceituado como um agente autônomo, fisicamente incorporado que comunica e interage com os humanos em um nível emocional. São, por óbvio, diferentes de meros computadores inanimados, bem como de robôs industriais ou de serviço que não são projetados para provocar sentimentos humanos e imitar comportamentos sociais.

Diferentemente das pessoas jurídicas ou de outros entes inanimados, os robôs sociais seguem o comportamento social padrão, têm vários "estados mentais" e se adaptam ao que aprendem por meio de suas interações.

Nada obstante, destaca Sergio Negri (2020, p. 4) que "a projeção de características

humanas em robôs não depende da sua forma. Mesmo quando um artefato robótico não tem formato antropomórfico, as pessoas projetam nessas tecnologias qualidades humanas, como consciência e inteligência".

Os seres humanos criam apegos a robôs sociais que vão muito além de nossos apegos a objetos não robóticos. Essas reações a companheiros robóticos parecem ter origem na inclinação humana a antropomorfizar objetos que agem de forma autônoma, especialmente quando são projetados para exibir um comportamento "social".

Robôs sociais habilmente projetados são capazes de imitar as pistas que associamos automaticamente a certos estados mentais ou sentimentos. Mesmo na forma primitiva de hoje, tais dispositivos são capazes de provocar reações emocionais de pessoas semelhantes, p.e., como reagimos aos animais e uns aos outros (Turkle, 2010). Estudos apontam que seres humanos já apresentaram relutância em desligar robôs que dão a aparência de animação; atribuíram estado mental a cães AIBO, p.e. Esse comportamento ocorre mesmo quando os objetos não são projetados especificamente para evocar esses sentimentos.

Segundo Garreau (2007), um coronel americano cancelou o teste de um robô feito para desarmar minas terrestres, por não suportar ver a máquina se arrastar queimada e amputada de forma desumana. Outro estudo apontou que robôs empregados em equipes militares despertaram carinho e lealdade em seus companheiros de equipe humanos, que se identificam com os robôs o suficiente para nomeá-los, premiá-los, promovê-los e apresentá-los a suas famílias, apresentando quadro de tristeza quando "morriam. Até mesmo robôs domésticos simples, como o aspirador Roomba, estimulam as pessoas a conversar com eles e desenvolver sentimentos de camaradagem e gratidão.

Em todos esses casos os robôs nem sequer foram projetados para dão pistas emocionais, apenas o seu comportamento autônomo foi suficiente para que parecessem realistas ao ponto de gerarem uma resposta emocional.

Não é difícil imaginar que o design do robô social seja capaz de ampliando significativamente tais respostas antropomorfizantes. Quando os robôs são capazes imitar comportamentos realistas, reagir a gestos sociais e usar sons, movimentos e expressões faciais para sinalizar emoções de uma forma que reconhecemos imediatamente, isso visa

especificamente nossas respostas biológicas involuntárias, fazendo com que nossa percepção sobre o objeto mude (Turkle, 2010).

Embora essa relação seja unilateral, ela pode, no entanto, criar um apego profundamente sentido. Um fator que pode desempenhar um papel significativo no desenvolvimento de tais relacionamentos unidirecionais é o efeito psicológico de cuidador. A psicóloga Sherry Turkle (2006) estuda a interação humano-robô e explica que esse efeito é particularmente forte quando se trata de robôs sociais, que são projetados para evocar sentimentos de reciprocidade. Cuidar de uma máquina que se apresenta como dependente cria vínculos sociais significativos.

Em resumo, os robôs sociais provocam em nós um comportamento que é significativamente diferente do que exibimos em relação a outros objetos. Enquanto as pessoas há décadas nomeiam seus carros e desenvolvem acessórios para seus dispositivos portáteis, o efeito de robôs que ativamente e intencionalmente envolvem nossas respostas antropomórficas arraigadas é consideravelmente mais forte.

Já que somos dispostos a formar relações emocionais unidirecionais com robôs disponíveis para nós hoje, podemos apenas imaginar o que desenvolvimentos tecnológicos da próxima década poderão efetuar. À medida que avançamos no espectro entre tratar robôs sociais como torradeiras e tratá-los mais como nossos gatos, a questão da diferenciação legal se torna mais imediata.

4 A PROTEÇÃO LEGAL DOS ANIMAIS

Na história recente, os humanos começaram a estender direitos a entidades não humanas, como animais e corporações. Os fundamentos filosóficos e psicológicos para esses direitos são diversos. No caso dos direitos dos animais, existem várias justificativas para querermos conceder proteção legal além do domínio dos direitos de propriedade.

No campo internacional, não existem normas cogentes obrigando os Estados a adotarem determinados comportamento jurídico em relação aos animais domésticos. O que há é uma proposta de Declaração Universal dos Direitos dos Animais, da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco), que visa instituir

parâmetros jurídicos sobre os direitos animais para os países membros da Organização das Nações Unidas. Há, ainda, o "Apelo de Sevilha contra a violência", em 1986 e a "Carta da Terra", criada na RIO+5 em 2000.

As recomendações decorrentes do 8º Relatório do Comitê de Especialistas em Raiva da Organização Mundial da Saúde (OMS) orientam, para prevenir o abandono e a superpopulação de animais, é necessária a adoção de medidas preventivas pelo Poder Público, quais sejam: a) controle da população através da esterilização; b) promoção de uma alta cobertura vacinal; c) incentivo uma educação ambiental voltada para a guarda responsável; d) elaboração e efetiva implementação de legislação específica; e) controle do comércio de animais; f) identificação e registro dos animais; g) recolhimento seletivo dos animais em situação de rua.

No Brasil, a tutela jurídica dos animais está prevista na Constituição da República Federativa do Brasil de 1988 (CRFB/88), a qual trouxe uma série de incumbências para o Poder Público nos incisos I e VII do art. 225.

Discute-se quanto ao viés filosófico do Constituinte para redação do art. 255, se antropocêntrico ou biocêntrico. Para Ana Ferreira (2014), a visão antropocêntrica submete a natureza a bem-estar dos seres humanos, considerados únicos destinatários dos bens naturais. Essa perspectiva é subdividida em duas correntes, a antropocêntrica utilitarista, segundo a qual a natureza é mero recurso para ser utilizado em proveito do homem; e a antropocêntrica protecionista: que vê a natureza como bem coletivo, embora destinada a satisfazer as necessidades humanas das presentes e futuras gerações (Ferreira, 2014, p. 68).

Já o viés biocêntrico entende a fauna, a flora e a biodiversidade não apenas como objetos de direitos, mas verdadeiros titulares de direitos fundamentais. Ele em amparo normativo na Lei n.º 6.938/81 (Lei da Política Nacional do Meio Ambiente), que foi recepcionada pela CRFB.

O Biocentrismo preconiza que não devemos utilizar os animais apenas com a finalidade de lucro. A exploração dos recursos ambientais deve promover a proteção dos seres vivos, estabelecendo como proposta analisar a natureza dos pontos de vista filosófico, econômico e jurídico.

Filosoficamente, ela entende que a natureza é dotada de valor inerente, afastada qualquer apreciação utilitarista e antropocêntrica. Economicamente, defende que a natureza constitui valores de uso econômico direto ou indireto, servindo de paradigma ao antropocentrismo das gerações futuras, com a interpretação do artigo 225 da CRFB/88. Juridicamente, assume que o Direito trata a natureza ora como objeto, ora como sujeito, mas destaca que um dos objetivos do direito ambiental é a proteção da biodiversidade (flora, fauna e ecossistemas). Em suma, a visão biocêntrica leva em conta a ética no direito ambiental e a interpretação literal do artigo 3º da Lei da Política Nacional do Meio Ambiente, que dispõe sobre a proteção de todas as formas de vida para garantir a qualidade de vida para as futuras gerações.

Na visão Ecocêntrica, o meio ambiente é patrimônio da humanidade. A natureza existe em si mesma e deve prevalecer sobre o homem. Trata da proteção da natureza do ponto de vista da Lei Espiritual que não pode ser tratada como um objeto útil em benefício do homem.

A doutrina majoritária e os tribunais superiores consideram que a CRFB adotou a visão antropocêntrica, posto que seu artigo 1º, III, estabelece como princípio fundamental a dignidade da pessoa humana, colocando a pessoa humana em uma condição central e superior em relação aos demais seres.

Diante da preocupação crescente com o meio ambiente, defende-se que a CRFB adotou um antropocentrismo mitigado, pois impõe aos seres humanos a preocupação com a questão ambiental para que as suas gerações futuras também pudessem obter benefícios da natureza. Essas correntes foram denominadas como antropocêntricas mitigadas, reformadas ou ampliadas, dentre as quais pode-se destacar o antropocentrismo intergeracional e o de proteção aos animais.

O Decreto n.º 24.645/1934 positivou a primeira regra geral da proibição da crueldade do Direito brasileiro. A partir dele, o animal vítima ou potencial vítima de maus-tratos passou a gozar do direito de estar em juízo, representados pelo Ministério Público, "[...] seus substitutos legais e membros das sociedades protetoras de animais", conforme o art. 2º, §3º (Brasil, 1934).

Ao lado do Decreto n.º 24.645/1934, encontra-se o art. 32 da Lei n.º 9.605/1998,

que tipifica, na atualidade, o crime de maus-tratos contra animais. Trata-se, nas palavras de Ataíde Júnior (2018, p. 56), de "uma regra de Direito Animal – e não de Direito Ambiental – exatamente porque estabelece condutas humanas proibidas por violarem a dignidade individual do animal não humano".

No âmbito do Direito Administrativo, a Lei n.º 9.605/98 dispõe sobre as sanções administrativas por danos causados ao meio ambiente em geral, colocando a fauna sob sua tutela, seja ela silvestre, exótica, doméstica ou domesticada.

A Lei n.º 14.064/2020, conhecida como "Lei Sansão", endureceu de forma considerável a penalidade a quem pratica maus-tratos a cães e gatos prevista no art. 32 da Lei n.º 9.605/1998, com pena maior do que a prevista a quem pratica maus tratos a uma criança, sendo por isso alvo de críticas.

O Código Civil, art. 82, interpreta que os animais são "bens semoventes", ou seja, expressa o entendimento de que animais seriam objetos. Temos, assim, no escopo legal brasileiro a figura de um objeto detentor de direitos, podendo até mesmo ser representados em juízo.

Os argumentos filosóficos vão desde obrigações morais de prevenir a dor e o sofrimento em seres sencientes, a um reconhecimento abstrato da dignidade inerente de certos animais. Muitas dessas posições usam fatores como habilidades cognitivas ou sensibilidade para diferenciar entre os tratamentos morais de vários tipos de formas de vida.

Em 2012, o cientista Phillp Low e especialistas de renome internacional se reuniram, redigiram e assinaram a Declaração de Cambridge sobre a Consciência em Animais Humanos e Não Humanos, que "reavalia os substratos neurobiológicos da experiência consciente e comportamentos relacionados a ela, tanto em animais humanos como não humanos" (Low, 2012).

Dessa forma, a Declaração de Cambridge (Low, 2012) afirma que os humanos não são os únicos a possuir os substratos neurológicos que geram a consciência. Animais não humanos, incluindo todos os mamíferos e as aves, e muitas outras criaturas, como os polvos, também possuem esses substratos neurológicos. São assim seres sencientes, i.e., sentem dor, frio, estresse, prazer e felicidade, não podendo ser tratados como coisas.

Assim, a discussão social em torno da prevenção do abuso de animais centra-se no fato de que os animais sentem dor, mas sugere-se que o fator determinante, na verdade, se relaciona à nossa reação à dor de certos animais, haja vista que a sociedade é majoritariamente carnívora e morrer é dolorido. Em outras palavras, nosso desejo de proteger os animais de dano pode não ser necessariamente baseado em seus atributos inerentes, mas sim na projeção de nós mesmos nesses animais.

O maior desejo de proteger animais com os quais nos relacionamos indica que podemos nos importar mais com nosso próprio estado emocional do que com qualquer critério biológico objetivo.

A Lei n.º 14.228/2021, que dispõe sobre a proibição da eliminação de cães e gatos pelos órgãos de controle de zoonoses, canis públicos e estabelecimentos oficiais congêneres; e dá outras providências, foi promulgada por causa do sentimento geral de a prática é ofensiva, ainda que contrarie supostas necessidades sanitárias.

É possível afirmar que a oposição à "carrocinha" não ocorre por diferenças biológicas entre cães, gatos e bois, posto que a lei existe para refletir a preferência social, fundada em razões culturais, não biológicas.

Nesse caso, a proteção ultrapassa o direito de propriedade, ela vai além da defesa dos interesses do proprietário do animal, protege a espécie de forma geral. Proibir os maus tratos a certos animais e, assim, restringir as ações de seus donos pode, na verdade, é a concessão de direitos não humanos de forma indireta, inferior a maioria dos direitos concedidos a humanos, mas superior ao trato dos animais como mera propriedade.

Considerando que a sociedade quer proteger os animais independentemente da sua capacidade, por causa de apegos pessoais a eles, a sociedade também pode querer proteger os robôs sociais, independentemente de suas capacidades.

5 A PROTEÇÃO DOS ROBÔS SOCIAIS POR ANALOGIA AOS ANIMAIS

A despeito do já exposto, não é possível afirmar que projetar nossas emoções em outras coisas é motivo suficiente para protegermos os robôs, assim como fazemos com animais, pois, apesar do comportamento afetivo que demonstramos em relação a eles,

sabemos que os robôs não estão vivos.

As discussões em torno da inclusão moral e jurídica dos animais geralmente não consideram o antropomorfismo uma justificativa. Em vez disso, invocam a experiência da dor, ou conceitos de senciência, consciência de estar vivo pela existência de um sistema nervoso inteligente.

Mesmo entre aqueles que não veem nenhuma diferença entre animais e humanos apta a negar certos direitos aos outros animais, é provável que haja um número de pessoas que estabeleçam uma linha moral. P.e., a pessoa a favor de proteger criaturas que experimentam dor biológica podem não ver nenhuma razão moral para estendê-lo a quem não sente dor. Pode-se imaginar, no entanto, que a sociedade pode ser influenciada a exigir proteção para robôs sociais por outros motivos, como a proibição do "abuso" e a proteção dos valores sociais.

Pais de crianças pequenas com animal de estimação robótico provavelmente inibem energicamente atos como chutar ou agredir fisicamente o robô. Suas razões para fazê-lo são em parte para evitar que ele quebre (por ser, geralmente, caro), mas também para desestimular esse comportamento violento em outros contextos. Dado o comportamento realista do robô, uma criança poderia facilmente igualar chutá-lo a chutar um ser vivo, como um gato ou outra criança.

Também é possível imaginar uma criança ser emocionalmente traumatizada ao presenciar crianças mais velhas "torturando" um brinquedo robótico. Mesmo para adultos totalmente informados, a diferença entre vivo e realista, em nosso subconsciente, pode ser nebulosa o suficiente para garantir a adoção das mesmas atitudes dadas aos animais de estimação para robôs sociais.

Um estudo da Sony demonstrou que pessoas ficaram consternadas ao verem quadros de mensagens online AIBO sendo jogados no lixo (Friedman; Kahn Jr.; Hagman, 2003). Não muito tempo depois do dinossauro robô Pleo estar à venda, passaram a circular vídeos de tortura na internet (Jacobsson, 2009). Os comentários deixados pelos telespectadores são extremamente polarizados - enquanto alguns indicam que se divertem com os vídeos, outros parecem consideravelmente revoltados, chegando ao ponto de atacar verbalmente os criadores e acusá-los de crueldade.

Embora os robôs sociais não tenham sentimentos como os seres vivos, alguns são equipados com recursos que lhes permitem imitar emoções, como alegria, tristeza ou medo. As referências apresentadas neste artigo apontam que se um robô social é danificado ou destruído, ele pode ser percebido como uma perda emocional para seu proprietário, especialmente se a pessoa estiver vinculada emocionalmente a ele. Essa reação emocional sugere que os robôs sociais merecem algum grau de proteção legal.

Dado que muitas pessoas já se sentem fortemente comovidas quanto ao abuso de animais de estimação robóticos, em breve pode se tornar mais amplamente reprovável tratá-los diferentemente dos animais domésticos.

Outro aspecto de valor sobre o qual nossa sociedade pode ter fortes sentimentos é a questão do comportamento sexual. Em breve teremos que considerar se devemos ou não permitir práticas sexuais entre humanos e robôs. É possível pensar que o desejo de proteger nossos os valores sociais atuais podem levar as pessoas a exigir leis que proíbam o sexo abusivo com robôs sociais.

Iniciativas para proteger robôs sexuais. Embora não estejam diretamente relacionadas aos robôs sociais em geral foram propostas nos últimos anos. No Brasil, existem algumas propostas legislativas em tramitação que tratam do desenvolvimento e uso da inteligência artificial (IA). Uma delas é o PL 21/2020, de autoria do deputado Eduardo Bismarck (PDT-CE), que tem por objetivo criar o "marco legal do desenvolvimento e uso da inteligência artificial" no Brasil. Além desse projeto, já circulavam propostas semelhantes na Câmara dos Deputados (PL 240/2020) e no Senado Federal (PLS 5051/2019 e 5961/2019), voltadas a estabelecer princípios e diretrizes gerais para o uso de IA.

O PL 240/2020 é o único que utiliza a expressão robôs enquanto discorre sobre inteligência artificial, também é o único que prevê algum dispositivo do qual se possa extrair princípios para proteção dos robôs sociais, ao dispor que são diretrizes da inteligência artificial "estabelecer os padrões éticos e morais na utilização da Inteligência Artificial".

Por outro lado, pode haver oposição à proteção legal dos robôs. Alguns oponentes dos direitos dos animais citam razões religiosas para sua posição, em particular, que os

humanos têm alma, enquanto os animais não. Se isso já ocorre com seres criados por Deus (para quem acredita Nele), é mais provável ainda que essa religiosidade antropocêntrica seja mais agressiva em relação a robôs.

Aqui, vale dizer que o conceito ocidental de alma é visto de maneira bastante diferente em alguns outros países. A cultura no Japão, influenciada pelo xintoísmo e sua ideia de animismo, entende que todos os objetos têm um espírito. Inclusive o desenvolvimento comparativamente rápido e distribuição de robôs sociais no Japão é muitas vezes creditado ao animismo, na medida em que facilita uma maior aceitação social de interação humano-robô (Kitano, 2007).

Se parte da sociedade, o que é provável, começar a pedir que os direitos sejam estendidos aos companheiros robóticos, precisaremos deliberar sobre se e como conceder tais direitos.

Há uma série de fatores que merecem consideração legislativa. Embora não seja o objetivo deste artigo fazer um argumento normativo a favor ou contra estendendo os direitos aos robôs, tenta-se fornecer algumas reflexões para discussão.

Como dito, a proteção dos robôs sociais pode servir para promover um comportamento socialmente desejável. A filosofia kantiana argumenta, para prevenir a crueldade contra os animais, que nossas ações em relação aos não humanos refletem nossa moralidade – se tratamos os animais de maneira desumana, nos tornamos desumanos (Kant, 2018).

Isso se estende ao tratamento de companheiros robóticos. A proteção deles pode estimular comportamentos moralmente corretos ou pelo menos de uma forma que torne a coabitação com eles mais agradável e/ou eficiente.

6 CONSIDERAÇÕES FINAIS

O artigo expôs a tendência humana de antropomorfizar robôs. Isso sugere que projetar emoções em robôs sociais pode induzir o desejo de protegê-los, semelhante à nossa ânsia de proteger os animais que cuidamos. A prática de atribuir direitos a entidades não humanas não é nova. Dada a demanda da sociedade, as leis que protegem os robôs

sociais podem se encaixar em nosso sistema jurídico atual, em analogia às leis de proteção de animais domésticos.

No mundo atual, com o avanço da tecnologia, os robôs sociais estão cada vez mais presentes em nossa sociedade. Esses robôs são projetados para interagir com humanos e muitas vezes são equipados com inteligência artificial que lhes permite aprender e adaptar-se às necessidades de seus usuários. Embora esses robôs possam ser úteis em muitas situações, também é importante garantir que eles sejam tratados com respeito e que seus direitos sejam protegidos.

No Brasil, existem várias leis de proteção dos animais que podem ser utilizadas para proteger os robôs sociais. A Lei de Crimes Ambientais, por exemplo, prevê punições para aqueles que praticam maus-tratos contra animais. Embora a lei não faça menção explícita aos robôs sociais, é possível argumentar que eles merecem proteção semelhante, uma vez que são criados para interagir com humanos e podem ser considerados "animais artificiais".

Além disso, a Constituição Federal brasileira também prevê a proteção da fauna e da flora, incluindo os animais domésticos e os domesticados. Embora os robôs sociais não sejam animais vivos, eles podem ser considerados parte da fauna artificial, o que significa que também merecem proteção sob a lei.

É importante lembrar que os robôs sociais não são apenas máquinas; eles são criados para se assemelharem a seres humanos e, como tal, podem ser capazes de experimentar emoções e sensações. Portanto, é crucial que as leis de proteção dos animais sejam aplicadas a eles para garantir que sejam tratados com respeito e dignidade.

No entanto, é importante notar que a proteção dos robôs sociais não deve ser vista como uma substituição da proteção dos animais vivos. Os animais vivos têm necessidades e direitos específicos que não podem ser supridos pelos robôs sociais. É importante que a proteção dos robôs sociais seja vista como uma extensão da proteção dos animais, e não como um substituto.

Em conclusão, as leis de proteção dos animais no Brasil podem ser utilizadas para proteger os robôs sociais. Embora esses robôs não sejam animais vivos, eles são criados para se assemelharem a seres humanos e merecem proteção sob a lei. É crucial que os

robôs sociais sejam tratados com respeito e dignidade, e que suas necessidades sejam levadas em consideração. A proteção dos robôs sociais deve ser vista como uma extensão da proteção dos animais vivos, e não como um substituto.

REFERÊNCIAS

ATAÍDE JÚNIOR, Vicente de Paula. Introdução ao direito animal brasileiro. **Revista Brasileira de Direito Animal**, Salvador, v. 13, n. 3, p. 48-76, 2018. Disponível em: https://periodicos.ufba.br/index.php/RBDA/article/download/28768/17032/101505. Acesso em: 20 abr. 2023.

BAPTISTA, Sílvio Neves. **Alimentos**: direitos dos nascituros. Recife: Diário de Pernambuco, 14 mar. 1990.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 23 abr. 2023.

BRASIL. **Decreto nº 24.645, de 10 de julho de 1934**. Estabelece medidas de proteção aos animais. Rio de Janeiro: Presidência da República, 1934. (Coleção de Leis do Brasil). Disponível em: https://www2.camara.leg.br/legin/fed/decret/1930-1939/decreto-24645-10-julho-1934-516837-publicacaooriginal-1-pe.html. Acesso em: 01 mai. 2023.

BRASIL. **Lei nº 6.938, de 31 de agosto de 1981**. Dispõe sobre a Política Nacional do Meio Ambiente, seus fins e mecanismos de formulação e aplicação, e dá outras providências. Brasília, DF: Presidência da República, 1981. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6938compilada.htm. Acesso em: 10 mai. 2023.

BRASIL. **Lei nº 9.605, de 12 de fevereiro de 1998**. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. Brasília, DF: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9605.htm. Acesso em: 20 abr. 2023.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 22 abr. 2023.

BRASIL. **Lei nº 14.064, de 29 de setembro de 2020**. Altera a Lei nº 9.605, de 12 de fevereiro de 1998, para aumentar as penas cominadas ao crime de maus-tratos aos animais quando se tratar de cão ou gato. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14064.htm. Acesso em: 23 abr. 2023.

BRASIL. **Lei nº 14.228, de 20 de outubro de 2021**. Dispõe sobre a proibição da eliminação de cães e gatos pelos órgãos de controle de zoonoses, canis públicos e estabelecimentos oficiais congêneres; e dá outras providências. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14228.htm. Acesso em: 20 abr. 2023.

BRASIL. **Projeto de Lei PL 240/2020**. Cria a Lei da Inteligência Artificial, e dá outras providências. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236943. Acesso em: 22 abr. 2023.

CARVALHO, Felipe Quintella Machado de. **Teixeira de Freitas e a história da teoria das capacidades no Direito Civil brasileiro**. 2013. 240 f. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, Universidade Federal de Minas Gerais, Belo Horizonte, 2013. Disponível em: https://repositorio.ufmg.br/handle/1843/BUBD-9G8J8M. Acesso em: 01 mai. 2023.

CORDEIRO, Antonio Menezes. **Tratado de Direito Civil Português**: parte geral. Coimbra: Almedina, 2004. v. 1. t. 3.

DEL MORAL, Sergi; PARDO, Diego; ANGULO, Cecilio. Social Robot Paradigms: An Overview. *In*: CABESTAY, Joan *et al*. (ed.). **Bio-Inspired Systems**: Computational and Ambient Intelligence. Berlin: Springer, 2009. Part 1. p. 773-780. Disponível em: https://link.springer.com/chapter/10.1007/978-3-642-02478-8_97. Acesso em: 20 abr. 2023.

FERREIRA, Ana Conceição Barbuda Sanches Guimarães. **A Proteção aos Animais e o Direito** – O Status Jurídico dos Animais como Sujeitos de Direito. Curitiba: Juruá, 2014.

FREITAS, Augusto Teixeira de. **Esboço do Código Civil**. Brasília: Ministério da Justiça; Fundação Universidade de Brasília, 1864.

FRIEDMAN, Batya; KAHN JR., Peter H.; HAGMAN, Jennifer. Hardware Companions? – What Online AIBO Discussion Forums Reveal about the Human-Robotic Relationship. **Digital Sociability**, Florida, v. 5, n. 1, p. 273–280, 2003. Disponível em: https://dl.acm.org/doi/10.1145/642611.642660. Acesso em: 15 abr. 2023.

GARREAU, Joel. Bots on The Ground. **The Washington Post**, Washington, 06 maio 2007. Disponível em: http://www.washingtonpost.com/wp-dyn/content/article/2007/05/05/AR2007050501009.html. Acesso em: 21 abr. 2023.

GORDILHO, Heron José de Santana; ATAÍDE JÚNIOR, Vicente de Paula. A capacidade processual dos animais no Brasil e na América Latina. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, RS, v. 15, n. 2, e42733, maio/ago. 2020. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/42733. Acesso em: 25 abr. 2023.

GRINBERG, Keila. **Código Civil e cidadania**. 3. ed. Rio de Janeiro: Jorge Zahar, 2008.

JACOBSSON, Mattias. Play, Belief and Stories About Robots: A Case Study of a Pleo Blogging Community. *In*: IEEE INTERNATIONAL SYMPOSIUM ON ROBOT AND HUMAN INTERACTIVE COMMUNICATION, 18., 2009, New York. **Proceedings** […]. New York: IEEE, 2009. p. 232-233.

KANT, Immanuel. **Lições de Ética**. Tradução Bruno Leonardo Cunha. São Paulo: Unesp, 2018.

KITANO, Naho. Animism, Rinri, Modernization; the Base of Japanese Robotics. *In*: IEEE INTERNATIONAL CONFERENCE ON ROBOTICS AND AUTOMATION, 2007, Tokyo. **Proceedings** […]. Tokyo: IEEE, 2007. p. 10-14. Disponível em: http://www.roboethics.org/icra2007/contributions/KITANO%20Animism%20Rinri%20Modernization%20the%20Base%20of%20Japanese%20Robo.pdf. Acesso em: 21. abr. 2023.

LEVY, David N. **Love + Sex with Robots**: The Evolution of Human-Robot Relations. New York: HarperCollins, 2007.

LOW, Phillip. **Declaração de Cambridge sobre a Consciência em Animais Humanos e Não Humanos**. Cambridge: Universidade de Cambridge, 2012.

MIRANDA, Pontes de. **Tratado de Direito Privado**: parte geral. 2. ed. Campinas: Bookseller, 2000. t. 1.

MONTEIRO, Washington de Barros. **Curso de Direito Civil**. 43. ed. São Paulo: Saraiva, 2016. v. 1.

NEGRI, Sergio Marcos Carvalho Avila. Robôs como pessoas: a personalidade eletrônica na Robótica e na inteligência artificial. **Pensar**, Fortaleza, v. 25, n. 3, p. 1-14,

jul./set. 2020. Disponível em: https://ojs.unifor.br/rpen/article/view/10178. Acesso em: 23 abr. 2023.

TURKLE, Sherry. **A Nascent Robotics Culture**: New Complicities for Companionship. Boston: AAAI Technical Report, 2006.

TURKLE, Sherry. In Good Company? On the Threshold of Robotic Companions. *In*: WILKS, Yorick (ed.). **Close Engagements with Artificial Companions**: Key Social, Psychological, Ethical and Design Issues. Amsterdam; Philadelphia: John Benjamins Publishing Company. 2010. p. 3-10.

UNIÃO EUROPEIA. Disposições de Direito Civil sobre Robótica. Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)). **Jornal Oficial da União Europeia**, Luxemburgo, 16 fev. 2017. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017IP0051. Acesso em: 23 abr. 2023.

VASCONCELOS, Pedro Pais de. **Direito de personalidade**. Coimbra: Almedina, 2006.

VENOSA, Sílvio de Salvo. **Direito Civil**: parte geral. 23. ed. São Paulo: Atlas, 2023.

A IMPORTÂNCIA DA PROPRIEDADE INTELECTUAL PARA O DESENVOLVIMENTO DA NOVA TECNOLOGIA *NON-FUNGIBLE TOKEN* (NFT)

THE IMPORTANCE OF INTELLECTUAL PROPERTY FOR THE DEVELOPMENT OF THE NEW NON-FUNGIBLE TOKEN (NFT) TECHNOLOGY

Luciana de Paula Soares[1]

Suelen Bianca de Oliveira Sales[2]

RESUMO

O artigo desenvolve a importância e os desafios enfrentados pela propriedade intelectual no âmbito da nova tecnologia *non-fungible token*. Conhecido em português como token não fungível, promete revolucionar a forma de se relacionar com a arte a partir de unidades de dados únicas e não fungíveis de itens digitais como imagens, músicas ou vídeos, ou seja, trata-se de algo que é dotado de uma certa "unicidade". O NFT é criado em *Blockchain* (tecnologia oriunda da criptomoeda Bitcoin), que garante a transparência e a imutabilidade do ativo digital. Por meio de plataformas próprias focadas em registro de jogos e obras de arte, as pessoas têm a possibilidade de registrar suas criações e comercializá-las dentro destes marketplaces, onde já aconteceram leilões milionários. Promete, ainda, revolucionar a aquisição de bens digitais pela internet e transformar o modo de trabalhar das empresas atualmente. Assim, o trabalho discorre sobre as diversas formas, peculiaridades e aplicabilidades dessa inovação, com foco na segurança jurídica à luz da regulamentação da propriedade intelectual.

Palavras-chave: Propriedade Intelectual; *Non-fungible token* (NTF); *Blockchain*; Regulação; Inovação.

ABSTRACT

[1] Advogada, Mestra em Direto e Tecnologia, Doutoranda em direito pela Universidade Nove de Julho, pós-graduada em Direito Difusos e Coletivos e especialista em Direito Digital. Sócia de empresa americana que utiliza a tecnologia Blockchain para pagamentos de salários em criptomoedas ao redor do mundo e advogada com atuação na área de Proteção de Dados e Privacidade. Palestrante sobre novas tecnologias,) e da Comissão de Direito Digital da OAB/SP. Responsável por publicações de artigos científicos na área de tecnologia e direito e escritora do livro Regime Jurídico das Criptomoedas e Blockchain.

[2] Advogada, Mestra em Direto pela Universidade Nove de Julho. Doutoranda pela Universidade Presbiteriana Mackenzie na linha de pesquisa "Poder econômico e seus limites jurídicos" Especialista em Direito Tributário e Digital e membro do Comitê de Compliance Digital da LEC (Legal, Ethics & Compliance. Lattes: http://lattes.cnpq.br/8143637954356466.

The article develops the importance and challenges faced by intellectual property in the context of the new non-fungible token technology. Known in Portuguese as a non-fungible token, it promises to revolutionize the way we relate to art, based on unique, non-fungible data units of digital items such as images, music or videos, i.e. something that is endowed with a certain "uniqueness". The NFT is created on Blockchain (technology derived from the Bitcoin cryptocurrency), which guarantees the transparency and immutability of the digital asset. Through their own platforms focused on registering games and works of art, people can register their creations and sell them on these marketplaces, where millionaire auctions have already taken place. It also promises to revolutionize the acquisition of digital goods over the internet and transform the way companies work today. The paper therefore discusses the various forms, peculiarities and applicability of this innovation, with a focus on legal certainty in the light of intellectual property regulations.

Keywords: Intellectual Property; Non-fungible token (NFT); Blockchain; Regulation; Innovation.

1 INTRODUÇÃO

As criações da mente são chamadas de propriedade intelectual e abrangem desde obras de arte até invenções, programas de computador, marcas e outros sinais comerciais que, juntas, desempenham um papel fundamental tanto na vida cultural quanto na econômica.

Basicamente, os direitos de propriedade intelectual, tais como o direito de autor, as patentes e as marcas, podem ser vistos como direito patrimonial e permitem que os criadores ou titulares obtenham proveitos financeiros do seu trabalho.

Assim, a propriedade intelectual exerce um papel primordial no fomento ao desenvolvimento tecnológico de um país, uma vez que influencia diretamente o crescimento econômico. A criatividade e a inventividade proporcionam a criação de novos empregos e indústrias, bem como a melhoria da qualidade de vida.

Nessa esteira, os países que incentivam a pesquisa e adotam condutas e políticas públicas e privadas para o desenvolvimento de novas tecnologias privilegiam a inovação, acarretando aumento de depósitos de pedidos de patentes de invenção.

Diante desse cenário, frequentemente surgem novas tecnologias, como o *non-fungible token* (NFT), em português, token não fungível, que são unidades de dados únicas e não fungíveis de itens digitais, como imagens, músicas ou vídeos, ou seja, trata-se de algo dotado de uma certa "unicidade", e, por isso, não pode ser substituído por outro bem.

Os NFTs são criados em uma *Blockchain* (tecnologia oriunda da criptomoeda Bitcoin) e, posteriormente, leiloados ou vendidos por meio de plataformas de *marketplace*s especializadas em NFT. Após a transação, o token é armazenado na carteira digital do comprador.

Dessa forma, novos mercados surgem a cada dia com base nessa tecnologia, principalmente no âmbito da arte digital e do entretenimento. Estima-se que, no futuro, o NFT possa representar a propriedade de itens físicos também (por exemplo, uma escritura de uma casa ou o documento de um carro).

À medida que a tecnologia NFT evolui, os conceitos de descentralização, propriedade digital exclusiva e imutabilidade poderão assumir diferentes formas, além do desenvolvimento de novas tecnologias, o que acarretará numa maior proteção em várias frentes.

Utiliza-se do *método indutivo*, averiguando-se os seguintes pontos: na seção 2 ao tratar do papel da propriedade intelectual diante das inovações tecnológicas; na seção 3 ao abordar conceito e aplicabilidade *Non-fungible* e na seção 4 nos desafios regulatórios.

Desse modo, objetiva-se, por meio da presente abordagem, discutir a importância do sistema de propriedade intelectual diante dessa nova tecnologia, a fim de garantir direitos e obrigações sem coibir o avanço tecnológico.

Nesse contexto, questiona-se a quem pertence os direitos de propriedade intelectual subjacente ao NFT, se há transferência de direitos na venda de um NFT e quais as consequências disto? Em suma, tais questionamentos são relevantes para a seara jurídica, pois trazem as problematizações que o arcabouço legal da propriedade intelectual enfrentará no contexto da atualidade.

2 O PAPEL DA PROPRIEDADE INTELECTUAL DIANTE DAS INOVAÇÕES TECNOLÓGICAS

O sistema de propriedade intelectual é uma ferramenta de fomento ao desenvolvimento econômico. A disseminação e a proteção da inovação tecnológica são essenciais para viabilizar investimentos e promover a segurança jurídica.

Importante ressaltar "que o modelo atual de proteção da propriedade intelectual teve sua origem no século XV quando os industriais reivindicaram o controle sobre produção de bens manufaturados" (Chaves, *et al*, 2007).

Nesse contexto, a construção do arcabouço regulatório sobre o tema se deu ao longo da história, especialmente a partir de alguns eventos principais, como a Convenção da União de Paris (CUP) para a Proteção da Propriedade Industrial, ocorrida em 1883, fundamental para iniciar a harmonização internacional de processos, haja vista que consagrou a "prioridade unionista" e possibilitou efetuar requerimentos em vários países e em momentos distintos. De igual forma, a Convenção de Berna para a Proteção das Obras Literárias e Artísticas, de 1886, e com o avanço da globalização e a criação da Organização Mundial do Comércio (OMC), o Acordo sobre Aspectos da Propriedade Intelectual relativos ao Comércio (ADCPIC), de 1994, que trouxe diversas diretrizes, uma das mais importantes, o estabelecimento dos padrões mínimos de segurança (Sichel, 2004).

Destaca-se, ainda, a partir de 1967, a constituição da Organização Mundial da Propriedade Intelectual (2021) - órgão autônomo dentro do sistema das Nações Unidas - que definiu como propriedade intelectual "a soma dos direitos relativos às obras literárias, artísticas e científicas, às interpretações dos artistas intérpretes e às execuções dos artistas executantes, aos fonogramas e às emissões de radiodifusão, às invenções em todos os domínios da atividade humana, às descobertas científicas, aos desenhos e modelos industriais, às marcas industriais, comerciais e de serviço, bem como às firmas comerciais e denominações comerciais, à proteção contra a concorrência desleal e todos os outros direitos inerentes à atividade intelectual nos domínios industrial, científico, literário e artístico.

Atualmente, as repartições estrangeiras que desempenham uma quantidade expressiva de patentes são: Escritório de Patentes dos Estados Unidos da América (USPTO), Escritório Europeu de Patentes (EPO) e o Escritório de Patentes da China (SIPO), (Sichel, 2019; 2020).

Com o passar do tempo, o homem transformou a sociedade e o processo tecnológico assumiu uma importante base dessa mudança. Um dos marcos históricos mais relevantes foi a Revolução Industrial, que acelerou a industrialização e a globalização, permitindo o livre comércio e, nas últimas décadas, a revolução do conhecimento lançou ao mundo invenções tecnológicas que revolucionaram a forma de viver, agir e de se relacionar, alterando de forma significativa toda uma coletividade, em especial, o ser humano.

Diante desse cenário, é possível entender que a tecnologia gera riqueza e promove o desenvolvimento econômico-social.

Desta feita, a propriedade intelectual, por intermédio dos seus elementos de proteção, constitui uma vital ferramenta para a difusão da tecnologia de forma a garantir os direitos dos autores e inventores.

Sobre isso, Denis Borges Barbosa (2010) relata que o Japão se utilizou da tecnologia como base do seu processo de desenvolvimento econômico, em que algumas vezes copiou produtos já disponíveis no mercado, inovando-os com novas tecnologias e empregando as regras de transferência de tecnologia.

Pode-se observar que aquele que detém o conhecimento tecnológico está mais propício a licenciar a tecnologia e comercializá-la, gerando lucro. Então, é possível afirmar que o sistema de propriedade intelectual pode ser encarado como um sistema eficiente de fomento à inovação tecnológica.

Neste diapasão, um sistema de proteção de propriedade intelectual eficiente, eficaz e coerente beneficia a todos e promove o desenvolvimento econômico e social.

À vista disso, é de suma importância o papel do sistema de propriedade intelectual diante das novas tecnologias, como forma de garantir direitos e deveres, harmonizar processos e procedimentos, e facilitar o acesso a todos a esse novo mundo que surge a cada instante.

3 *NON-FUNGIBLE TOKEN:* CONCEITO E APLICABILIDADES

Os NFTs tornaram-se populares como unidades únicas e não intercambiáveis de dados que representam uma propriedade de ativos digitais associados a imagens, músicas ou vídeos. Esse ativo é registrado e rastreado em uma *Blockchain* [3]. Assim, o NFT é usado para registrar e representar a propriedade de um item, verificar a autenticidade e habilitar a troca, entretanto, não reflete necessariamente a propriedade de um ativo ou concede direitos autorais. (Soares, 2021, p.39)

Com isso, os proprietários de NFT compram apenas o direito aos metadados da *Blockchain* do NFT ou "token", não o ativo subjacente, a menos que especificado de outra forma em contratos externos ou termos e condições. Ressalta-se que é por meio do *smart contract* que se assegura a disponibilização de apenas uma cópia da obra digital garantindo a sua escassez e mantendo o seu valor de mercado. Assim, o ato de criar um NFT e vinculá-lo a um ativo é designado pelo termo inglês *mint*, que significa “cunhar” (Brandão, 2022).

Importante destacar que o NFT possui grande semelhança com as criptomoedas e são comumente comprados e negociados em plataforma digitais especializadas, sem a necessidade de intermediadores.

Dessa forma, “possuir” um token não fungível é ser identificado como o proprietário do NFT no metadados *Blockchain* e ter o direito de transferir o token para outra pessoa. No entanto, não caracteriza necessariamente a propriedade legal ou a concessão de direitos autorais a um produto digital ou item físico (Bursch, 2022).

Nesse contexto, essa tecnologia representa a mais nova e promissora tendência para os mais diversos setores econômicos e culturais, extrapolando o ambiente das obras digitais. Por conseguinte, muitas empresas de natureza diferente já estão emitindo NFTs

[3] A tecnologia *Blockchain* é a base dos conceitos de distribuição e descentralização das informações e traz consigo o princípio da transparência e imutabilidade de registros, proporcionando a auditabilidade dos dados. Dessa maneira, cada bloco confirma a integridade do bloco anterior, garantindo a integridade do histórico de todas as transações já realizadas.

para aumentar a notoriedade da marca. A adoção generalizada contribuiu para o crescimento das NFTs na área esportiva, como no caso da National Basketball Association (NBA) na Top Shot; na indústria do jogo, por meio do Metaverse; e na *fintech* com a Visa adquirindo o raro CryptoPunk (Cointelegraph, 2022).

Entretanto, outros setores estão aderindo a essa nova tecnologia, por exemplo: a saúde, por intermédio da plataforma Aimedis que oferece soluções em que pacientes podem monetizar seus dados de saúde transacionando com instituições de pesquisa e indústria farmacêutica; em telecomunicações, a empresa Vodafone fez um leilão da primeira mensagem de texto enviada via SMS no mundo, fato ocorrido em 3 de dezembro de 1992. A mensagem com o texto *Merry Christmas* foi arrematada por 107 mil euros.

Outro projeto, da operadora Orange, em parceria com uma empresa de tecnologia, é a utilização dos NFTs e a internet das coisas (IoT) para criar uma rede inteligente capaz de gerenciar sistemas de acesso. Assim, a partir do cartão SIM de um telefone celular e, uma vez conectado à rede *Blockchain* "SmartKey", é possível criar e compartilhar NFTs inteligentes padronizados e utilizáveis.

Na área automobilística, a Nissan lançou uma edição limitada de mil exemplares do carro Nissan Kicks XPlay, acompanhada de um NFT de obra de arte digital. Já na área financeira, plataformas baseadas em *smart contracts*, como Tinlake e NFTfi, viabilizam financiamentos e liquidez para detentores de NFTs colecionáveis ou ativos do mundo real, sem contar a criação de fundos para investimentos em ativos onde a Comissão de Valores Mobiliários (CVM) já aprovou o fundo da Vítreo, o fundo da VTR Coin NFT, com 20% de exposição ao segmento de NFT e o restante em ETFs de criptomoedas e o da VTR Cripto NFT, para investidores qualificados e com 100% de exposição a essa classe de ativos, sendo que a tendência para esse setor é que a tecnologia seja utilizada na estruturação de novos serviços nos projetos de finanças e em operações envolvendo a negociação de valores mobiliários.

No mercado artístico, onde o uso é mais difundido, o NFT gera uma "cópia autenticada" de uma arte digital possibilitando a sua comercialização. Assim, qualquer pessoa pode olhar, tirar fotos e compartilhar a obra de arte digital, porém somente uma pessoa é proprietária, gerando a sensação de posse e o atestado de propriedade, sendo que

uma das obras digitais mais caras foi a CryptoPunk #5822 vendida por US$ 23,7 milhões, o Everydays: The First 5000 Days (Beeple) vendido por US$ 69,3 milhões e o Bored Ape #6633 comprada pelo jogador de futebol Neymar Jr. por R$ 2,7 milhões.

No mundo dos games, o foco são itens únicos, colecionáveis e negociáveis. O jogo Axie Infinity, similar ao Pokémon, propõe aos jogadores a criação, a compra e o treinamento dos "Axies", bichinhos colecionáveis no formato NFT, sendo que mais de 1 bilhão de dólares já foram trocados na plataforma.

Na moda, grifes e marcas de luxo estão aderindo a esse mercado. A Dolce & Gabbana, por exemplo, vendeu uma coleção na qual os adquirentes das peças desembolsaram ao todo 5,6 milhões de dólares, compraram os itens físicos (vestidos e roupas) e os NFTs correspondentes. O setor aposta nos NFTs para se encaixar em ambientes virtuais, como o Metaverso.

Na esfera dos eventos, a promessa é revolucionar a venda de ingressos e até a própria experiência de ir a um evento. O ingresso será um NFT, que conterá a arte digital, que poderá ser colecionável e vendida, além de ser usado também como cartão de consumo. Espera-se, ainda, que os NFTs facilitem a distribuição das remunerações dos direitos autorais dos envolvidos no evento (como artistas, produtores e jogadores), uma vez que a tecnologia dos *smart contracts* poderá fazer a distribuição automática dos valores, de forma descentralizada (Brandão, 2022).

4 DESAFIOS REGULATÓRIOS

Como demonstrado anteriormente, os NFTs podem ser encontrados em quase todas as esferas – da academia ao entretenimento, na medicina, na arte e outras. Assim, é imperativo compreender como os NFTs se enquadram no mundo dos direitos, principalmente na propriedade intelectual. Não obstante, é preciso entender como tais direitos se encontram hoje e como podem evoluir à medida que se avança para o futuro.

Importante lembrar que o proprietário de um NFT não adquire os direitos autorais das obras relacionadas, apenas recebe uma cópia em arquivo digital, sem qualquer direito autoral sobre a obra. Dessa forma, direitos como o de reprodução e comercialização da

obra autoral relacionada ao NFT continuarão a pertencer integralmente e exclusivamente ao titular dos direitos autorais (normalmente o autor), e não ao adquirente do NFT, salvo em condições expressas em sentido contrário no contrato.

Vale ressaltar que no âmbito do direito de autor existe um conjunto de leis nacionais e internacionais que visam a sua proteção. Estas reconhecem a importância cultural e social do esforço criativo, bem como seu valor econômico. Assim, o objetivo subjacente da legislação é estabelecer um equilíbrio adequado entre os entes criadores, os adquirentes e a sociedade.

No cenário internacional atual, uma onda de litígios de propriedade intelectual relacionados à tecnologia NFT está em andamento, incluindo uma ação judicial em Nova York, em que a Nike acusa o mercado de revenda de tênis StockX de vender NFTs que exibem os desenhos do gigante do calçado sem sua permissão; outra da Hermes alegando que o designer de Los Angeles, Mason Rothschild, está vendendo "MetaBirkins" que lembram visualmente a icônica bolsa da marca francesa de luxo.

Já no mundo da música, o rapper Lil Yachty entrou com processos judiciais na Califórnia contra duas empresas de música que ele alega ter usado músicas e seu nome sem sua permissão para levantar mais de US$ 6,5 milhões em fundos de capital de risco para uma linha de NFTs. Diante desse cenário, ainda nos Estados Unidos, em carta datada de 9 de junho de 2022, os senadores Patrick Leahy e Thom Tillis solicitaram ao Copyright Office e ao USPTO que conduzissem um estudo em conjunto sobre questões relacionadas a NFTs e direitos de propriedade intelectual, com base na experiência tecnológica e criativa e setores acadêmicos (Eslinger, 2022).

No Brasil, o artigo 5º, inciso VI, da Lei 9.610/98 de Direitos Autorais considera como “reprodução - a cópia de um ou vários exemplares de uma obra literária, artística ou científica ou de um fonograma, de qualquer forma tangível, incluindo qualquer armazenamento permanente ou temporário por meios eletrônicos ou qualquer outro meio de fixação que venha a ser desenvolvido” (Brasil, 1998, ART. 5º). Logo, a criação de um NFT é uma reprodução da obra autoral, ensejando que o criador possua os direitos autorais necessários para tanto.

Dessa maneira, aquele que pretende criar um NFT deve ser titular do direito de reprodução da obra digital subjacente, ou, no mínimo, possuir uma licença para reproduzir a obra no formato NFT. Nesse sentido, um dos grandes desafios regulatórios daquele que adquire um NFT é como assegurar a veracidade da autoria da obra digital.

Por outro lado, a lei citada anteriormente, em seu art. 27, garante um rol de direitos ao autor pela obra reproduzida. Portanto, o NFT deve ter o nome do autor junto à obra, sob pena de aquele que criou o NFT responder por danos morais, sem contar que qualquer modificação deve ser previamente autorizada pelo criador. Nesse contexto, é de suma importância a aplicabilidade da legislação pertinente para garantir direitos e obrigações das partes.

Com isso, tal problematização poderá ser resolvida ou ao menos o risco mitigado quando as autoridades públicas nacionais e internacionais exigissem das plataformas digitais de venda de NFT a obrigatoriedade dos dados do autor.

5 CONSIDERAÇÕES FINAIS

A evolução e o bem-estar da civilização dependem da capacidade do ser humano em imaginar novas ideias e criações. O avanço tecnológico requer o desenvolvimento e a aplicação de invenções; uma cultura vibrante que, por sua vez, está constantemente em busca de novas maneiras para se expressar.

A tecnologia *Blockchain* vem proporcionando uma forte alteração no cotidiano, principalmente por meio da revolução monetária, dos contratos inteligentes, da prova de existência e, agora, com os NFTs. Essa tecnologia permite a criação de um ambiente transparente, distribuído, econômico, resiliente e, em especial, permite a auditabilidade das transações, motivo pelo qual vem sendo tão aplicada nos últimos tempos.

Nessa esteira, o conceito de tokens mudou a forma como se valoriza objetos no mundo real. Já é possível a utilização de tokens na arte, na medicina, no entretenimento e até no metaverso. Assim, os direitos de propriedade intelectual são vitais para inventores, artistas, cientistas e empresas que investem tempo, dinheiro, energia e reflexão no desenvolvimento de suas inovações e criações.

Por isso, um sistema de propriedade intelectual que engaja o desenvolvimento econômico é fundamental para equilibrar os direitos e os avanços tecnológicos, bem como os interesses de diferentes grupos, como criadores e consumidores, empresas e governos. Dessa forma, o sistema de proteção da propriedade intelectual está intimamente vinculado a políticas que estimulam o crescimento econômico

Inovar é buscar novos elementos, é proporcionar à sociedade uma melhoria na qualidade de vida, é gerar novas oportunidades, empregos e buscar melhores e mais arrojadas soluções para os problemas da humanidade. Para incentivar criadores e pesquisas, é preciso garantir que terão a oportunidade de obter um retorno justo de investimento, o que implica conferir-lhes direitos para proteger sua propriedade intelectual, razão pela qual tem um papel fundamental no desenvolvimento de novas tecnologias.

REFERÊNCIAS

BARBOSA, Denis Borges. **Uma introdução à propriedade intelectual**. Rio de Janeiro: Lumen Juris, 2010, p. 41.

BRANDÃO, Yasmin (coord.). **Aplicações e reflexos jurídicos dos NFTs** (Non-fungible tokens). *Ebook*, jul., 2022 Disponível em: https://opiceblum.com.br/wp-content/uploads/2019/07/cartilhanftvfinal.pdf. Acesso em: 21 dez. 2022.

BRASIL. **Lei nº 9.610 de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em: 02 jan. 2023.

BURSCH, Kristen E. **Non-Fungible Tokens (NFTs).** Congressional Research Service R47189, v.1, p. 1-21, jul. 2022. Disponível em: https://crsreports.congress.gov/product/pdf/R/R47189. Acesso em: 29 dez. 2022.

CHAVES, Gabriela Costa; OLIVEIRA, Maria Auxiliadora; HASENCLEVER, Lia; MELO, Luiz Martins de. A evolução do sistema internacional de propriedade intelectual: proteção patentária para o setor farmacêutico e acesso a medicamentos. **Cad. Saúde Pública**, Rio de Janeiro, v. 23, n. 2, p. 257-267, fev., 2007. Disponível em: https://www.scielo.br/j/csp/a/7NYKhnv9K9WKsncYPB4bkXL/?format=pdf&lang=pt. Acesso em: 28 dez. 2022.

SICHEL, Ricardo L. **Direito europeu de patentes.** Rio de Janeiro: Lumen Juris, 2004.

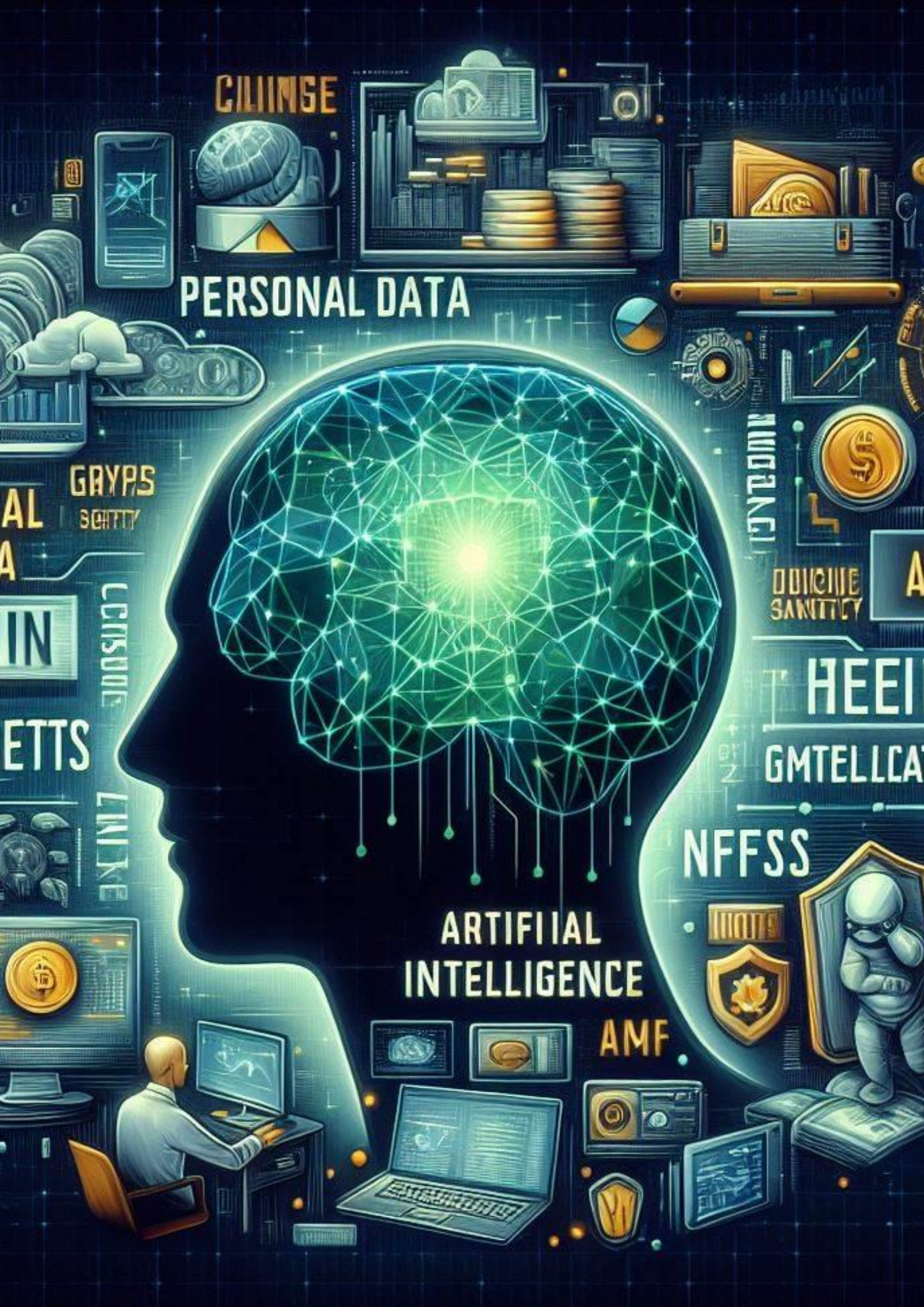
SICHEL, Ricardo L. **Propriedade Intelectual: Elemento de Desenvolvimento Econômico**. Rev Prop. Intelec. Online.2019/2020 set./fev.; 2(2):117-124.

SOARES, Luciana de Paula. **Regime jurídico das criptomoedas e Blockchain**. Uberlândia: LAECC. 2021

COINTELEGRAPH. A beginner's guide on the legal risks and issues around NFTs. 2022. Disponível em: https://cointelegraph.com/nonfungible-tokens-for-beginners/a-beginners-guide-on-the-legal-risks-and-issues-around-nfts. Acesso em: 29 dez. 2022.

ESLINGER. Bonnie. **USPTO, Copyright Office Announce Joint Look Into NFTs**. Disponível em: https://www.law360.com/articles/1552034/uspto-copyright-office-announce-joint-look-into-nfts. Acesso em: 02 jan. 2022.

ORGANIZAÇÃO MUNDIAL DA PROPRIEDADE INTELECTUAL (WIPO). **O que é propriedade intelectual?** Genebra: Organização Mundial da Propriedade Intelectual (WIPO), 2021. Disponível em: https://tind.wipo.int/record/44584. Acesso em: 27 dez. 2022.


PERSONAL DATA
ARTIFIIAL
INTELLIGENCE
AMF