XIII ENCONTRO INTERNACIONAL DO CONPEDI MONTEVIDÉU - URUGUAI

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS II

EDSON RICARDO SALEME

EUDES VITOR BEZERRA

CINTHIA OBLADEN DE ALMENDRA FREITAS

Copyright © 2024 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

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

Diretoria – CONPEDI
Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU – São Paulo
Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:
Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão
Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais
Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte
Prof. Dr. Fernando Passos – UNIARA - São Paulo
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná
Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia
Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal
Comunicação:
Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul
Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe
Relações Internacionais para o Continente Americano:
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão
Prof. Dr. Felipe Chiarello de Souza Pinto - UPM – São Paulo
Relações Internacionais para os demais Continentes:
Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará
Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul
Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI – Santa Catarina
Eventos:
Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo
Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina
Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UNICAP – Pernambuco

D597

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS II

[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Edson Ricardo Saleme, Eudes Vitor Bezerra, Cinthia Obladen de Almendra Freitas – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-85-5505-990-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: ESTADO DE DERECHO, INVESTIGACIÓN JURÍDICA E INNOVACIÓN

1. Direito – Estudo e ensino (Pós-graduação) – 2. Governo digital. 3. Novas tecnologias. XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU (2: 2024 : Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS II

Apresentação

O conjunto de pesquisas que são apresentadas neste livro faz parte do Grupo de Trabalho de "DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II", ocorrido no âmbito do XIII Encontro Internacional do CONPEDI, realizado entre os dias 18, 19 e 20 de setembro de 2024, na cidade de Montevidéu, Uruguai, promovido pelo Conselho Nacional de Pesquisa e Pós-Graduação em Direito – CONPEDI e que teve como temática central "Estado de Direito, Investigação Jurídica e Inovação".

Os trabalhos expostos e debatidos abordaram de forma geral distintas temáticas atinentes DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS, especialmente relacionadas aos principais desafios que permeiam a tecnologias jurídica, passando pela inteligência artificial, demais meios digitais, também apontando para problemas emergentes e propostas de soluções advindas de pesquisas em nível de pós-graduação, especialmente, Mestrado e Doutorado.

Os artigos apresentados no Uruguai trouxeram discussões sobre: Tecnologias aplicáveis aos tribunais, Governança digital e governo digital, Função notarial e novas tecnologias, Exclusão digital derivando tanto para exclusão social quanto para acesso à justiça, Eleições, desinformação e deepfake, cidades e TICs. Não poderiam faltar artigos sobre privacidade e proteção de dados pessoais, com atenção aos dados sensíveis, consentimento e LGPD, liberdade de expressão, censura em redes sociais, discriminação, herança digital, microtrabalho e o trabalho feminino, uso de sistemas de IA no Poder Judiciário e IA Generativa.

Destaca-se a relevância e artigos relacionados ao tema de Inteligência Artificial, tratando de vieses algorítmicos e do AI Act. E, ainda, aplicação de sistemas de IA ao suporte de pessoas com visão subnormal. Para além das apresentações dos artigos, as discussões durante o GT foram profícuas com troca de experiências e estudos futuros. Metodologicamente, os artigos buscaram observar fenômenos envolvendo Direito e Tecnologia, sem esquecer dos fundamentos teóricos e, ainda, trazendo aspectos atualíssimos relativos aos riscos que ladeiam as novas tecnologias, destacando os princípios e fundamentos dos direitos fundamentais

Considerando todas essas temáticas relevantes, não pode ser outro senão de satisfação o sentimento que nós coordenadores temos ao apresentar a presente obra. É necessário, igualmente, agradecer imensamente aos pesquisadores que estiveram envolvidos tanto na confecção dos trabalhos quanto nos excelentes debates proporcionados neste Grupo de Trabalho. Por fim, fica o reconhecimento ao CONPEDI pela organização e realização de mais um relevante evento internacional.

A expectativa é de que esta obra possa contribuir com a compreensão dos problemas do cenário contemporâneo, com o a esperança de que as leituras dessas pesquisas ajudem na reflexão do atual caminhar do DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS.

Prof. Dr. Edson Ricardo Saleme (UNISANTOS)

Prof. Dr. Eudes Vitor Bezerra (PPGDIR – UFMA)

Profª. Dra. Cinthia Obladen de Almendra Freitas (PPGD - PUCPR)

AI ACT

AI ACT

Luis Frederico De Medeiros Portolan Galvao Minnicelli
Renata Capriolli Zocatelli Queiroz
Daniel Zonzini Lattanzio

Resumo

O presente artigo tem por objetivo geral analisar o AI ACT (Artificial Intelligence Act) como um marco regulatório pioneiro na governança da IA na União Europeia, considerando seus objetivos, abrangência e mecanismos de aplicação, dado inclusive que em 13 de março de 2024 o plenário do Parlamento Europeu aprovou o projeto do AIACT, com eficácia após 24 meses. A metodologia adotada é de revisão bibliográfica abrangente sobre o AI ACT e questões relacionadas à governança da IA na UE, seguida de uma abordagem qualitativa para examinar criticamente as disposições do AI ACT e seu potencial impacto nos diversos setores da sociedade europeia. Os principais resultados obtidos permitem concluir que o AI ACT representa um avanço significativo na regulamentação da inteligência artificial na UE, com diretrizes éticas e foco na segurança e proteção dos direitos individuais. Os desafios associados ao AI ACT incluem a necessidade de uma implementação eficaz e coordenada entre os Estados membros e a importância de uma abordagem transnacional para lidar com os impactos da IA em escala global.

Palavras-chave: Ai act, União europeia, Regulamentação da ia, Capitalismo informacional, Proteção da dignidade e da privacidade

Abstract/Resumen/Résumé

The general objective of this article is to analyze the AI ACT (Artificial Intelligence Act) as a pioneering regulatory framework in the governance of AI in the European Union, considering its objectives, scope and application mechanisms, given that on March 13, 2024 the plenary of the European Parliament approved the AIACT project, effective after 24 months. The methodology adopted is a comprehensive literature review on the AI ACT and issues related to AI governance in the EU, followed by a qualitative approach to critically examine the provisions of the AI ACT and their potential impact on the different sectors of European society. The main results obtained allow us to conclude that the AI ACT represents a significant advance in the regulation of artificial intelligence in the EU, with ethical guidelines and a focus on security and protection of individual rights. Challenges associated with AI ACT include the need for effective and coordinated implementation among member states and the importance of a transnational approach to addressing the impacts of AI on a global scale.

Keywords/Palabras-claves/Mots-clés: Ai act, European union, Ai regulation, Informational capitalism, Protection of dignity and privacy

INTRODUÇÃO

O avanço exponencial da Inteligência Artificial (IA) tem revolucionado diversos setores da sociedade contemporânea, trazendo consigo inúmeras possibilidades e desafios. A Comissão Europeia propôs, em 21 de abril de 2021, um marco regulatório abrangente, denominado AI ACT, visando estabelecer diretrizes comuns para o uso ético e seguro da IA em todo o bloco.

A delimitação do tema abrange a análise das implicações do AI ACT no contexto europeu, considerando seus objetivos, alcance e impacto potencial sobre os direitos individuais, a economia e a inovação tecnológica na região. Nesse sentido, surge a problemática central: como garantir um ambiente regulatório eficaz para promover o desenvolvimento responsável da IA, protegendo os direitos fundamentais dos cidadãos europeus e fomentando a inovação e competitividade no mercado único da UE?

Diante dessa problemática, o objetivo geral deste estudo consiste em analisar o AI ACT como um marco regulatório pioneiro na governança da IA na UE, considerando seus objetivos, abrangência e mecanismos de aplicação. Os objetivos específicos são: investigar as origens e implicações do capitalismo informacional no surgimento do capitalismo de vigilância, adotando uma perspectiva fundamentada na Ciência da Informação; analisar a legislação brasileira e as normas internacionais de segurança da informação, com foco na proteção da dignidade e privacidade dos cidadãos, especialmente em meio às transformações da era digital, e comparar os avanços proporcionados pelo GDPR da UE e pela LGPD brasileira; avaliar o AI ACT como um marco regulatório inovador na governança da inteligência artificial na União Europeia, examinando seus objetivos, alcance e mecanismos de aplicação, bem como investigar os desafios e oportunidades associados à sua transnacionalidade e cronograma de implementação.

A justificativa para este estudo reside na relevância e urgência de compreender e avaliar o impacto do AI ACT no contexto europeu, dada a rápida evolução da IA e suas potenciais ramificações sociais, econômicas e éticas. Além disso, a análise crítica do AI ACT contribuirá para informar o debate público e a formulação de políticas relacionadas à IA não apenas na UE, mas também em outras jurisdições que buscam desenvolver suas próprias estratégias regulatórias para essa tecnologia emergente.

A metodologia adotada neste estudo compreenderá uma revisão bibliográfica abrangente sobre o AI ACT e as questões relacionadas à governança da IA na UE. Além disso, será empregada uma abordagem qualitativa para examinar criticamente as disposições do AI

ACT, sua coerência com os princípios éticos e direitos fundamentais e seu potencial impacto nos diversos setores da sociedade europeia. A análise crítica de conteúdo dos dados será realizada com base em documentos oficiais, estudos acadêmicos e relatórios especializados, visando proporcionar uma compreensão abrangente e aprofundada do tema em questão.

Visando proporcionar melhor compreensão dos resultados, optou-se pela seguinte estrutura: inicialmente, a pesquisa aborda questões fundamentais no contexto contemporâneo da sociedade da informação e da era digital, destacando a transição do capitalismo industrial para o capitalismo informacional e, mais recentemente, para o emergente capitalismo de vigilância. Por meio de uma análise embasada na perspectiva da Ciência da Informação, investiga-se como a coleta massiva de dados e a vigilância digital têm moldado as dinâmicas econômicas e sociais.

Feito isso, o estudo examina a legislação brasileira e as normas internacionais de segurança da informação, com foco na proteção da dignidade e da privacidade dos cidadãos. Destaca-se a importância da garantia da liberdade e privacidade na era digital e os avanços proporcionados pelo GDPR (Regulamento Geral de Proteção de Dados) na União Europeia e pela Lei Geral de Proteção de Dados (LGPD) no Brasil.

Por fim, o artigo analisa o marco regulatório da inteligência artificial (IA) na União Europeia, explorando tanto os avanços quanto os desafios enfrentados. Discute-se a questão dos riscos sistêmicos associados à IA, bem como os mecanismos de fiscalização e aplicação das normativas relacionadas à IA na UE. Adicionalmente, destaca-se a transnacionalidade do AI ACT (Ato de Inteligência Artificial) na UE, incluindo aspectos relacionados à preparação e ao cronograma de implementação dessa legislação pioneira na governança da IA.

1 CAPITALISMO INFORMACIONAL E O SURGIMENTO DO CAPITALISMO DE VIGILÂNCIA: UMA ANÁLISE NA PERSPECTIVA DA CIÊNCIA DA INFORMAÇÃO

O conceito de Capitalismo Informacional, como mencionado, emerge em um contexto marcado pela revolução da tecnologia da informação, que transformou significativamente a economia global. De acordo com Castells (1999), essa nova economia é caracterizada pela dependência da capacidade de gerar, processar e aplicar informações baseadas no conhecimento. Nesse sentido, a informação torna-se um recurso fundamental para o desenvolvimento econômico e social.

Na perspectiva da Ciência da Informação, a compreensão da informação como algo que reduz a incerteza no indivíduo é essencial. Afinal, é por meio da informação que ocorre a produção, interação, organização, representação e socialização do conhecimento (Caribé, 2019).

O surgimento do Capitalismo Informacional e Global, conforme descrito por Castells (1999), é resultado direto da revolução da tecnologia da informação. Nessa nova economia, o poder econômico está intrinsecamente ligado à capacidade de gerar, processar e aplicar informações de maneira eficaz. Esse contexto dá origem ao que hoje chamamos de Capitalismo de Vigilância.

O Capitalismo de Vigilância é uma forma específica de organização econômica e social em que as empresas coletam dados pessoais dos usuários para monetizá-los por meio de publicidade direcionada, personalização de serviços e manipulação comportamental. Essa prática, muitas vezes realizada sem o consentimento explícito dos usuários, levanta questões éticas e de privacidade (Koerner, 2021).

Empresas como Google, Facebook e Amazon são exemplos proeminentes de empresas que operam dentro do paradigma do Capitalismo de Vigilância. Elas acumulam enormes quantidades de dados sobre seus usuários e utilizam algoritmos sofisticados para analisar e manipular esse comportamento. Essa prática levanta questões sobre o poder dessas empresas e seu impacto na sociedade, incluindo questões de concentração de poder, desigualdade e democracia.

Portanto, o Capitalismo de Vigilância representa uma nova fase no desenvolvimento do Capitalismo Informacional, caracterizada pela exploração comercial dos dados pessoais dos usuários. Nesse contexto, é essencial refletir sobre os limites éticos e políticos dessa prática e buscar formas de regulamentação e controle que garantam a proteção dos direitos individuais e a integridade da sociedade como um todo (Caribé, 2019).

Para Zuboff (2020), o fenômeno do capitalismo de vigilância emerge como um aspecto intrínseco e muitas vezes invisível da sociedade contemporânea. Trata-se, pois, de uma nova fase do capitalismo, em que a coleta massiva de dados pessoais dos usuários é utilizada como uma ferramenta fundamental para gerar lucro. Conforme a autora, esse modelo econômico se baseia na vigilância constante dos comportamentos individuais na internet, visando à previsão de desejos e necessidades dos consumidores. Como resultado, os dados pessoais se tornam uma mercadoria valiosa, sendo explorados por empresas em busca de vantagem competitiva.

Um aspecto crucial do capitalismo de vigilância é a sua relação com a privacidade e os direitos individuais. O direito à privacidade é frequentemente sacrificado em prol do acesso

gratuito a serviços digitais, como aponta Zuboff (2020). Essa troca, na qual os usuários cedem seus dados em troca de conveniência e acesso à informação, levanta questões éticas sobre consentimento e transparência, tal como relatado pela autora.

Além disso, o capitalismo de vigilância está intrinsecamente ligado à desigualdade social e econômica. Como mencionado por Koerner (2021), a concentração de poder e riqueza nas mãos de poucas empresas de tecnologia reforça as disparidades existentes na sociedade. Segundo o autor, o acesso desigual à tecnologia e a exploração dos dados pessoais de grupos vulneráveis ampliam ainda mais essas disparidades, criando um ciclo de desigualdade difícil de ser quebrado.

Outro aspecto importante é a emergência de um novo paradigma econômico, como discutido por Castells (1999) em "A Sociedade em Rede". A ascensão do capitalismo informacional e a dependência cada vez maior da capacidade de processamento e aplicação eficaz da informação marcam uma mudança significativa na estrutura econômica global. Segundo Koerner (2021), o capitalismo de vigilância se encaixa nesse contexto, explorando a informação como uma mercadoria valiosa e promovendo uma nova forma de relação entre empresas e consumidores.

Entre os esforços em curso para regulamentar o capitalismo de vigilância e proteger os direitos dos usuários, destaca-se a implementação de legislações e políticas de proteção de dados, como a GDPR na União Europeia. Essas iniciativas representam um passo importante na busca por um equilíbrio entre inovação tecnológica e proteção dos direitos individuais, conforme apontado por Fornasier e Knebel (2020). Essas medidas refletem a crescente preocupação com a privacidade e a segurança dos dados pessoais, um tema que também ganha destaque na legislação brasileira e nas normas internacionais de segurança da informação.

No Brasil, a proteção da dignidade e da privacidade das pessoas é um princípio fundamental que permeia a legislação nacional, garantindo o respeito aos direitos individuais (Doneda, 2021). Além disso, normas como a ISO 27001 estabelecem padrões para a gestão de segurança da informação, contribuindo para a garantia da disponibilidade, confidencialidade e integridade dos dados (Doneda, 2021). Esse contexto legal e normativo reflete uma preocupação global crescente com a proteção dos dados pessoais na era digital, destacando a importância da regulamentação e da conscientização sobre esse tema, tal como se verá especificamente na seção seguinte.

2 A PROTEÇÃO DA DIGNIDADE E DA PRIVACIDADE NA LEGISLAÇÃO BRASILEIRA E NAS NORMAS INTERNACIONAIS DE SEGURANÇA DA INFORMAÇÃO

No Brasil, a dignidade da pessoa humana, consagrada como um dos fundamentos do Estado Brasileiro no artigo 1º, inciso III, da Constituição Federal Brasileira de 1988, é o princípio norteador que permeia a tutela efetiva dos direitos fundamentais estabelecidos na Carta Magna de 1988 (Gunther; Comar; Rodrigues, 2020). Esse princípio é intrinsecamente ligado à proteção da intimidade, vida privada, honra e imagem das pessoas, como estabelecido no artigo 5º, inciso X, da mesma Constituição, que garante o direito à indenização pelo dano decorrente de sua violação (Doneda, 2021).

O Código de Defesa do Consumidor, Lei 8.078/90, reforça essa proteção ao assegurar, em seu artigo 43, o acesso do consumidor às informações arquivadas sobre ele, evidenciando a importância da transparência e controle sobre dados pessoais. Tal disposição está em consonância com o direito constitucional à inviolabilidade da vida privada, estabelecido no artigo 5º, inciso LXXII, que prevê o habeas data como instrumento para garantir o acesso a informações pessoais constantes de registros ou bancos de dados (Doneda, 2021).

No âmbito civil, o Código Civil, em seu artigo 21, reforça a inviolabilidade da vida privada da pessoa natural, conferindo ao juiz a responsabilidade de adotar medidas para impedir ou cessar atos contrários a essa norma. Recentemente, o Supremo Tribunal Federal, em decisão sobre a ADI - Ação Direta de Inconstitucionalidade - 4815, reiterou a importância da proteção à privacidade ao declarar inexigível a autorização prévia para a publicação de biografias, em consonância com os direitos fundamentais à liberdade de expressão (Doneda, 2021).

Além da legislação nacional, normas internacionais como a ISO 27001 estabelecem padrões para a gestão de segurança da informação em empresas, garantindo a disponibilidade, confidencialidade e integridade dos dados. Uma organização certificada conforme a ISO 27001 demonstra seu compromisso em gerir as informações de forma segura, oferecendo garantias aos seus clientes e parceiros (Doneda, 2021).

Dessa forma, tanto no âmbito legal nacional quanto nas normas internacionais, a proteção da dignidade e da privacidade das pessoas é um princípio fundamental, que permeia a legislação e as práticas de segurança da informação, garantindo o respeito aos direitos individuais e a confiança na gestão de dados pessoais (Barbosa *et al*., 2021; Doneda, 2021).

2.1 A garantia da liberdade e privacidade na era digital

O Dia Internacional da Proteção de Dados, celebrado globalmente em 28 de janeiro, remonta à assinatura da Convenção do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, que foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. Mas foi apenas em 2006 que essa data foi formalmente reconhecida, marcando o compromisso com a defesa dos direitos individuais. Essa celebração destaca a importância da proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade, especialmente através da proteção de dados pessoais (Doneda, 2021).

A norma internacional ISO 27002, de gestão de segurança da informação, desempenha um papel crucial nesse contexto. Estabelecendo diretrizes e princípios para garantir a segurança da informação em organizações, a ISO 27002 orienta na seleção, implementação e gerenciamento de controles, assegurando a disponibilidade, confidencialidade e integridade dos dados. Empresas certificadas conforme a ISO 27002 demonstram um compromisso sério com a proteção da informação, transmitindo confiança ao mercado quanto à gestão segura de dados pessoais (Doneda, 2021).

Além disso, legislações como a Lei Carolina Dieckmann (Lei nº 12.737/2012) e o Marco Civil da Internet (Lei n° 12.965/2014) são importantes na defesa dos direitos digitais e na punição de crimes virtuais. A Lei Carolina Dieckmann, inspirada pelo caso da atriz que teve sua privacidade violada, tipifica e pune invasões de aparelhos eletrônicos para obtenção de dados pessoais. Já o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para os usuários da rede, bem como diretrizes para a atuação do Estado, garantindo uma internet livre, aberta e segura para todos (Gunther; Comar; Rodrigues, 2020).

Essas legislações refletem a necessidade crescente de proteger os direitos individuais no ambiente digital e reforçam a importância do Dia Internacional da Proteção de Dados como uma oportunidade para promover a conscientização sobre a privacidade e a segurança dos dados na era digital (Barbosa *et al*., 2021; Doneda, 2021).

2.2 GDPR e LGPD: avanços na proteção de dados pessoais

O *General Data Protection Regulation* (GDPR), tradução livre para Regulamento Geral sobre a Proteção de Dados, é uma das legislações mais abrangentes e impactantes no

campo da privacidade de dados pessoais. Iniciado pela União Europeia (UE) em 2012, o GDPR foi publicado em abril de 2016 e entrou em vigor em maio de 2018. Sua implementação representa um marco crucial na defesa dos direitos individuais, estabelecendo padrões rigorosos para o tratamento de dados pessoais e impactando não apenas os países membros da UE, mas também entidades que realizam transações comerciais com o bloco europeu (Gunther; Comar; Rodrigues, 2020; Doneda, 2021).

O GDPR estabelece uma série de direitos e obrigações tanto para empresas quanto para indivíduos, visando garantir a privacidade e a segurança dos dados pessoais em um cenário cada vez mais digitalizado. Além disso, sua influência vai além das fronteiras da UE, estimulando a adoção de práticas de proteção de dados em todo o mundo (Barbosa *et al*., 2021; Doneda, 2021).

No contexto brasileiro, a LGPD, promulgada em agosto de 2018, reflete uma tendência global em direção à proteção dos direitos individuais no ambiente digital (Gunther; Comar; Rodrigues, 2020). Inspirada pelo GDPR e pela necessidade de fortalecer a proteção de dados pessoais no Brasil, a LGPD busca fornecer às pessoas um maior controle sobre suas informações pessoais, estabelecendo regras claras para o tratamento de dados por parte das empresas e instituições (Barbosa *et al*., 2021; Doneda, 2021).

A relação entre o GDPR e a LGPD não se limita apenas às semelhanças em seus objetivos e princípios. A norma ISO/IEC 27701, por exemplo, pode ser vista como uma ferramenta que ajuda as organizações a se adequarem tanto ao GDPR quanto à LGPD, fornecendo diretrizes e requisitos para a gestão de informações de privacidade (Doneda, 2021).

A trajetória histórica da proteção de dados revela uma evolução gradual e constante na conscientização e regulamentação dessa área (Gunther; Comar; Rodrigues, 2020). Desde as legislações pioneiras na Europa na década de 1970 até os marcos legislativos mais recentes, como o GDPR e a LGPD, percebe-se um esforço contínuo para adaptar o direito à privacidade às mudanças tecnológicas e sociais (Doneda, 2021).

Diante desse panorama, é evidente a importância crescente da proteção de dados pessoais na sociedade contemporânea (Gunther; Comar; Rodrigues, 2020). Tanto o GDPR quanto a LGPD representam avanços significativos nesse sentido, fornecendo um arcabouço legal robusto para garantir a privacidade e a segurança dos dados em um mundo cada vez mais conectado e digital (Doneda, 2021).

3 MARCO REGULATÓRIO DA IA NA UE: AVANÇOS E DESAFIOS

A Carta de Direitos Fundamentais da UE garante uma série de prerrogativas essenciais, incluindo o direito à não discriminação, liberdade de expressão, dignidade humana, proteção de dados pessoais e privacidade. No entanto, o avanço descontrolado da Inteligência Artificial (IA) tem colocado em risco esses direitos fundamentais (Ebers *et al*., 2021; Oprea *et al*., 2022).

Para lidar com essa questão, a Comissão Europeia lançou, em 2019, as Diretrizes Éticas para IA Confiável e Recomendações de Política e Investimento, que são consideradas *soft law*, ou seja, não legalmente vinculativas para os Estados-membros. No mesmo ano, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) emitiu recomendações não vinculativas sobre o tema (Carter, 2020; Madiega, 2019; Oprea *et al*., 2022).

Em 2020, a Comissão Europeia assumiu o compromisso de promover a adoção da IA e abordar os riscos associados a determinados usos dessa tecnologia por meio do *White Paper on Artificial Intelligence*. Em 2021, a Unesco adotou Recomendações sobre a Ética da IA. Em abril do mesmo ano, a Comissão Europeia propôs a primeira estrutura regulatória da UE para IA, visando harmonizar a regulamentação no mercado único dos 27 Estados-membros (Carter, 2020; Oprea *et al*., 2022).

Em dezembro de 2023, um acordo foi estabelecido entre o Parlamento Europeu e o Conselho Europeu sobre o projeto do texto europeu para regulamentar o uso da IA generativa na UE. Em fevereiro de 2024, foi realizada a última atualização sobre o texto final do projeto da Lei de Inteligência Artificial da UE, aprovado pelos 27 Estados-membros, tornando-se a primeira estrutura jurídica horizontal abrangente do mundo para regulamentar sistemas de IA em toda a EU (Madiega, 2019).

Em 13 de março de 2024, o projeto foi aprovado no Parlamento Europeu. Essa aprovação representa um marco significativo na proteção dos direitos fundamentais em um contexto de rápida evolução tecnológica, e tem por propósito alcançar uma série de objetivos cruciais para garantir a segurança, proteção dos direitos fundamentais e promoção da inovação dentro do mercado único da UE (Cabrera; Mcgowan, 2024).

Em primeiro lugar, um dos principais objetivos do AI Act é assegurar que os sistemas de IA disponibilizados no mercado da UE sejam seguros e estejam em conformidade com a legislação em vigor. Isso implica estabelecer padrões rigorosos de segurança e conformidade para proteger os consumidores e usuários contra potenciais riscos associados à utilização desses sistemas. Além disso, a regulamentação busca proporcionar segurança jurídica para incentivar investimentos e inovação no campo da IA. Ao estabelecer regras claras e previsíveis, a intenção

é promover um ambiente favorável ao desenvolvimento e adoção de tecnologias de IA de forma ética e responsável (Oprea *et al*., 2022; Veale *et al*., 2021).

Outro objetivo essencial é fortalecer a governança e a aplicação efetiva da legislação da UE sobre direitos fundamentais no contexto da IA. Isso inclui garantir que os sistemas de IA não violem direitos como a privacidade, a não discriminação e a dignidade humana, promovendo assim uma abordagem ética no desenvolvimento e uso dessas tecnologias (Ebers *et al*., 2021).

Por fim, a regulamentação busca facilitar o desenvolvimento de um mercado único para aplicativos de IA legais e seguros, a fim de evitar a fragmentação e promover a interoperabilidade dentro do mercado europeu. Isso contribuiria para uma maior eficiência econômica e facilitaria a adoção generalizada de soluções de IA inovadoras em toda a UE (Veale *et al*., 2021).

Em sua essência, o projeto de regulamentação da IA busca criar um ambiente que promova a inovação tecnológica enquanto protege os direitos e interesses dos cidadãos europeus, garantindo ao mesmo tempo uma concorrência justa e um mercado único digital coeso e seguro. Ao alinhar-se com outras legislações digitais importantes da UE, como o GDPR e o *Digital Services Act* (DSA), busca-se garantir uma abordagem consistente e abrangente para regulamentar o espaço digital em toda a UE (Veale *et al*., 2021).

A abrangência do AI ACT se estende aos fornecedores, implementadores e importadores de sistemas de IA que são disponibilizados no mercado da UE ou que afetam pessoas físicas ou jurídicas dentro da EU (Cabrera; Mcgowan, 2024). No entanto, certas atividades, como pesquisa, desenvolvimento e criação de protótipos antes da comercialização, estão isentas das obrigações estabelecidas pelo regulamento, juntamente com algumas outras exceções (European Parliament, 2024).

Para garantir uma regulamentação proporcional ao risco, o projeto classifica os sistemas de IA com base em seu potencial de risco, com regulamentos mais rigorosos aplicados a sistemas de alto risco. Isso inclui sistemas que apresentam riscos significativos à saúde, segurança, direitos fundamentais, meio ambiente, democracia e Estado de Direito (Cabrera; Mcgowan, 2024).

Os fornecedores de sistemas de IA classificados como de alto risco devem realizar e documentar uma avaliação prévia da conformidade com diversos princípios, como transparência para os usuários. Além disso, esses sistemas estão sujeitos a obrigações claras, como a avaliação obrigatória do impacto sobre os direitos fundamentais e a garantia de direitos

dos cidadãos, incluindo o direito de apresentar reclamações e receber explicações sobre decisões baseadas em IA que afetem seus direitos (Ebers *et al*., 2021).

No entanto, algumas categorias de sistemas de IA são regulamentadas independentemente do nível de risco. Por exemplo, os projetistas de modelos de IA de uso geral, como *Large Language Models* (LLMs), devem fornecer documentação técnica para transparência e adotar protocolos que respeitem os direitos autorais durante o aprendizado, independentemente do risco envolvido. No entanto, isenções podem ser concedidas a modelos de código aberto, a menos que apresentem riscos sistêmicos (European Parliament, 2024).

3.1 Riscos sistêmicos

Os riscos sistêmicos relacionados aos modelos de IA referem-se a ameaças ou perigos que podem afetar não apenas um indivíduo ou uma organização, mas todo um sistema ou mercado. No contexto do AI ACT, esses riscos são cuidadosamente definidos e avaliados com base em diversos critérios detalhados no anexo IX do reguamento (Cabrera; Mcgowan, 2024; European Parliament, 2024).

Um dos critérios para determinar o risco sistêmico de um modelo de IA é o número de parâmetros do modelo. Quanto maior o número de parâmetros, maior a complexidade e, potencialmente, os riscos associados ao modelo. Além disso, a qualidade e o tamanho do conjunto de dados utilizados para treinar o modelo são considerados, uma vez que dados de baixa qualidade ou insuficientes podem levar a resultados imprecisos ou tendenciosos (Cabrera; Mcgowan, 2024; European Parliament, 2024).

A quantidade de computação necessária para treinar o modelo também é um fator crucial na avaliação dos riscos sistêmicos. Isso é medido em Flops (operações de ponto flutuante por segundo) ou por meio de uma combinação de outras variáveis relacionadas à capacidade de processamento do modelo (Cabrera; Mcgowan, 2024; European Parliament, 2024).

Outros aspectos considerados incluem as modalidades de entrada e saída do modelo, ou seja, como ele interage com o ambiente ao seu redor, e as referências e avaliações de suas capacidades. Um modelo de IA com alto impacto no mercado interno da UE, presumido quando disponibilizado a um grande número de usuários comerciais registrados na UE, também pode ser considerado de alto risco sistêmico (Cabrera; Mcgowan, 2024; European Parliament, 2024).

Em resumo, os riscos sistêmicos associados aos modelos de IA envolvem uma série de fatores, desde a complexidade e o tamanho do modelo até a qualidade dos dados e seu

impacto no mercado. Avaliar e mitigar esses riscos é essencial para garantir a segurança e a confiabilidade dos sistemas de IA em um contexto mais amplo (Cabrera; Mcgowan, 2024; European Parliament, 2024).

3.2 A fiscalização da IA na UE: normativas e aplicações

A regulamentação da IA na UE não se limita à definição de padrões de segurança e ética, mas estende-se também ao estabelecimento de mecanismos de fiscalização e punição para garantir o cumprimento das normativas estabelecidas (Cabrera; Mcgowan, 2024; Veale *et al*., 2021).

Em nível nacional, cada Estado-membro da UE deverá designar uma autoridade reguladora específica para lidar com reclamações e infrações relacionadas à IA. Essa autoridade não apenas será responsável por receber queixas, mas também terá um assento no futuro Comitê Europeu de Inteligência Artificial, garantindo uma conexão direta com o Comitê Europeu de Proteção de Dados estabelecido pela GRPD. As autoridades nacionais competentes serão investidas de poderes de aplicação, incluindo a capacidade de impor multas significativas, dependendo do grau de não conformidade com as regulamentações e dos riscos apresentados pelos sistemas de IA (Oprea *et al*., 2022; Veale *et al*., 2021).

Além disso, a Comissão Europeia estabeleceu um Escritório Europeu de IA, encarregado de supervisionar as regras que os modelos de IA de uso geral devem cumprir. Este escritório, por meio de códigos de conduta e protocolos de transparência, trabalhará para garantir a conformidade e a ética no desenvolvimento e na utilização de sistemas de IA (Cabrera; Mcgowan, 2024).

No que diz respeito às penalidades por infrações, que se estendem, inclusive, aos fornecedores de modelos de IA de uso geral, a regulamentação estabelece valores específicos para diferentes tipos de violações. As falhas em cumprir obrigações do IA ACT estão sujeitas a multas de até 35 milhões de euros ou, tratando-se de empresa, até 7% do faturamento anual mundial do ano anterior, o que for maior (Cabrera; Mcgowan, 2024).

Além das penalidades financeiras, haverá restrições específicas para o uso de sistemas de identificação biométrica (RBI) em espaços públicos, com autorização judicial prévia sendo necessária em muitos casos. O projeto de lei também introduz regras para o uso de tecnologias de reconhecimento facial, diferenciando entre seu uso de alto risco e baixo risco (Ebers *et al*., 2021; European Parliament, 2024).

3.3 A transnacionalidade do AI ACT na UE: preparação e cronograma de implementação

O AI ACT é uma legislação ambiciosa que visa regulamentar a IA na UE, não apenas para sistemas desenvolvidos dentro da UE, mas também para aqueles que impactam os seus cidadãos, independentemente de sua origem geográfica. Essa abordagem transnacional busca garantir um ambiente regulatório consistente e abrangente para a IA em toda a UE (Veale *et al*., 2021).

Para se preparar para a implementação do AI ACT e garantir a conformidade, as pessoas jurídicas devem iniciar uma série de medidas proativas. Primeiramente, é essencial realizar um inventário de todos os sistemas de IA desenvolvidos ou implementados, seguido pela classificação dos riscos associados a esses sistemas para determinar os requisitos de conformidade aplicáveis. Além disso, é crucial analisar a interação com outras regulamentações dentro e fora da UE e desenvolver planos para garantir a conformidade com todas as exigências (Veale *et al*., 2021).

Uma das medidas importantes destacadas no projeto é a declaração de conformidade, que deverá ser elaborada pelos fornecedores de serviços de IA. Essa declaração conterá informações detalhadas sobre o sistema de IA em questão e confirmará sua conformidade com as disposições do regulamento, sendo emitida sob a exclusiva responsabilidade do fornecedor (Ebers *et al*., 2021; Veale *et al*., 2021).

Quanto ao cronograma de implementação do AI ACT, está previsto um processo escalonado para garantir uma transição suave para as novas regulamentações. Após a aprovação do texto final pelos Comitês de Mercado Interno e Liberdades Civis do Parlamento Europeu, o projeto foi submetido e aprovado pelo plenário em 13 de março de 2024. A entrada em vigor do regulamento ocorrerá no 20º dia após sua publicação no Jornal Oficial da UE, com eficácia após 24 meses (European Parliament, 2024).

No entanto, algumas disposições terão aplicação imediata após períodos específicos, como as vedações previstas no Título I e II, que serão aplicadas seis meses após a entrada em vigor. Outras medidas, como os códigos de prática e as penalidades, terão prazos diferenciados para implementação, visando garantir uma adaptação gradual e eficaz às novas regulamentações (European Parliament, 2024).

CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo geral analisar o AI ACT como um marco regulatório pioneiro na governança da IA na União Europeia, considerando seus objetivos, abrangência e mecanismos de aplicação. Para tanto, foram estabelecidos objetivos específicos que envolviam a investigação das origens do capitalismo informacional e do surgimento do capitalismo de vigilância, a análise da legislação brasileira e das normas internacionais de segurança da informação, com foco na proteção da dignidade e privacidade na era digital, e a avaliação dos avanços e desafios associados ao marco regulatório da IA na UE.

Ao longo deste estudo, foi possível constatar que o AI ACT representa um importante avanço na regulamentação da inteligência artificial na UE. Suas diretrizes éticas e foco na segurança e proteção dos direitos individuais demonstram um compromisso significativo com o desenvolvimento responsável da IA. Além disso, a análise das origens do capitalismo informacional e do surgimento do capitalismo de vigilância proporcionou insights valiosos sobre as dinâmicas econômicas e sociais moldadas pela coleta massiva de dados e pela vigilância digital.

No que diz respeito à legislação brasileira e às normas internacionais de segurança da informação, observou-se que tanto o GDPR da UE quanto a LGPD brasileira representam avanços significativos na proteção da privacidade e dos dados pessoais dos cidadãos. A comparação entre essas legislações permitiu identificar pontos de convergência e divergência, contribuindo para um entendimento mais abrangente das abordagens regulatórias adotadas em diferentes contextos jurídicos.

Quanto aos desafios e oportunidades associados ao AI ACT, destacou-se a necessidade de uma implementação eficaz e coordenada entre os Estados membros da UE, bem como a importância de uma abordagem transnacional para lidar com os impactos da IA em escala global. A discussão sobre os riscos sistêmicos e os mecanismos de fiscalização e aplicação das normativas relacionadas à IA na UE ressaltou a complexidade desse processo regulatório e a importância de uma abordagem multidisciplinar e colaborativa.

Embora os objetivos específicos tenham sido abordados de forma abrangente ao longo deste estudo, foi detectado que há espaço para estudos futuros que aprofundem certos aspectos. Recomenda-se uma análise mais detalhada do impacto do AI ACT sobre a inovação e competitividade no mercado único da UE, bem como estudos comparativos entre o AI ACT e outras estratégias regulatórias adotadas em diferentes regiões do mundo. Além disso, sugere-se

a realização de pesquisas empíricas para avaliar a eficácia do AI ACT na prática e seu impacto sobre os direitos individuais e a economia europeia.

REFERÊNCIAS BIBLIOGRÁFICAS

BARBOSA, Mafalda Miranda *et al*. **Direito Digital e Inteligência Artificial**: diálogos entre Brasil e Europa. Indaiatuba, SP: Foco, 2021.

CABRERA, Laura Lazaro; MCGOWAN, Iverna. **A Series on the EU AI Act, Part 1:** An Explainer, Center for Democracy and Technology. CDT Europe, United States of America, 2024. Disponível em: https://policycommons.net/artifacts/12309840/cdt-europe-a-series-on-the-eu-ai-act-part-1/13206200/ on 19 May 2024. CID: 20.500.12592/hmgqv1k. Acesso em: 19 maio 2024.

CARIBÉ, João Carlos Rebello. Uma perspectiva histórica e sistêmica do capitalismo de vigilância. **Inteligência Empresarial**, v. 41, p. 5-13, 2019.

CARTER, Denise. Regulation and ethics in artificial intelligence and machine learning technologies: Where are we now? Who is responsible? Can the information professional play a role? **Business Information Review**, volume 37, Issue 2, 2020.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999. (A Era da Informação: economia, sociedade e cultura, 2).

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: **Tratado de Proteção de Dados Pessoais**. MENDES, Laura Schertel. DONEDA, Danilo. SARLET, Ingo Wolfgang. RODRIGUES JR, Otavio Luiz. Rio de Janeiro: Forense, 2021.

EBERS, Martin; HOCH, Veronica R. S.; ROSENKRANZ, Frank; Hannah, RUSCHEMEIER; STEINRÖTTER, Björn. The European Commission's Proposal for an Artificial Intelligence Act, A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). **Multidisciplinary Scientific Journal**, 2021, Volume 4, Issue 4.

EUROPEAN Parliament Legislative Resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html. Acesso em 19 maio 2024.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, Rio de Janeiro, v. 12, n. 2, p. 1002-1033, junho 2020.

GUNTHER, Luiz Eduardo; COMAR, Rodrigo Thomazinho; RODRIGUES, Luciano Ehlke. A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade: os limites da intervenção do Estado. **Relações Internacionais no Mundo Atual**, v. 2, n. 27, p. 25-41, 2020.

KOERNER, Andrei. Capitalismo e vigilância digital na sociedade democrática. **Revista Brasileira de Ciências Sociais**, v. 36, n. 105, p. 1-6, 2021.

MADIEGA, Tambiama. **EU guidelines on ethics in artificial intelligence**: Context and implementation. EPRS: European Parliamentary Research Service, Belgium, 2019. Disponível em: https://policycommons.net/artifacts/1337743/eu-guidelines-on-ethics-in-artificial-intelligence/1945725/ on 19 May 2024. CID: 20.500.12592/vqq0nr. Acesso em: 19 maio 2024.

OPREA, Octavian; HOINARU, Razvan; PACURARU-IONESCU, Catalin-Paul; NEAMTU, Daniela. **Accounting for the future:** practice, Artificial Intelligence and regulation. Sciendo, 2022. DOI: 10.2478/picbe-2022-0076

VEALE, Michael; BORGESIUS, Frederik Zuiderveen. Demystifying the draft EU AI Act. **Computer Law Review International**, v. 22, n. 4, July 2021.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira de poder. Trad. George Schlesinger. Rio de Janeiro: Intrínseca, 2020.