

I INTERNATIONAL EXPERIENCE PERUGIA - ITÁLIA

INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL III

PAULO CEZAR DIAS

VALTER MOURA DO CARMO

FERNANDO GALINDO AYUDA

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

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

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

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

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

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

I61

Inteligência Artificial: Desafios da Era Digital III [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Fernando Galindo Ayuda, Paulo Cezar Dias, Valter Moura do Carmo. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia

ISBN: 978-65-5274-097-7

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

Tema: Inteligência Artificial e Sustentabilidade na Era Transnacional

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Inteligência Artificial. 3. Desafios da Era Digital. I
International Experience Perugia – Itália. (1: 2025 : Perugia, Itália).

CDU: 34



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

I INTERNATIONAL EXPERIENCE PERUGIA - ITÁLIA

INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL III

Apresentação

APRESENTAÇÃO

O I International Experience – Perúgia – Itália foi realizado nos dias 28, 29 e 30 de maio de 2025, com o tema "Inteligência Artificial e Sustentabilidade na Era Digital". O Grupo de Trabalho (GT) "Inteligência Artificial: Desafios da Era Digital III" ocorreu nos dias 29 e 30 de maio, nos períodos vespertinos, na Universidade de Perúgia.

O GT destacou-se não apenas pela qualidade dos trabalhos apresentados, mas também pelo nível acadêmico dos autores — doutores, mestres, professores pesquisadores e seus alunos pós-graduandos. O evento também proporcionou um importante espaço de interlocução internacional, contando com a participação de renomados juristas e professores de instituições estrangeiras, como os Professores Doutores Roberto Cippitani (Universidade de Perúgia) e Fernando Galindo (Universidade de Zaragoza – Espanha), que enriqueceram os debates e contribuíram para o sucesso da atividade.

Foram apresentados 15 (quinze) artigos, os quais foram objeto de intenso debate presidido pelos coordenadores e enriquecido pela participação ativa do público presente na Faculdade de Direito de Perúgia – ITÁLIA.

A apresentação dos trabalhos permitiu discussões atualizadas e profícuas sobre temas como inteligência artificial, uso de dados pessoais, dever de informação, riscos e interações tecnológicas. As abordagens trataram dos desafios enfrentados pelas diversas linhas de pesquisa jurídica no estudo do futuro da regulação no Brasil, dos abusos relacionados à inteligência artificial e das possíveis soluções para a proteção de dados em um mundo globalizado.

As temáticas incluíram: tecnologias relacionadas a fake news, deepfakes e bots; compliance; a consideração do elemento humano na aplicação da I.A. nas decisões judiciais; a inteligência artificial como ferramenta de proteção no sistema de justiça criminal; o consentimento informado e o uso de dados pessoais; regulamentação e governança da I.A.; precarização do governo digital e aplicação da inteligência artificial em distintos setores jurídicos.

A seguir, apresenta-se a relação dos trabalhos que compõem este Grupo de Trabalho, acompanhados de seus respectivos autores:

1. CAPACIDADE ARTIFICIAL DAS MÁQUINAS E A EXIGÊNCIA DE TRANSFORMAÇÕES NA MANEIRA DO SABER DE PROFISSIONAIS, de Fernanda Conceição Pohlmann.
2. AI, VOCÊ ESTÁ AÍ? O PANORAMA JURÍDICO RELATIVO À (AUTO) IDENTIFICAÇÃO DA INTELIGÊNCIA ARTIFICIAL, de Gabriel Siqueira Eliazar de Carvalho, André Fortes Chaves e Marcello Silva Nunes Leite.
3. DEMOCRACIA EM REDE: O PAPEL DA INTELIGÊNCIA ARTIFICIAL E DOS ALGORITMOS NA LIBERDADE DE EXPRESSÃO E NO PLURALISMO POLÍTICO, de Kennedy da Nobrega Martins, Alexandre Manuel Lopes Rodrigues e Jadgleison Rocha Alves.
4. INTELIGÊNCIA ARTIFICIAL E DIREITOS FUNDAMENTAIS: DESAFIOS E TENSÕES NA ERA DIGITAL, de Jesualdo Eduardo de Almeida Junior e Gustavo Roberto Dias Tonia.
5. INTELIGÊNCIA ARTIFICIAL E DEMOCRACIA: O PERIGO DA MANIPULAÇÃO DE INFORMAÇÕES, de Claudia Maria da Silva Bezerra e Luiz Eduardo Simões de Souza.
6. INFLUÊNCIAS DO REALISMO JURÍDICO E O USO DA INTELIGÊNCIA ARTIFICIAL NA ELABORAÇÃO DE DECISÕES JUDICIAIS NO BRASIL: VIESES COGNITIVOS E HEURÍSTICAS NO PROCESSO DECISÓRIO, de Kerry Barreto, Fausto Santos de Moraes e Júlia Regina Bassani Caus.
7. CRITÉRIOS QUANTITATIVOS PARA A MENSURAÇÃO DE RESULTADOS NO JUÍZO 100% DIGITAL: RISCOS PARA A QUALIDADE DA PRESTAÇÃO JURISDICIONAL NO BRASIL, de Orides Mezzaroba, José Renato Gaziero Cella e Lia Loana Curial Oliva.
8. AS PROVAS DIGITAIS NO PROCESSO CIVIL E O (DES)CABIMENTO DA CADEIA DE CUSTÓDIA, de Jesualdo Eduardo de Almeida Junior e Gustavo Roberto Dias Tonia.
9. A REVOLUÇÃO DA INTELIGÊNCIA ARTIFICIAL NOS GABINETES JUDICIAIS: EFICIÊNCIA COM GARANTIAS CONSTITUCIONAIS, de Lisbino Geraldo Miranda do Carmo, Deise Neves Nazaré Rios Brito e Jimmy Souza do Carmo.

10. GENEALOGIA E INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA ERA DIGITAL PARA ELABORAÇÃO DE UM ONOMÁSTICO DOS IMIGRANTES ITALIANOS QUE DESENVOLVERAM O SUL DO ESTADO DE SANTA CATARINA DE 1877 A 1897, de Júlio Cesar Cancellier de Olivo.

11. A REDE-LAB COMO INOVAÇÃO NA POLÍTICA ANTILAVAGEM DE CAPITAIS NO BRASIL, de Lorryne Souza Galli e Matheus Felipe de Castro.

12. ARMAS AUTÔNOMAS LETAIS: OS IMPACTOS DA INTELIGÊNCIA ARTIFICIAL PARA OS DIREITOS HUMANOS E SUA CONSEQUENTE REGULAMENTAÇÃO, de Alexandre Gonçalves Ribeiro e Renata Mantovani de Lima.

13. A INTELIGÊNCIA ARTIFICIAL COMO FERRAMENTA ESSENCIAL NA ELUCIDAÇÃO DE CRIMES SEXUAIS PRATICADOS COM VIOLÊNCIA CONTRA A MULHER, de Eneida Orbage de Britto Taquary e Catharina Orbage de Britto Taquary Berino.

14. A INTELIGÊNCIA ARTIFICIAL NO DIREITO PENAL: AVANÇOS, DESAFIOS E IMPACTOS NA INVESTIGAÇÃO E NO SISTEMA JUDICIAL, de Eneida Orbage de Britto Taquary, Bianca Cristina Barbosa de Oliveira e Tiago de Lima Mascarenhas Santos.

15. ENTRE CÓDIGOS E DIREITOS: UMA ANÁLISE CONSTITUCIONAL DA PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA INTELIGÊNCIA ARTIFICIAL, de Lisbino Geraldo Miranda do Carmo, Deise Neves Nazaré Rios Brito e Paulo Henrique da Silva Costa.

Por fim, os organizadores e coordenadores do Grupo de Trabalho "Inteligência Artificial: Desafios da Era Digital III" parabenizam e agradecem aos autores pelos valiosos trabalhos apresentados, cuja leitura certamente contribuirá para o aprofundamento do debate acadêmico e científico na área.

Prof. Dr. Fernando Galindo - Universidad de Zaragoza - Espanha

Prof. Dr. Valter Moura do Carmo – PPGPJDH - ESMAT e UFT

Prof. Dr. Paulo Cezar Dias – Centro Universitário Eurípides de Marília - SP

A CIDADANIA ELETRÔNICA DO HOMO DIGITALIS: PERSPECTIVAS JURÍDICAS À LUZ DO REGULAMENTO (UE) 2024/1689 SOBRE INTELIGÊNCIA ARTIFICIAL

ELECTRONIC CITIZENSHIP OF HOMO DIGITALIS: LEGAL PERSPECTIVES IN THE LIGHT OF REGULATION (EU) 2024/1689 ON ARTIFICIAL INTELLIGENCE

**Olivia Oliveira Guimarães
Helen Caroline Cardoso Santos
Lucas Gonçalves da Silva**

Resumo

A presente pesquisa tem como objetivo geral investigar a cidadania eletrônica do homo digitalis como elemento fundamental da democracia e da salvaguarda de direitos fundamentais do indivíduo no ciberespaço à luz do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho da União Europeia. Destarte, o estudo buscou esmiuçar brevemente os meandros do novo império ditado pelos algoritmos; esmiuçar brevemente os meandros do novo império ditado pelos algoritmos; investigar quais direitos fundamentais possuem riscos de serem violados no universo digital; mapear os direitos fundamentais tutelados à luz do Regulamento (UE) nº 2024/1689 do Parlamento Europeu; discorrer sobre cidadania eletrônica na dimensão virtual; e analisar a sinergia do exercício da cidadania eletrônica com o Regulamento (UE) nº 2024/1689. Para tanto, a abordagem da pesquisa fundou-se em estudo qualitativo, utilizando-se de procedimentos de pesquisa bibliográfica, documental, legislativa, jornalística, além de informações extraídas de fontes oficiais e de repositórios digitais. Por fim, depreende-se do estudo que há uma relação simbiótica entre a cidadania, a privacidade e a democracia, e, por isso, a verdadeira liberdade não está apenas em escolher o que consumir, mas em garantir que os dados, a privacidade e a autonomia não sejam os produtos a serem vendidos no capitalismo de vigilância.

Palavras-chave: Algorithms, Artificial intelligence, Democracy, Electronic citizenship, Fundamental rights

Abstract/Resumen/Résumé

The present research aims to investigate the electronic citizenship of the homo digitalis as a fundamental element of democracy and the safeguarding of individuals' fundamental rights in cyberspace, in light of Regulation (EU) 2024/1689 of the European Parliament and the Council of the European Union. To this end, the study sought to briefly examine the intricacies of the new empire dictated by algorithms; investigate which fundamental rights are at risk of being violated in the digital realm; map the fundamental rights protected under Regulation (EU) No. 2024/1689 of the European Parliament; discuss electronic citizenship in the virtual dimension; and analyze the synergy between the exercise of electronic citizenship and Regulation (EU) No. 2024/1689. To achieve this, the research approach was grounded in

qualitative study, utilizing bibliographic, documentary, legislative, journalistic research procedures, as well as information from official sources and digital repositories. In conclusion, the study shows that there is a symbiotic relationship between citizenship, privacy, and democracy, and thus, true freedom is not merely in choosing what to consume, but in ensuring that data, privacy, and autonomy are not the products to be sold in surveillance capitalism.

Keywords/Palabras-claves/Mots-clés: Algorithms, Artificial intelligence, Democracy, Electronic citizenship, Fundamental rights

1 INTRODUÇÃO

As inovações tecnológicas foram aprimoradas por meio do desenvolvimento da inteligência artificial [IA], a qual foi amplamente difundida na vida moderna, tornando-se uma revolucionária ferramenta para atender as necessidades humanas na era da sociedade de informação e para inaugurar uma nova ordem social, econômica e cultural, ditada pela lógica do mercado, qual seja, produtividade, eficiência e lucro.

Em um panorama em que o uso da máquina se elevou à categoria essencial da vida moderna, sobretudo após a pandemia, o *homo sapiens* transmudou-se em *homo digitalis*, que é o indivíduo anônimo integrante de um aglomerado digital, cada vez mais enclausurado e conectado ao ambiente virtual (Han, p. 28, 2018).

O espaço digital tornou-se um universo de difusão do comércio eletrônico, de interconexão global, de exercício de direitos, como liberdade de expressão e acesso à informação e ao conhecimento, mas também se criou uma dimensão em que direitos fundamentais são constantemente violados em decorrência da algocracia – “ditadura com algoritmos”, que é o controle exercido (por quem o detém) através de algoritmos (Cabitza; Floridi, 2021, p. 27)¹.

Desse modo, o presente estudo tem como objetivo geral investigar a cidadania eletrônica do *homo digitalis* como elemento fundamental da democracia e da salvaguarda de direitos fundamentais do indivíduo no ciberespaço.

Nesse mister, os objetivos específicos desta pesquisa são: esmiuçar brevemente os meandros do novo império ditado pelos algoritmos; investigar quais direitos fundamentais possuem riscos de serem violados no universo digital; mapear os direitos fundamentais tutelados à luz do Regulamento (UE) nº 2024/1689 do Parlamento Europeu; discorrer sobre cidadania eletrônica na dimensão virtual; e analisar a sinergia do exercício da cidadania eletrônica com o Regulamento (UE) nº 2024/1689.

Para tanto, a abordagem da pesquisa fundar-se-á em estudo qualitativo, utilizando-se de procedimentos de pesquisa bibliográfica, documental, legislativa, jornalística, além de informações extraídas de fontes oficiais e de repositórios digitais.

2 BIG OTHER: O NOVO IMPÉRIO DITADO PELOS ALGORITMOS

¹ Tradução livre do texto original: “sarebbe piuttosto una forma di potere esercitato (da chi ce l’ha) mediante gli algoritmi, una ‘dittatura con gli algoritmi’”.

O homem, dotado com genuíno espírito de inventividade, cria, desde os primórdios, ferramentas que o auxilia em suas tarefas cotidianas. Ao longo da existência do *homo sapiens*, surgiram invenções revolucionárias e disruptivas, como as máquinas e a internet, as quais causaram profundos impactos sociais, econômicos, ideológicos e culturais na sociedade, como o surgimento dos sistemas de produção em massa e da globalização.

Diante dos incessantes avanços tecnológicos, há quem sustente que a criação da inteligência artificial [IA] pode ser considerada “o maior evento da história da humanidade” (Russell, 2019). Harari (2024, p. 308-309) sinaliza que “[...] a invenção de novas tecnologias da informação está fadada a mudar a sociedade.” e que “[...] é inevitável que isso resulte numa profunda revolução social e política.”

Por certo, o enraizamento da IA no âmago da vida moderna e das operações comerciais vem transformando visceralmente a sociedade, o mercado e o próprio homem, deslocando o domínio de poder [*outrora centralizado*] do Estado para as grandes empresas do ramo de tecnologia. Inclusive, essas grandes corporações transnacionais possuem capital superior ao PIB de muitos países (Galindo, 2017) e daí exsurge o poder de influenciar as regras do jogo mercadológico, político e jurídico.

Em um cenário pós-panóptico, onde a conquista do território e o uso do espaço físico para exercer o controle sobre o indivíduo cedem frente à velocidade do sinal eletrônico de modo que o domínio se constitui extraterritorial² (Bauman, 2021, p. 19), ou seja, o exercício do poder não exige uma presença física de quem o detém, pois a ordem pode ser propagada por meio digital.

Nesse cenário, as *big techs* são empresas que estão em todo lugar porque se localizam em “algum lugar entre a natureza e Deus [...] *Big Other*” (Zuboff, 2018, p. 43) diante da dimensão globalizada, da natureza imaterial e sem fronteiras dos serviços tecnológicos e do caráter transnacional, que rompe as barreiras dos Estados nacionais e que cria armaduras corporativas jurídicas “imunes” à aplicação efetiva da lei.

Essas empresas ditam as regras do modelo dominante do capitalismo de vigilância, onde os dados dos usuários são o novo ativo valioso do mercado (Harari,

² Vander Maelen (2020) sustenta que: “Territorialmente falando, a indústria de tecnologia oferece outro desafio que talvez seja ainda mais assustador: as fronteiras jurisdicionais políticas não conseguem mais conter esses serviços imateriais e essencialmente sem fronteiras, resultando em uma espécie de ‘desterritorialização’ (Barkan, 2013, 87) que permite que atores tecnológicos moldem em grande parte o debate sobre quais normas devem estar sujeitos (Kilovaty 2019; Peng 2018). Isso leva as autoridades nacionais a enfrentarem problemas jurisdicionais ao tentar regular ou aplicar regras.” (tradução livre do texto original)

2021, p.69). Disso decorre que o capitalismo de vigilância é uma forma de mercado onde há a necessidade intrínseca de coletar uma quantidade massiva de dados [*big data*³] como matéria-prima para a predição assertiva de comportamentos do indivíduo, cujos produtos de predições [dados comportamentais] são comercializados “de modo a incentivar, persuadir, sintonizar e arrebanhar comportamento em busca de resultados lucrativos” em prol das empresas (Zuboff, 2021, p. 22-23).

Noutras palavras, o comportamento cotidiano do ser humano é alvo de vigilância nas plataformas digitais e de estratégias comerciais sob o domínio do *Big Other*, que é uma nova arquitetura configurada em “[...] regime institucional em rede que registra, modifica e mercantiliza a experiência cotidiana, desde o uso de um eletrodoméstico até seus próprios corpos, da comunicação ao pensamento, tudo com vista a estabelecer novos caminhos para a monetização e o lucro” (Zuboff, 2018, p. 43-44).

O homem não é visto como um sujeito de direitos, mas, sim, como o produto no capitalismo de vigilância, cuja liberdade de escolha e autonomia são tolhidas frente à nova forma de poder, que “[...] é identificado com a propriedade dos meios de modificação comportamental” (Zuboff, 2018, p. 45). Para tanto, serviços gratuitos em plataformas virtuais são disponibilizados com o escopo de minerar dados pessoais, biométricos e bancários para traçar o perfil do usuário, que calibram o valor preditivo das análises comportamentais, e, posteriormente, tais dados transformam-se em ativo no mercado de vigilância.

Percebe-se que os indivíduos são tratados como mercadorias e transformados em “pessoas eletrônicas” inseridas como meras “abstrações no ciberespaço” da sociedade da informação (Rodotá, 2021, p. 156). Ou seja, o homem é dissolvido para formar o *enxame digital*, perdendo seu perfil próprio (Han, 2018, p. 27) e tornando-se mais um [dado] no universo digital.

Para efetivar o mecanismo - por vezes oculto e invisível- desse novo imperativo econômico e tecnológico, as empresas

[...] capturam nossa atenção fornecendo-nos gratuitamente informação, serviços e entretenimento, e depois revendem nossa atenção aos anunciantes. [...] E sim, ao captar nossa atenção, eles conseguem acumular imensa quantidade de dados sobre nós, o que vale mais do que qualquer receita de publicidade. Nós não somos seus clientes — somos seu produto (Harari, 2018, p. 68).

³ Zuboff (2018, p. 18) conceitua *big data* como “componente fundamental de uma nova lógica de acumulação, profundamente intencional e com importantes consequências, que chamo de *capitalismo de vigilância*. Essa nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado”.

E é justamente nesse contexto contemporâneo que as empresas encontram um campo fértil e sem barreiras [legais efetivas] para exploração econômica de suas atividades, apropriando-se dos recursos relacionados à inteligência artificial para extrair, sorrateiramente, dados pessoais, com o fim de, por meios dos algoritmos, analisar, criar padrões e comercializar os dados e moldar o comportamento humano em prol de seus interesses financeiros.

3 A PRIMEIRA LEGISLAÇÃO MUNDIAL SOBRE INTELIGÊNCIA ARTIFICIAL: BREVE ANÁLISE DO REGULAMENTO (UE) 2024/1689 DO PARLAMENTO EUROPEU E DO CONSELHO DA UNIÃO EUROPEIA

O Regulamento da Inteligência Artificial (UE) 2024/1689, aprovado pelo Parlamento Europeu e Conselho da União Europeia, representa um marco significativo e inédito, em nível global, na regulação e na promoção de uma abordagem da IA centrada no ser humano, colocando a União na posição de vanguarda mundial do desenvolvimento de uma IA segura, ética e de confiança.

O instrumento normativo foi publicado no Jornal Oficial da União Europeia em 12/07/2024 e entrou em vigor em 01/08/2024, mas as disposições somente serão integralmente válidas a partir de 02/08/2026 e, para os sistemas de alto risco, a partir de 02/08/2027. No entanto, considerando-se o risco inaceitável associado à utilização da IA, as proibições bem como as disposições gerais do regulamento deverão aplicar-se a partir de 02/02/2025⁴.

Esse período de vacância tem como escopo o de garantir a segurança jurídica, proporcionando um período de adaptação razoável para os operadores de sistema de IA se amoldarem aos requisitos obrigatórios estipulados no regulamento. Nesse interregno, os prestadores de IA de risco elevado são incentivados a começar a cumprir, de uma forma voluntária, as obrigações preconizadas na nova legislação durante o período de transição.

O Regulamento (UE) 2024/1689 teve como objetivo a criação de um regime jurídico uniforme

em conformidade com os valores da União, a fim de promover a adoção de uma inteligência artificial (IA) **centrada no ser humano e de confiança**, assegurando simultaneamente um elevado nível de **proteção da saúde**, da **segurança**, dos **direitos fundamentais** consagrados na Carta dos Direitos

⁴ Vide artigo 113º do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho.

Fundamentais da União Europeia («Carta»), nomeadamente a **democracia**, o **Estado de direito** e a **proteção do ambiente**, a **proteção contra os efeitos nocivos dos sistemas de IA na União**, e de **apoiar a inovação** (Regulamento Europeu, 2024, p. 1). [sem grifo no original]

Para tanto, a União Europeia buscou harmonizar o emprego e o incentivo à inovação tecnológica com os princípios éticos e com a proteção das pessoas, das empresas, dos direitos fundamentais, do meio ambiente, da democracia e do Estado de Direito. Partiu-se do fundamento central que a IA deve ser uma tecnologia centrada no ser humano ao passo em que servirá de instrumento para as pessoas, com o objetivo de aumentar o bem-estar humano e respeitar a democracia, o meio ambiente e o Estado de Direito.

A abordagem dessas regras vinculativas baseou-se no risco, adaptando-se o tipo e o conteúdo dessas normas à intensidade e ao âmbito dos riscos que podem ser criados pelos sistemas de IA. O intento é tornar o regulamento eficaz com base em riscos previamente definidos e em requisitos mais rigorosos para o funcionamento e a disponibilização no mercado de sistemas de IA de risco elevado.

Além do mais, para assegurar uma proteção eficaz dos direitos e das liberdades das pessoas e ao se considerar à natureza digital e imaterial da IA, determinados sistemas bem como prestadores e responsáveis pela implementação da rede inteligente estão inseridos no âmbito de incidência das previsões vinculativas do regulamento, independentemente de estarem estabelecidos na União Europeia, desde que o resultado produzido pelo sistema seja utilizado na União, conforme estipula o artigo 2º do novo regime legal.

Percebe-se, portanto, que essa previsão normativa se destina a expandir as concepções jurídicas vinculativas do ordenamento para abarcar empresas não sediadas na União Europeia quando o produto for utilizado ou posto em serviço na União, dissolvendo-se, assim, as fronteiras que poderiam dificultar a adoção de medidas necessárias para a proteção da saúde e dos direitos fundamentais bem como para o implemento de uma IA confiável.

A inédita estrutura normativa também recomenda a aplicação dos princípios éticos, estabelecidos nas orientações éticas para uma IA de Confiança elaboradas pelo Grupo de Peritos de Alto Nível em IA (AI HLEG)⁵, na concepção e na utilização de modelos de IA, bem como na elaboração de códigos de conduta.

⁵ AI HLEG, do inglês *High-Level Expert Group on Artificial Intelligence*.

Nessas orientações, são sete os princípios éticos que se destinam a contribuir para a construção de um modelo de IA coerente, de confiança e centrado no ser humano, em consonância com a ética, a Carta e com os valores em que se funda a União: iniciativa e supervisão por humanos; solidez técnica e segurança; privacidade e governação dos dados; transparência; diversidade, não discriminação e equidade; bem-estar social e ambiental e responsabilização.

O capítulo XII prevê as sanções, as quais devem ser efetivas, proporcionais e preventivas, que podem incluir advertências e medidas não pecuniárias, além de multas que podem chegar até 35 milhões de euros ou 7% do volume de negócios anual a nível mundial do exercício anterior para as empresas que descumprirem as proibições previstas no artigo 5º do regulamento.

Por fim, cabe destacar que o Regulamento (UE) 2024/1689 é um regime jurídico criado em harmonia com direitos preconizados em outros sistemas legislativos, como a Carta dos Direitos Fundamentais da União Europeia e o Tratado da União Europeia, promovendo, por conseguinte, a coexistência normativa.

A guisa de exemplo, o direito fundamental à proteção de dados pessoais é brevemente citado em algumas passagens da norma regulamentar, mas o tratamento de dados das pessoas está salvaguardado especialmente pelos Regulamentos (UE) 2016/679 e (UE) 2018/1725 do Parlamento Europeu e do Conselho e pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de acordo com o artigo 2º, nº 7 do Regulamento (UE) 2024/1689.

Ou seja, como regra geral, o inédito instrumento legal não deve ser entendido como um fundamento jurídico para o tratamento de dados pessoais, salvo disposição específica presente no novo regime jurídico, porque o direito da União, citado alhures, é aplicado aos dados pessoais tratados em virtude dos direitos e obrigações estabelecidos no regulamento.

Com isto, criou-se um sistema jurídico interconectado, coeso e harmonizado com normas preconizadas em outras legislações da União Europeia, dispensando-se a repetição de dispositivos porquanto o próprio regulamento faz menção expressa quando determinado direito ou mecanismo jurídico deve ser aplicado em conjunto com as regras do novo regime legal.

Após firmar, brevemente, os aspectos mais relevantes do Regulamento (UE) 2024/1689 para o presente estudo, passa-se a esmiuçar a abordagem jurídica calcada nos

riscos e os direitos fundamentais tutelados no novo sistema normativo, sem, no entanto, exaurir todas as perspectivas que envolvem o tema.

3.1 Dos riscos inaceitáveis dos sistemas de IA

Em suma, a abordagem do regulamento é baseada em categorias de riscos: proibido, elevado, limitado e mínimo. Para os casos de riscos mínimos, os sistemas podem ser implementados e não estão abrangidos pelo Regulamento da UE em estudo por não representarem ameaça a direitos fundamentais e à segurança das pessoas, como nos casos de filtro de *spam* dos e-mails ou softwares de tradução de idioma.

Quanto aos riscos limitados, exige-se a adoção de obrigações de transparência [artigo 50] com o escopo primordial de o usuário ser informado de que está interagindo com uma IA ou com texto gerado por meio de um sistema inteligente quando versar sobre questões de interesse público. Da mesma maneira, quando houver criação ou manipulação de imagem, áudio ou vídeo que constitua uma falsificação profunda, os responsáveis pela implantação do sistema deve informar que o conteúdo foi gerado ou manipulado.

Apesar desse risco ser considerado como limitado, em uma análise apressada, os últimos eventos sinalizam uma enorme preocupação diante da disseminação das *deepfakes*, que é a utilização de IA para criar imagens, vídeos ou áudios falsificados de uma forma bastante realista. Acontece que tal técnica manipuladora tem proporcionado imensuráveis prejuízos, sobretudo pela dificuldade em identificar se o conteúdo é ou não falso, colocando o indivíduo em uma posição de extrema vulnerabilidade frente à tecnologia *deepfake* e violando-se direitos fundamentais.

À título de exemplo, circulou na rede a notícia de que um funcionário de uma multinacional foi enganado e transferiu US\$ 25 milhões a golpistas, que usaram IA sob o viés de *deepfake* para manipular a imagem e a voz e, assim, se passaram pelo diretor financeiro da empresa em uma chamada de videoconferência (Chen; Magramo, 2024). A *deepfake* também tem sido utilizada no universo pornográfico, sobretudo vitimizando mulheres, crianças e adolescentes (Pinto; Oliveira, 2023).

Por isso, o regulamento proibiu determinadas práticas inaceitáveis de IA, como as manipuladoras, exploratórias e de controle social, por serem consideradas prejudiciais e abusivas além de desrespeitarem valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como os direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia,

especialmente o direito à não discriminação e à proteção de dados pessoais e à privacidade.

O artigo 5º prevê expressamente as seguintes práticas proibidas: (I) sistema de IA que utilize técnicas subliminares, manipuladoras ou enganadoras para distorcer substancialmente o comportamento de uma pessoa a fim de prejudicar a sua capacidade de tomar uma decisão; (II) sistema que explore vulnerabilidades de uma pessoa em decorrência da idade, incapacidade ou situação socioeconômica específica; (III) sistema de classificação social com base em comportamento social ou em características pessoais ou de personalidade; (IV) sistema de reconhecimento de emoções no local de trabalho e nas instituições de ensino, salvo por razões médicas ou de segurança; (V) sistemas de identificação biométrica à distância em tempo real e em espaços acessíveis ao público para efeitos de aplicação da lei, salvo quando estritamente necessário para busca de vítimas ou pessoas desaparecidas, prevenção de ameaça real à vida ou à segurança das pessoas e para a localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos; e (VI) sistemas que criam ou expandem bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais da Internet ou de imagens de televisão em circuito fechado.

Em caráter excepcionalíssimo, é permitida a utilização de sistemas de identificação biométrica à distância e em tempo real em locais acessíveis ao público desde que autorizada previamente por uma autoridade judiciária ou uma autoridade administrativa independente, cuja decisão seja vinculativa, com supedâneo em dados objetivos ou indícios claros de que a medida é necessária e proporcional para alcançar as finalidades previstas na legislação, como as citadas anteriormente.

Além do mais, a utilização desse tipo de sistema deve ser limitada ao estritamente necessário no que diz respeito ao período de tempo e ao âmbito geográfico e pessoal, bem como somente será autorizada se a autoridade responsável pela aplicação da lei tiver concluído uma avaliação de impacto sobre os direitos fundamentais, conforme previsto no artigo 27, e tiver registrado o sistema na base de dados da UE em conformidade com o artigo 49.

Contudo, em casos de urgência devidamente justificados, a utilização desses sistemas pode ser iniciada sem uma autorização, desde que essa autorização seja solicitada o mais rápido possível, dentro do prazo máximo de 24 horas. Se o pedido de autorização for rejeitado, o uso do monitoramento é suspenso com efeito imediato, e todos

os dados, bem como os resultados dessa utilização, são imediatamente descartados e eliminados.

Com o fim de resguardar a segurança e os direitos fundamentais envolvidos, cada vez que houver o uso do sistema de identificação biométrica à distância em tempo real, deve-se notificar a autoridade de fiscalização do mercado pertinente e a autoridade nacional de proteção de dados, as quais emitirão relatórios anuais à Comissão sobre a utilização desse sistema. Note-se que a legislação da UE criou mecanismos de supervisão, transparência e “dupla checagem” por diversas autoridades a fim de verificar o caráter estritamente excepcional da medida para salvaguardar os direitos das pessoas e evitar abusos e discriminações.

A propósito, insta salientar que identificação biométrica, para os fins estipulados no regulamento, refere-se ao reconhecimento automatizado de características humanas físicas, fisiológicas e comportamentais, tais como o rosto, o movimento dos olhos, a forma do corpo, a voz, a pronúncia, a marcha, a postura, a frequência cardíaca, a pressão arterial, o odor, as características da digitação, com o objetivo de verificar a identidade de uma pessoa comparando-se os dados biométricos desse indivíduo com os dados biométricos armazenados em uma base de dados de referência, independentemente de a pessoa ter ou não dado consentimento prévio.

Com o mapeamento de tais dados, seria possível criar um sistema de categorização biométrica com a classificação de pessoas a classes específicas com base nos seus dados biométricos, cujos aspectos poderiam abranger informações sobre sexo, idade, cor do cabelo, cor dos olhos, tatuagens, traços comportamentais ou de personalidade, língua, religião, pertencimento a uma minoria, orientação sexual ou política. Por certo, a coleta desses dados, sobretudo sem o consentimento da pessoa, deve ser proibida violar os direitos fundamentais, incluindo o direito à privacidade.

Por último, permite-se a verificação biométrica com o objetivo de autenticação, ou seja, para confirmar que uma pessoa é quem afirma ser a fim de que esse indivíduo possa acessar um serviço ou um local e desbloquear um dispositivo. De igual modo, o uso dos filtros nos serviços de redes sociais, ainda que acessem características faciais ou corporais do usuário, é permitido e não é proibido pela norma da UE.

3.2 Dos sistemas de IA de alto risco

O artigo 6º estabelece que são considerados sistemas de alto risco aqueles que envolvem as seguintes áreas: dados biométricos; educação e formação profissional; emprego e gestão de trabalhadores; acesso a serviços privados ou públicos essenciais; infraestruturas digitais críticas [*transporte e redes de abastecimento de água, gás, aquecimento ou eletricidade*] e de segurança; gestão da migração, do asilo e do controle de fronteiras; administração da justiça e processos democráticos; e aplicação da lei.

Nestes casos, deve-se permitir o registro automático de eventos durante a vida útil do sistema e a supervisão humana para prevenir ou minimizar riscos para a saúde, segurança e direitos fundamentais, além da obrigatoriedade de criar sistema de gestão da qualidade que assegure a conformidade com os requisitos do ordenamento.

Nas hipóteses em que se verificar que o sistema apresenta não conformidade formal com os requisitos do Regulamento, a autoridade competente poderá adotar medidas adequadas para restringir ou proibir a disponibilização no mercado do sistema de IA de risco elevado ou, ainda, garantir que o produto seja recolhido ou retirado do mercado [artigo 83].

Há, também, a obrigatoriedade de criar e manter um sistema de gestão de riscos contínuo, planejado e executado ao longo do ciclo de vida de um sistema de IA de risco elevado, devendo compreender, por exemplo, a identificação e análise dos riscos conhecidos e razoavelmente previsíveis que o sistema de IA de risco elevado pode representar para a saúde, a segurança ou os direitos fundamentais quando é utilizado em conformidade com a sua finalidade prevista, além de selecionar as medidas adequadas e específicas para minimizar esses riscos de forma eficaz.

Ainda, ressalte-se que o novo ordenamento prevê requisitos juridicamente vinculativos antes, durante e após a comercialização/disponibilização de modelos de IA de risco elevado na UE diante do impacto que podem efetivamente causar na saúde, na segurança e nos direitos fundamentais. Inclusive, estipula as responsabilidades de todos os atores envolvidos ao longo da cadeia de valor da IA [artigo 25º] de modo a individualizar as obrigações legais do distribuidor, do importador, do prestador, do responsável pela implementação do sistema ou outro terceiro, o que contribui para a uma responsabilização mais efetiva.

Por outro lado, os sistemas listados acima, que não representem risco significativo de danos à saúde, à segurança ou aos direitos fundamentais, não serão classificados como de risco elevado e desde que não influenciem, visceralmente, o resultado da tomada de decisões. Evidencia-se, portanto, que os elementos “saúde,

segurança e direitos fundamentais” servem como critérios centrais para a classificação de um sistema como de alto risco.

Importante registrar que antes de implementarem um sistema de IA de risco elevado, com exceção do sistema utilizado nas infraestruturas críticas, os responsáveis pela implantação que sejam organismos de direito público, ou entidades privadas que prestam serviços públicos e sejam responsáveis pela implantação de modelos de IA de acesso a serviços essenciais relacionados à avaliação da capacidade de solvabilidade de pessoas, de sua classificação de crédito ou de fixação de preços no caso de seguros de vida e de saúde, devem executar uma avaliação do impacto que a utilização desse sistema possa ter nos direitos fundamentais.

Para esse efeito, os responsáveis necessitam executar uma avaliação criteriosa, que inclua, dentre outros requisitos, as categorias de pessoas e grupos suscetíveis de serem afetados e as medidas a serem tomadas caso esses riscos se concretizem, incluindo os mecanismos de apresentação de queixas. Estas regras não são apenas uma precaução, mas refletem uma necessidade jurídica para assegurar que a implementação da IA em setores críticos seja feita de maneira ética, transparente e em conformidade com as normas que resguardam a saúde, a segurança e os direitos fundamentais dos indivíduos.

Em última análise, o regulamento estabelece um quadro jurídico robusto e detalhado que visa equilibrar os benefícios tecnológicos da IA com a proteção dos direitos fundamentais dos indivíduos. Ao classificar certos sistemas de IA como de "alto risco" – em áreas como saúde, segurança, educação, emprego, administração da justiça e serviços públicos essenciais – o regime jurídico reconhece os potenciais impactos significativos dessas tecnologias, não apenas em termos de eficiência e inovação, mas também nos direitos essenciais dos cidadãos.

4 A CIDADANIA ELETRÔNICA DO *HOMO DIGITALIS*

O *homo digitalis* é o indivíduo hiperconectado ao admirável mundo novo – e viciante – das plataformas digitais. Esse ser, ao ingressar no mundo virtual, adentra em uma dimensão em que, de certo modo, deixa de ser visto como um sujeito de direitos para se transformar em dados passíveis de negociação no novo capitalismo de vigilância.

Sob uma perspectiva sem precedentes e, praticamente, sem regulação cogente a nível mundial, o ambiente virtual tornou-se uma arena propícia para violação de direitos fundamentais dos usuários. Neste sentido, Zuboff (2021, p. 27) alerta que

[...] o capitalismo de vigilância é uma força nefasta comandada por novos imperativos econômicos que desconsideram normas sociais e anulam direitos básicos associados à autonomia individual e os quais são essenciais para a própria possibilidade de uma sociedade democrática.

O documentário “O dilema das redes” foi lançado, pela plataforma de *streaming* Netflix, com o *slogan* “especialistas em tecnologia e profissionais da área fazem um alerta: as redes sociais podem ter um impacto devastador sobre a democracia e a humanidade”.

Shoshana Zuboff e especialistas de gigantes da tecnologia, como Google e Facebook, relatam como as redes e plataformas digitais são minuciosamente projetadas para manter o usuário conectado pelo maior tempo possível, por meio de técnicas intencionais de sedução e de interação para mineração dos dados comportamentais do indivíduo com base em cliques, curtidas, compartilhamentos de conteúdo, etc.

As *big techs* não reconhecem que suas práticas podem violar os direitos do indivíduo, sustentam que instituem plataformas neutras (Sampaio; Furbino; Bocchino, 2021) e adotam o discurso “Não obrigamos ninguém a usar os nossos serviços nem violamos nenhuma lei. Se não gostam do que fazemos, os clientes deveriam ir embora” (Wood; Lehdonvirta, 2023). Ou seja, baseiam-se na premissa de que as pessoas aceitaram voluntariamente os Termos de serviços e de uso das redes digitais.

Ocorre que esses termos são elaborados unilateralmente pelas empresas, sem qualquer participação ou interferência do usuário nas cláusulas, sendo formulados com o objetivo exclusivo de atender os interesses econômicos das grandes corporações, ao mesmo tempo que as isentam de responsabilidade. Algumas plataformas, inclusive, condicionam o acesso irrestrito aos seus serviços à obrigatoriedade de concordância com esses termos.

Em muitos casos, a violação de direitos já começa quando a pessoa clica em “aceitar” os termos de uso, oportunidade em que seus dados pessoais, bancários, de localização e de preferências são mapeados e compartilhados com empresas ou para outros bancos de dados. A Netflix, por exemplo, informa, na Declaração de Privacidade, que os dados pessoais podem ser transferidos para outros países (Netflix)⁶.

O Regulamento (UE) 2024/1689 não prevê, expressamente, o conteúdo desses instrumentos contratuais, apesar desses termos se constituírem em verdadeiras armas

⁶ A Netflix informa sobre divulgação e transferência internacionais. Disponível em: <https://help.netflix.com/legal/personal-information-international-transfers>. Acesso em: 05 nov. 2024.

violadoras de direitos fundamentais, como a proteção de dados pessoais e o direito à privacidade.

Nesse cenário, em que subsistem conflitos entre os interesses econômicos das grandes empresas e os direitos fundamentais do cidadão, exsurge a premente necessidade de delinear os contornos da nova cidadania exercida no ciberespaço, denominada de “cidadania eletrônica” por Rodotá (2008, p. 145), com o intuito de reforçar a democracia e o Estado de direito.

Rodotá (2008, p. 144-145) defende que a sociedade de informação demanda novos instrumentos jurídicos, como a Carta dos Direitos da Informação [*Information Bill of Rights*], bem como que a privacidade constitui o elemento fundamental da cidadania e indispensável para a liberdade existencial nessa nova realidade, sobretudo quando as informações se tornam elementos de riquezas. Rodotá (2008, p. 144) sustenta que a mitigação da privacidade pode representar riscos para as liberdades individuais e, conseqüentemente, para a democracia.

Por isso, deve-se tutelar a privacidade como um direito de controlar o uso das informações pessoais [direito à autodeterminação informativa] e como um poder social de ditar como os sujeitos públicos e privados tratam os dados pessoais (Rodotá, 2008, p. 144, 149). Há, portanto, uma intrínseca relação entre privacidade, liberdade, igualdade e democracia, que devem ser resguardadas juridicamente, especialmente quando existe um desnível de poder entre os cidadãos e aqueles que coletam as informações.

Nesse toar, o universo digital se tornou palco não só de exercício de direitos civis, políticos e sociais, como o direito à liberdade de expressão e de acesso à informação, mas também de graves violações a direitos fundamentais. Por tal razão, instrumentos jurídicos devem ser criados para tutelar esses direitos de forma eficaz a fim de resguardar a própria democracia. Rodotá (2008, p. 158) defende que

A Internet e as suas transformações, e o ciberespaço devem permanecer disponíveis para permitir a livre formação da personalidade, o exercício da liberdade de expressão e de associação, o desenvolvimento de iniciativas cívicas, a experimentação de novas formas de democracia.

Assim, a cidadania eletrônica garantiria ao cidadão o acesso a serviços públicos e o respeito aos seus direitos fundamentais no espaço virtual, sobretudo a participação ativa, livre e autônoma na política. Noutras palavras, o *homo digitalis* teria liberdade de escolha e autonomia para tomar suas próprias decisões, sejam elas pessoais ou políticas,

livres da manipulação dos algoritmos e das *fakes news*, o que contribui para reforçar o regime democrático.

Tendo vista o grande impacto que a IA pode ter na sociedade e com arrimo na democracia e no Estado de Direito, o Regulamento 2024/1689 estipula que o novo regime jurídico deve ser desenvolvido em conformidade com os valores da União consagrados no artigo 2.º do Tratado da União Europeia (TUE), com os direitos e liberdades fundamentais consagrados nos Tratados e, nos termos do artigo 6.º do TUE, com a Carta.

Esse artigo aduz que a União reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia. A Carta prevê, como direitos fundamentais, os seguintes: Dignidade do ser humano; Cidadania, direito à vida; direito à integridade do ser humano; Direito à liberdade e à segurança; Respeito pela vida privada e familiar; Proteção de dados pessoais; Liberdade de pensamento, de consciência e de religião; Liberdade de expressão e de informação; direito à educação; igualdade; não discriminação; diversidade; defesa dos consumidores; proteção do ambiente; justiça.

Diante de tais premissas, ao se interpretar de forma sistêmica e harmonizada o arcabouço jurídico da União Europeia, verifica-se que são tutelados, pelo regulamento, os direitos à não discriminação, à privacidade, à proteção de dados pessoais, à liberdade e à igualdade, à defesa dos consumidores, à justiça e à proteção do meio ambiente.

De acordo com a nova legislação, o direito à privacidade e à proteção de dados pessoais tem de ser garantido ao longo de todo o ciclo de vida do sistema de IA, criando-se, para tanto, mecanismos de governação de dados. À título exemplificativo, esse mecanismo é usado quando se torna necessário tratar categorias de dados pessoais em situações de correção de enviesamentos em sistemas de alto risco, suscetíveis de afetar a saúde e a segurança das pessoas, de ter repercussões negativas nos direitos fundamentais ou de resultar em discriminações proibidas pelo direito da União.

Esse tratamento somente será possível em casos excepcionais [artigo 10], com a utilização de medidas rigorosas e restritivas de segurança para preservação da privacidade e desde que não seja possível a correção do enviesamento através do tratamento de dados sintéticos ou anonimizados. As categorias especiais de dados pessoais não podem ser transmitidas nem transferidas para terceiros, nem consultadas por esses terceiros, sendo eliminadas assim que o enviesamento tenha sido corrigido ou que os dados pessoais atinjam o fim do respectivo período de conservação.

Durante esse procedimento, os dados pessoais tratados devem estar seguros, protegidos e sujeitos a garantias adequadas, incluindo controles rígidos e uma

documentação criteriosa do acesso a esses dados, a fim de evitar uma utilização abusiva, além de assegurar que apenas tenham acesso a esses dados as pessoas autorizadas e com as devidas obrigações de confidencialidade.

Com isto, evidencia-se que a tutela da privacidade, idealizada por Rodotá (2008), encontra-se codificada em um aparato jurídico com instrumentos normativos sólidos para a proteção desse direito, bem como para evitar enviesamentos prejudiciais e a discriminação com riscos para os indivíduos, para a sociedade e para os valores democráticos e os direitos humanos.

As previsões regulamentares enaltecem a cidadania eletrônica porque estão em harmonia com os valores da União, que se funda no respeito à dignidade humana, à liberdade, à democracia, à igualdade, ao Estado de direito e ao respeito pelos direitos do Homem, incluindo os direitos das pessoas pertencentes a minorias. Estes valores são resguardados para garantir o pluralismo, a não discriminação, a tolerância, a justiça, a solidariedade e a igualdade entre homens e mulheres.

Contudo, em que pese a criação de diversos mecanismos de redução ou eliminação de riscos à saúde, à segurança e aos direitos fundamentais com o uso de sistemas de IA, o regulamento apenas estipulou nos artigos 85 e 87, como mecanismo de defesa do cidadão em caso de ocorrência de infração às disposições da nova lei, o direito de apresentar queixa à autoridade de fiscalização do mercado de forma genérica⁷.

Em conclusão, a cidadania eletrônica surge como uma resposta essencial e jurídica aos desafios impostos pela IA, reforçando-se o livre exercício de direitos fundamentais. O Regulamento (UE) 2024/1689, ao estabelecer mecanismos para salvaguardar esses direitos na dimensão virtual com a difusão da IA, representa um avanço significativo, alinhando-se aos valores democráticos e à proteção da dignidade humana. Contudo, a efetividade dessa tutela dependerá de uma implementação rigorosa

⁷ Artigo 85.º

Direito de apresentar queixa a uma autoridade de fiscalização do mercado

Sem prejuízo de outras vias de recurso administrativas ou judiciais, qualquer pessoa singular ou coletiva que tenha motivos para considerar que houve uma infração às disposições do presente regulamento pode apresentar uma queixa à autoridade de fiscalização do mercado competente.

Em conformidade com o Regulamento (UE) 2019/1020, essas queixas devem ser tidas em conta para efeitos da realização das atividades de fiscalização do mercado e tratadas em conformidade com os procedimentos específicos estabelecidos para o efeito pelas autoridades de fiscalização do mercado.

Artigo 87.º

Denúncia de infrações e proteção dos denunciantes

A Diretiva (UE) 2019/1937 aplica-se à denúncia de infrações ao presente regulamento e à proteção das pessoas que denunciam essas infrações.

e da criação de instrumentos mais específicos que garantam a transparência e o controle efetivo do cidadão sobre suas informações e sobre seus direitos.

A cidadania eletrônica, portanto, não deve ser vista apenas como uma ferramenta de acesso aos serviços digitais, mas como um mecanismo fundamental de fortalecimento da democracia, onde a privacidade, a autonomia e a igualdade sejam preservadas e respeitadas no ciberespaço.

CONCLUSÃO

A difusão do *Big Other*, decorrente da ditadura com os algoritmos realizada por grandes corporações tecnológicas, traz à tona desafios jurídicos e éticos para os direitos fundamentais dos cidadãos. A hiperconexão do *homo digitalis*, nesse novo contexto, expõe um conflito visceral entre os interesses econômicos das *big techs* e a proteção dos direitos fundamentais dos cidadãos, como a privacidade, a liberdade e a autonomia.

Nesse contexto, a presente pesquisa buscou investigar a cidadania eletrônica do *homo digitalis* como elemento fundamental da democracia e da salvaguarda de direitos fundamentais do indivíduo no ciberespaço.

Para tanto, no primeiro tópico deste artigo, enveredou-se no novo império ditado pelos algoritmos em prol dos interesses das empresas de tecnologia. Desse modo, chegou-se à conclusão de que na nova ordem digital, o homem não é visto como um sujeito de direitos, mas, sim, como o produto no capitalismo de vigilância, cuja liberdade de escolha e autonomia são tolhidas.

Na sequência, o segundo tópico versou sobre os aspectos mais relevantes do Regulamento (UE) 2024/1689 sobre inteligência artificial, perpassando pela abordagem jurídica com base nos riscos dos sistemas de IA. Esse novo regime jurídico, ao tratar da IA e seus impactos, oferece um marco regulatório importante mundial, pois estabelece medidas para salvaguardar direitos fundamentais, como a privacidade e a proteção de dados pessoais.

No terceiro e último tópico, a partir da análise do conceito de cidadania eletrônica proposta por Stefano Rodotà, percorreu-se sobre a importância de garantir ao *homo digitalis* a capacidade de exercer seus direitos no ambiente digital com autonomia e sem manipulação algorítmica. A tutela da proteção da privacidade e da

autodeterminação informativa são ferramentas essenciais para o fortalecimento da democracia e para a preservação da liberdade individual.

Reforçar a cidadania eletrônica reflete uma garantia jurídica e de democrática de que, no ciberespaço, os direitos humanos e a dignidade do indivíduo permanecem intocáveis, resguardando-se a liberdade e autonomia da pessoa sem manipulação algorítmica. Para tanto, as previsões regulamentares da nova legislação são cruciais para a construção de uma verdadeira cidadania eletrônica, protegida por normas jurídicas robustas a fim de salvaguardar os direitos e liberdades fundamentais, além de fortalecer os valores democráticos que sustentam a nossa sociedade.

Contudo, a eficácia dessa legislação depende de sua implementação rigorosa e da criação de instrumentos mais concretos que possibilitem o controle efetivo dos cidadãos sobre suas informações pessoais e sobre a transparência no tratamento de seus dados.

Na era digital, a verdadeira liberdade não está apenas em escolher o que consumir, mas em garantir que os dados, a privacidade e a autonomia não sejam os produtos a serem vendidos no capitalismo de vigilância.

REFERÊNCIAS

BAUMAN, Zygmunt. **Vigilância Líquida: diálogos com David Lyon**. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Editora Zahar, 2013.

CHEN, Heather; MAGRAMO, Kathleen. **Golpistas usam *deepfake* de diretor financeiro e roubam US\$ 25 milhões**. *CNN BRASIL*, 05 de fevereiro de 2024. Disponível em: Acesso em: 05 nov. 2024.

FLORIDI, Luciano; CABITZA, Federico. ***Intelligenza Artificiale - L'uso delle nuove machine***. *Prima edizione digitale: ottobre 2021*. Italia: Giunti Editore S.p.A./Bompiani, 2021.

GALINDO, Cristina. **Quando as empresas são mais poderosas que os países**. *El País*, Brasília, 07 nov. 2017. Disponível em: https://brasil.elpais.com/brasil/2017/11/03/economia/1509714366_037336.html. Acesso em 04 nov. 2024.

HAN, Byung-Chul. **No Exame: perspectivas do digital**. Tradução: Lucas Machado. Rio de Janeiro: Editora Vozes, 2018.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução: São Paulo: Companhia das Letras, 2018.

HARARI, Yuval Noah. **Nexus – Uma breve história das redes de informação, da Idade da Pedra à inteligência artificial**. Tradução: Berilo Vargas e Denise Bottmann. São Paulo: Companhia das Letras, 2024.

NETLIX. **Divulgação e transferências internacionais**. Disponível em: <https://help.netflix.com/legal/personal-information-international-transfers>. Acesso em: 05 nov. 2024.

O DILEMA das redes. Direção: Jeff Orlowski. Produção: Larissa Rhodes. Roteiro: Vickie Curtis, Davis Coombe e Jeff Orlowski-Yang. Boulder: Exposure Labs, 2020 (94 min.). Disponível em: <https://www.netflix.com/br/title/81254224> Acesso em: 03 nov. 2024.

PINTO, Felipe Chiarello de Souza; OLIVEIRA, Gabriela Franklin de. Não acredite em tudo que vê: *deepfake pornography* e responsabilidade civil no ordenamento jurídico brasileiro. **Revista Eletrônica Direito e Política** [Recurso Eletrônico], Itajaí, SC, v.18, n.2, 2023. Disponível em: <https://dspace.almg.gov.br/handle/11037/52217>. Acesso em: 05 nov. 2024.

RUSSELL, Stuart J. **Human Compatible. Artificial Intelligence and the Problem of Control**. London: Penguin, 2019.

SAMPAIO, José Adércio Leite; FURBINO MARQUES, Meire Aparecida; BOCCHINO, Lavínia Assis. Capitalismo de vigilancia y tecnopolítica: los derechos fundamentales de privacidad y libertad de expresión bajo ataque. **Opinión Jurídica**, [S. l.], v. 20, n. 42, p. 509–527, 2021. DOI: 10.22395/ojum.v20n42a21. Disponível em: <https://revistas.udem.edu.co/index.php/opinion/article/view/3589>. Acesso em: 3 nov. 2024.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024**. Bruxelas: Comissão Europeia, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L_202401689. Acesso em: 03 nov. 2024.

UNIÃO EUROPEIA. **CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA**. Nice: Parlamento Europeu, Conselho e Comissão Europeia, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 03 nov. 2024.

UNIÃO EUROPEIA. **TRATADO DA UNIÃO EUROPEIA**. Nice: Parlamento Europeu, Conselho e Comissão Europeia, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12016ME/TXT>. Acesso em: 03 nov. 2024.

VANDER MAELEN, Carl. *From opt-in to obligation? Examining the regulation of globally operating tech companies through alternative regulatory instruments from a material and territorial viewpoint*. **International Review of Law, Computers & Technology**, v. 34, n. 2, p. 183-200, 2020. DOI: 10.1080/13600869.2020.1733754.

Disponível em: <https://www.tandfonline.com/doi/full/10.1080/13600869.2020.1733754>.
Acesso em: 4 nov. 2024.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância. A luta por um futuro humano na nova fronteira do poder**. 1ª edição. Rio de Janeiro: Editora Intrínseca Ltda., 2021.

ZUBOFF, Shoshana (2018). *Big other*: capitalismo de vigilância e perspectivas para uma civilização de informação. No F., Bruno, B., Cardoso, B., M. Kanashiro, M., L., Guilhaon e L., Melgaço, L. (Orgs.). **Tecnologias da vigilância: perspectivas da margem**. (pp. 17-68). (H.M., Cardozo, et al., trans.). Boitempo.

WOOD, Alex J.; LEHDONVIRTA, Vili. *Platforms Disrupting Reputation: Precarity and Recognition Struggles in the Remote Gig Economy*. *Sociology*, v. 57, n. 5, pp. 999-1016, 2023.