INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 05 · n. 02 · maio/agosto 2024 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.5.n.2

05

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

IJDL – INTERNATIONAL JOURNAL OF DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FÓRUM
Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Rua Paulo Ribeiro Bastos, 211 – Jardim Atlântico – CEP 31710-430
Belo Horizonte/MG – Brasil – Tel.: (31) 99412.0131
www.editoraforum.com.br / E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil / Distribuída em todo o Território Nacional

IN61 International Journal of Digital Law – IJDL. – ano 1, n. 1 (abr. 2020) –.– Belo Horizonte: Fórum, 2020-.

Quadrimestral; Publicação eletrônica
ISSN: 2675-7087

1. Direito. 2. Direito Digital. 3. Teoria do Direito. I. Fórum.

CDD: 340.0285
CDU: 34.004

Coordenação editorial: Leonardo Eustáquio Siqueira Araújo
Capa: Igor Jamur
Projeto gráfico: Walter Santos
Revisão: Gabriela Sbeghen
Diagramação: Reginaldo César de Sousa Pedrosa

Sumário

Contents

EDITORIAL Nº 14

Chegamos ao décimo quarto número da *International Journal of Digital Law*. Desde o primeiro número da revista, temos procurado um elevado nível tanto em uma perspectiva material quanto formal. Cumprimos rigorosamente com todos os critérios para uma classificação no nível mais alto do Qualis Periódicos, além de vários outros requisitos das principais bases internacionais de indexação. Infelizmente, a precariedade do sistema de classificação da Capes, por intermédio do Qualis, nem sempre retratou de forma adequada a qualidade das revistas brasileiras na base.

De todo modo, a IJDL já tem demonstrado excelente desempenho no Google Metrics, sendo citada em diferentes periódicos científicos não só no Brasil como ao redor do mundo. Isso nos deixa muito felizes e orgulhosos do trabalho realizado.

Agradecemos à confiança da comunidade acadêmica e à frutífera parceria entre o Nuped – Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR e a Editora Fórum.

Emerson Gabardo
Editor-Chefe da IJDL

EDITORIAL Nº 14

We have reached the fourteenth issue of the International Journal of Digital Law. Since the journal's first issue, we have sought to achieve a high level of both material and formality. We have rigorously complied with all the criteria for classification at the highest level of Qualis Periódicos and several other requirements of the main international indexing databases. Unfortunately, the precariousness of the CAPES classification system, through Qualis, has not always adequately reflected the quality of Brazilian journals in the database.

In any case, IJDL has already demonstrated excellent performance in Google Metrics and is cited in various scientific journals not only in Brazil but around the world. This makes us very happy and proud of the work we have done.

We are grateful for the trust of the academic community and the fruitful partnership between NUPED – Center for Research in Public Policies and Human Development of PUCPR and Editora Fórum.

Emerson Gabardo
IJDL Editor in Chief

INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 05 · n. 02 · maio/agosto 2024 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.5.n.2

05

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

International Journal of Digital Law – IJDL
ISSN 2675-7087
DOI: 10.47975/digital.law.vol.5.n.2.melo

A regulamentação da proteção de dados pessoais e seus desafios no contexto da tragédia dos (anti)comuns – Evitando a tragédia da desconfiança

Regulating personal data protection and its challenges in the context of the (anti)commons tragedy – Avoiding the tragedy of distrust

Lígia Maria Silva Melo*
I Universidade Federal do Ceará (Fortaleza, Ceará, Brasil)
meloligia@gmail.com
https://orcid.org/0000-0001-7987-4381

Nélida Astezia de Castro Cervantes**
I Universidade Federal do Ceará (Fortaleza, Ceará, Brasil)
nelidacervantes@hotmail.com
https://orcid.org/0000-0003-0614-9300

William Magalhães Lessa***
I Universidade Federal do Ceará (Fortaleza, Ceará, Brasil)
williamlessa_1@hotmail.com
https://orcid.org/0000-0002-9692-4536

Como citar esse artigo/*How to cite this article*: MELO, Lígia Maria Silva; CERVANTES, Nélida Astezia de Castro; LESSA, William Magalhães. A regulamentação da proteção de dados pessoais e seus desafios no contexto da tragédia dos (anti)comuns – Evitando a tragédia da desconfiança. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 11-29, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.melo.

* Docente da Faculdade de Direito da Universidade Federal do Ceará (Fortaleza, Ceará, Brasil). Doutora em Direito Econômico e Desenvolvimento pela PUCPR. Mestra em Direito do Estado pela PUC-SP. Presidente do Instituto Cearense de Direito Administrativo – ICDA. Diretora do Instituto Brasileiro de Direito Administrativo – IBDA. Coordenadora Regional do Instituto Brasileiro de Direito. *E-mail*: meloligia@gmail.com.

** Docente da Faculdade de Direito da Universidade Federal do Ceará (Fortaleza, Ceará, Brasil). Doutora em Ciências Políticas pela Universidade de Lisboa (ISCSP). Mestra em Direito Constitucional pela UFC-CE. Coordenadora do Núcleo de Prática Jurídica da Faculdade de Direito da UFC-CE. *E-mail*: nelidacervantes@hotmail.com.

*** Mestrando do Programa de Pós-Graduação em Direito da Universidade Federal do Ceará (Fortaleza, Ceará, Brasil). Especialista em Direito Processual Civil pelo Centro Universitário Damásio de Jesus. *E-mail*: williamlessa_1@hotmail.com.

Recebido/Received: 26.08.2024 / August 26th, 2024
Aprovado/Approved: 28.09.2024 / September 28th, 2024

Resumo: O presente estudo busca realizar uma análise econômica dos modelos regulatórios da privacidade e proteção de dados pessoais, tomando por referência o clássico texto *A tragédia dos comuns*, a metodologia adotada partiu da literatura de referência nacional e estrangeira. Inicialmente, apresentou-se breve exposição das características e etapas da regulação acerca do tema para daí iniciar uma análise econômica da privacidade – seja como bem econômico, seja como lastro da confiança na economia da informação. O objetivo deste trabalho é analisar como o modelo da tragédia dos comuns pode auxiliar na crítica da regulação do tema e identificar melhorias e forma de operacionalizá-las. A relevância da pesquisa insere-se no contexto da necessidade de uma mais eficiente regulamentação da proteção de dados pessoais no Brasil e das dificuldades de um consentimento informado pelos titulares de dados pessoais face a relações assimétricas com os controladores e processadores. Concluiu-se que a missão regulatória segue incompleta, mostrando-se necessária a responsabilização dos controladores, e assim como o fomento da confiança dos titulares de dados. A partir desta realidade, foram apresentadas algumas propostas de soluções tecnológicas para fomentar essa confiança, na figura das chamadas PETs, tecnologias de aprimoramento de privacidade, mesmo considerando que a difusão dessas tecnologias esbarra na ausência de adesão por ausência de uma regulação vinculante acerca do tema.

Palavras-chave: Proteção de dados pessoais; tragédia dos comuns; regulamentação; sociedade da informação; tecnologia.

Abstract: This study seeks to carry out an economic analysis of regulatory frameworks for privacy and personal data protection, taking the classic text "The Tragedy of the Commons" as a reference. The methodology adopted was based on national and foreign reference literature. Initially, a brief presentation was made of the characteristics and stages of regulation on the subject, in order to begin an economic analysis of privacy – both as an economic good and as a basis for trust in the information economy. The aim of this work is to study how the "Tragedy of the Commons" model can help to critically investigate the regulation of the subject and identify improvements and ways of making them operational. The research is relevant in the context of the need for more efficient regulation of personal data protection in Brazil and the difficulties of informed consent by personal data subjects in the face of asymmetrical relationships with controllers and processors. In conclusion, the regulatory mission is still incomplete and there is a need to hold controllers accountable, as well as to foster the trust of data subjects. Based on this reality, some proposals were put forward for technological solutions to foster such trust, in the form of the so-called PETs, privacy enhancing technologies, even considering that the diffusion of these technologies comes up against the lack of adherence due to the absence of binding regulation on the subject.

Keywords: Personal data protection; Tragedy of the commons; Regulation; Information society; Technology.

1 Introdução

As constantes transformações, em nível mundial, têm apresentado reflexos nos mais diversos setores, quer sejam econômicos ou políticos. A partir da metade do século XX e início do século XXI. É evidente que a tecnologia foi responsável

por grande parte dessas transformações, contudo, junto aos avanços tecnológicos, surge a insegurança na proteção do que é disponibilizado na internet, sobretudo de dados pessoais.

Transacionar com base em dados pessoais para se ter acesso a diferentes tipos de produtos e serviços não é uma opção na sociedade da informação,[1] mas uma necessidade. Todavia, a economia da informação não implica uma renúncia automática da privacidade – devendo-se fugir de simplificações nesse sentido.

De acordo com dados do Banco Interamericano de Desenvolvimento (BID), em 2021, danos decorrentes de delitos cibernéticos alcançaram incríveis seis bilhões de dólares. Ademais, de acordo com pesquisas realizadas, menos de 50% (cinquenta por cento) da população mundial com acesso à internet acredita que a tecnologia melhorará sua vida, o que representa uma crescente falta de confiança no que tange à privacidade e à proteção de dados.[2]

A regulação do tema se sofisticou substancialmente nas últimas décadas, desde o enfoque em gigantescos bancos de dados estatais, evoluindo para dar lugar a um protagonismo do consentimento qualificado dos cidadãos titulares de seus dados.

Há muito a literatura de referência debate entre modelos de intervenção estatal forte e de autorregulação do setor pelas corporações controladoras e processadoras de dados pessoais – havendo relativo consenso na relevância da participação do titular dos dados mediante seu consentimento. Normalmente, esse consentimento é expresso nos famosos "avisos de privacidade" que aparecem ao se acessar *sites* e aplicações eletrônicas, pressupondo que o usuário leu e revisou extensas políticas de privacidade.

Nas palavras de Stefano Rodotà,[3] a questão não é mais "regulação, sim ou não", pois isso há muito foi superado. Trata-se, na realidade, de como atribuir um valor orientador para essa regulação, para o futuro. Para formular categorias e conceitos envolvendo contratantes hipossuficientes e sua privacidade, cujo sistema de tutela em grande parte ainda remonta a uma época em que a informação não era um recurso central para a economia e para a sociedade.

---

1 Termo aqui adotado na acepção de Manuel de Castells: "O termo sociedade da informação enfatiza o papel da informação na sociedade [...] Ao contrário, o termo [sociedade] informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico". *Vide*: CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2005. p. 64-65.

2 BANCO INTERAMERICANO DE DESENVOLVIMENTO; ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Cibersegurança*: riscos, avanços e o caminho a seguir na América Latina e no Caribe. Relatório de Cibersegurança. 2020. Disponível em: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

3 RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução de Danilo Doneda e Lucial Cabral Doneada. Rio de Janeiro: Renovar, 2008. p. 57.

O presente estudo pretende fazer uma breve análise da evolução dos marcos e modelos regulatórios sobre privacidade e proteção de dados pessoais e correlacioná-la com um modelo clássico de análise econômica, chamado *tragédia dos comuns*, de Garrett Harding.

A literatura existente traz interessantes contributos correlacionando o modelo a análises da privacidade como um bem econômico e sua função na geração e manutenção de confiança na sociedade, servindo como premissa para criticar modelos regulatórios e pensar em contribuições.

Nesse contexto, o estudo tem como objetivo central analisar como o modelo da *tragédia dos comuns* pode auxiliar na crítica da regulação do tema e identificar melhorias e forma de operacionalizá-las.

Parte do desafio é vislumbrar os titulares de dados pessoais e da privacidade como *stakeholders* (interessados) fundamentais nas transações informacionais e cuja confiança é fundamental para o sustento e sucesso da economia da informação, pensando em maneiras de romper as assimetrias entre estes e os controladores e processadores de dados, representados pelo Estado e pelas grandes corporações – especialmente no caso brasileiro.

A metodologia proposta será qualitativa e aplicada, tendo por procedimento a pesquisa analítico-descritivo da literatura de referência (artigos científicos, livros, periódicos), com a técnica proposta sendo a pesquisa bibliográfica e documental.

2 A evolução dos marcos regulatórios de proteção de dados pessoais

O presente estudo organizará a regulamentação da privacidade e da proteção de dados pessoais, por meio da sua evolução histórica em *gerações*, seguindo o critério de Viktor Mayer-Schönberger –[4] que as divide em quatro gerações – com as contribuições de Bruno Bioni[5] e Danilo Doneda[6] acerca do tema.

Cumpre ressalvar que a análise de Mayer-Schönberger se limita ao universo norte-americano e europeu, pelo que não reflete a evolução da matéria em todo o mundo.

4 MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection. *In*: ROTENBERG, Marc; AGRE, Philip E. *Technology and privacy*: The new landscape. [s.l.]: [s.n.], 1998. p. 219.

5 BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 170-173.

6 DONEDA, Danilo César Maganhoto. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2020. p. 166-169.

Geração	1ª – Normas de proteção para dados	2ª – Proteção contra ofensores maiores e diferentes	3ª – O direito à autodeterminação informativa	4ª – Perspectivas holísticas e setoriais
Características	– Receio de uma realidade orwelliana de controle estatal por meio de dados. – Enfoque na função social do processamento de dados, não na proteção individual. – Necessidade de autorização governamental para criação de grandes bancos de dados.	– Proteção de direitos individuais (privacidade como um direito de ser "deixado só"). – Obrigação de o titular escolher entre exclusão social e transações informacionais.	– O direito do indivíduo de definir quais dados e em que medida serão processados. – Pressuposição do exercício de direitos. – Proteção de dados continua sendo um direito reservado a poucos. – Surgimento das autoridades nacionais de proteção de dados.	– Certos tratamentos de dados recebem maior regulação independentemente do consentimento (*e.g.*, dados sensíveis). – Preocupação com o equilíbrio entre titular e controlador de dados. – Setorização da matéria (proteção de dados para a saúde, para a administração pública etc.). – Permanece o protagonismo do consentimento.
Tecnologia	Bancos de dados centralizados estatais.	Corporações privadas adquirem os meios para criar e manter grandes bancos de dados. Início de trocas internacionais de dados baseadas em "reciprocidade".	Disseminação dos bancos de dados interligados e dificuldade em se localizar onde se realizava efetivamente o tratamento.	Disseminação de políticas de privacidade e avisos de consentimento.
Marco legal	Lei Estadual de Proteção de Dados de Hesse (1970).	Estatuto de proteção de dados francês (1978).	Decisão do Tribunal Constitucional alemão sobre o censo (1983). Convenção nº 108 do Conselho da Europa (1980).	*General Data Protection Act* (GDPR, 2016).
Outros exemplos	Estatuto de Proteção de Dados do Estado de Reno-Pfalz (1974). *Privacy Act* estadunidense (1974).	Estatutos de proteção de dados austríaco e dinamarquês.	Ato de Registro de Pessoas Naturais, Finlândia (1987).	LGPD brasileira (2018).

Pode-se perceber que o modelo adotado em *gerações* não é suficiente para esclarecer o processo evolutivo dos marcos regulatórios em todas as instâncias.

No Brasil, por exemplo, o processo de regulação das leis de privacidade e proteção de dados seguiu um caminho distinto. A própria Constituição de 1988 trouxe dispositivos esparsos acerca do tema, como exemplo: o direito fundamental à privacidade (art. 5º, X, CF); mecanismos de acesso e retificação de dados, como *habeas data* (art. 5º, XXXIV, a); direito de petição (art. 5º, LXXII); acesso à informação na administração pública (art. 5º, XXXIII, 37, §2º, III).[7]

Quanto à legislação infraconstitucional, verifica-se que o Código de Defesa do Consumidor (Lei nº 8.072/1990) –[8] a exemplo da legislação estadunidense anterior – trouxe parâmetros para bancos de dados consumeristas (art. 43); a Lei de Acesso à Informação (Lei nº 12.257/2011)[9] foi importantíssima para a transparência de dados pessoais ou não tratados pela administração pública. O Marco Civil da Internet (Lei nº 12.965/2014),[10] por sua vez, regulamentou os provedores de internet e trouxe uma promessa de regulamentação acerca da proteção de dados pessoais (art. 10).

Esta regulação finalmente veio com a promulgação da LGPD –[11] já considerada uma lei da chamada quarta geração, vez que surgida e assemelhada ao *General Data Protection Regulation* (GDPR) europeu. Todavia, os últimos desdobramentos da regulação da proteção de dados no país vieram com o ingresso do Brasil no Comitê Observador da Convenção nº 108,[12] marco legal mundial de compromisso com a proteção de dados, que elevou a Autoridade Nacional de Proteção de Dados

---

7 BRASIL. *Constituição da República Federativa do Brasil de 5 de outubro de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 jun. 2022.

8 BRASIL. *Código de Defesa do Consumidor*. Lei nº 8.078 de 11 de setembro de 1990. Ementa: Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 1º jun. 2022.

9 BRASIL. *Lei de Acesso à Informação*. Lei nº 12.527 de 18 de novembro de 2011. Ementa: Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 1º jun. 2022.

10 BRASIL. *Marco Civil da Internet*. Lei nº 12.965 de 23 de abril de 2014. Ementa: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1º jun. 2022.

11 BRASIL. *Lei Geral de Proteção de Dados*. Lei nº 13.709 de 14 de agosto de 2018. Ementa: Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1º jun. 2022.

12 Importante ressalvar que o Brasil ainda não ratificou a Convenção, sendo membro de seu Comitê Observador que se reúne em Estrasburgo 2 vezes ao ano para debater questões mundiais acerca do tema. *Vide*: BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. ed. 1. fev. 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais#:~:text=0%20Brasil%20n%C3%A3o%20%C3%A9%20signat%C3%A1rio,de%20prote%C3%A7%C3%A3o%20de%20dados%20pessoais. Acesso em: 10 jun. 2022.

ao nível de autarquia autônoma[13] e incitando a promulgação da Emenda Constitucional nº 115/2022.

A constitucionalização da proteção de dados pessoais não é medida que todos os países tomam, porém, no caso brasileiro, a EC nº 115/2022[14] não procurou apenas acrescer nova garantia ao rol do art. 5º (novo inc. LXXIX), mas principalmente uniformizar a competência legislativa acerca da matéria, tornando-a competência exclusiva da União (novo art. 21, XXVI).

Na América Latina, verifica-se que Argentina e Uruguai lideraram na regulamentação matéria, já possuindo regramentos consolidados em seus ordenamentos acerca do tema há bastante tempo. No caso argentino, também se optou por constitucionalizar a proteção aos dados pessoais (art. 43, §3º, da Constituição Federal argentina) ainda em 1994, com a promulgação da Lei de Proteção de Dados Pessoais (Lei nº 25.326) em 2001, regulamentada pelo Decreto nº 1.558. Em 2019, houve a adesão da Argentina à Convenção nº 108.[15]

O Uruguai, a seu turno, não constitucionalizou esse direito, porém há muito mantém um regramento coerente sobre a proteção de dados pessoais. Promulgou sua Lei de Proteção de Dados Pessoais em 2018 (Lei nº 18.331), regulamentando-a no ano seguinte (via Decreto nº 414), aderindo à Convenção nº 108 ainda em 2012. Com o lançamento do GDPR europeu em 2018, o Uruguai tão somente realizou adaptações em seu ordenamento por via do Decreto nº 64/2020.

Malgrado os diferentes processos regulatórios, a literatura segue constatando o grande protagonismo do consentimento do titular como um dos pilares da regulamentação da privacidade e da proteção de dados pessoais. Isso traz grandes implicações para o sucesso das normas, uma vez que permanecem fortemente dependentes de decisões individuais para que a proteção seja efetiva.

Para os objetivos do presente estudo, será útil fazer uso de um modelo econômico de análise para estudar as repercussões de decisões de agentes individuais sobre direitos comuns a todos.

3 A tragédia dos (anti)comuns aplicada à privacidade e à proteção de dados pessoais

Em 1968, no artigo *A tragédia dos comuns*, Garrett Harding[16] propôs um modelo de análise acerca da maneira como indivíduos, agindo em interesse próprio,

[13] Isso ocorreu com a publicação da MP nº 1.124/2022, que torna a ANPD autarquia federal especial.

[14] SENADO FEDERAL DO BRASIL. *Proposta de Emenda à Constituição nº 17/2019*. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline. Acesso em: 13 jun. 2022.

[15] DATA PROTECTION LAW OF THE WORLD. *Legislação*. Disponível em: https://www.dlapiperdataprotection.com/index.html. Acesso em: 2 jun. 2022.

[16] HARDIN, Garrett. The tragedy of the commons: the population problem has no technical solution; it requires a fundamental extension in morality. *Science*, v. 162, n. 3859, p. 1243-1248, 1968.

podem esgotar um recurso natural comum e limitado, caso regras não sejam estabelecidas. O exemplo era de pecuaristas explorando um pasto coletivo – eventualmente todos o exploravam até nada restar. A criação do direito à propriedade seria uma forma de romper o impasse e assegurar um uso razoável dos bens coletivos.

Em contraste, a literatura propôs também o cenário inverso, em que o excesso de regras cria uma tragédia dos "anticomuns", no qual poucos ou ninguém conseguem acessar bens pela existência de demasiadas limitações

A ideia da racionalidade do jogo busca explicar como os indivíduos, que compõem as organizações e instituições sociais, agem individualmente, por meio do cálculo consciente da sua racionalidade, para atingir seus objetivos pessoais. Costa, corroborando esse entendimento, explicita que "Indivíduos, políticos, burocratas, empresários, partidos e o próprio governo (ou quem o representa) agem em função de seus próprios interesses",[17] contudo, apenas os indivíduos decidem, já que a sociedade, o Estado e o governo não têm preferências, sendo a escolha pública a soma das preferências individuais. A ação racional é a que foi eleita, dentre as várias possíveis, como a melhor pelo ator, exprimindo suas preferências, desejos e crenças.[18]

A premissa da teoria da escolha racional é a de que o valor agregado[19] à sociedade se baseia na soma de todas as escolhas feitas pelos indivíduos, que se confrontam com várias alternativas possíveis de ação, os quais escolhem de acordo com os seus interesses e limitações.

Os seres humanos, na realidade, não se comportam, exatamente, como prescreve a teoria da escolha racional; contudo, os indivíduos tendem a reconhecer a força normativa da racionalidade, e isso influencia as suas ações — que se aproximam, ao menos um pouco, daquilo que criaturas de racionalidade ideal fariam nas mesmas circunstâncias. O comportamento é regido pela necessidade de sobrevivência e crescimento das instituições sociais nas quais as regras são seguidas e desempenhadas.[20]

Embora o indivíduo conheça o ambiente (mercado) e otimize suas ações para atingir os fins desejados, essa teoria considera, também, a falibilidade humana. Nesse sentido, a teoria da escolha racional considera que a racionalidade é limitada ao cognitivo (racionalidade limitada) fruto da coleta e processamento de informações

[17] COSTA, Frederico Lustosa da. Bases teóricas e conceituais da reforma dos anos 1990: crítica do paradigma gerencialista. *Revista Brasileira de Administração Política*, 2.2. p. 79.

[18] FEREJOHN, John; PASQUINO, Pasquale. The countermajoritarian opportunity. Universidade da Pensilvânia. *Pan Carey Law*, v. 13, p. 353, 2010.

[19] Valor agregado é o valor criado por um agente econômico a um bem, quando este é modificado durante o processo produtivo. É o valor que o processo produtivo adiciona a determinado bem.

[20] FEREJOHN, John; PASQUINO, Pasquale. A teoria da escolha racional na ciência política: conceitos de racionalidade em teoria política. *Revista Brasileira de Ciências Sociais*, v. 16, p. 5-24, 2001.

pelo homem.[21] A teoria também encontra interessante aplicação na análise de diferentes políticas públicas,[22] mostrando-se oportuna especialmente quando a política brasileira de proteção de dados pessoais está literalmente sendo formulada e consolidada pela ANPD, pelos titulares e pelos controladores e processadores de dados no país.

João Luís Nogueira Matias e Afonso de Paula Pinheiro Rocha aplicam o modelo de Garrett Harding à evolução do direito da propriedade, explicando que retrata um cenário em que os benefícios da atividade econômica são internalizados por apenas alguns pecuaristas e os custos externalizados para os demais produtores, que não poderão fazer uso do pasto. A criação de um regime de propriedade para parametrizar o uso racional do recurso comum é uma das maneiras para romper esse impasse:[23]

> Os direitos de exclusividade/propriedade são necessários e surgiram exatamente para delimitar o uso desses recursos. Retornando ao exemplo dos terrenos baldios, se os criadores de gado delimitarem as áreas, irão internalizar os benefícios referentes ao seu terreno sem onerar os terrenos designados para os outros.

Se o direito à propriedade é uma das maneiras de se romper o impasse gerado pelas disputas em torno de bens comuns e livremente acessíveis na sociedade, a absolutização da propriedade – típica dos momentos (neo)liberais – pode trazer um outro tipo de tragédia, a chamada tragédia dos anticomuns ou antibaldios.[24] Os autores oferecem um exemplo brasileiro bem peculiar: o de concentração fundiária em prejuízo da máxima eficiência na utilização da terra em favor de outras culturas.

Noutras palavras, a propriedade como ferramenta regulatória – como todo remédio – depende de sua *dosagem* para alcançar melhores efeitos ou mesmo para evitar a criação de outros entraves.

Fairfield e Engels, por sua vez, aplicaram o modelo da tragédia dos comuns para analisar a privacidade e a proteção de dados pessoais como bens comuns da sociedade. Nessa perspectiva:[25]

---

21 CYERT, R.; MARCH, J. *A behavioral theory of the firm*. Englewood Cliffs: Prentice Hall, 1963.

22 CERVANTES, Nélida Astezia Castro. *A influência do TRIPS no Programa da SIDA no Brasil*: uma investigação no âmbito da perspectiva neoinstitucional da teoria da escolha racional. Tese (Doutorado em Ciências Sociais) – Universidade de Lisboa, Lisboa, 2021. Disponível em: https://www.repository.utl.pt/handle/10400.5/21855. Acesso em: mar. 2023.

23 MATIAS, João Luis Nogueira; ROCHA, Rocha. *Repensando o direito de propriedade*. [s.l.]: [s.n.], 2006. p. 13-14.

24 HELLER, Michael. The tragedy of the anti-commons: property in the transition from Marx to Markets. *Harvard Law Review*, n. 111, jun. 1997.

25 FAIRFIELD, Joshua A. T.; ENGEL, Christoph. Privacy as a public good. *Duke LJ*, v. 65, 2015. p. 423. Tradução livre pelo autor. No original: "Translated to privacy, the public-goods model assumes that at least some individuals calculate the following way: If I disclose information, I will receive a private benefit— access to

> Em verdade, nós defendemos que a privacidade é um bem público no sentido literal da literatura econômica. A privacidade pode ser vítima de dilemas sociais. [...] E sem uma intervenção ponderada, as decisões informadas de indivíduos sobre a privacidade tendem a reduzir a privacidade de todos, mesmo se todos apreciarem-na igual e intensamente.

Para Fairfield e Engels, portanto, a privacidade e a consequente necessidade de proteção dos dados pessoais dos indivíduos seriam bens econômicos do tipo não exclusivos (*nonexcludable*, no sentido de disponíveis a todos) e não competitivos (*non-rivalrous*, no sentido de que seu consumo não limita o consumo de outros). E aqui os autores reconhecem o desafio da economia baseada em produtos e serviços informacionais como geradores da sensação nos indivíduos de que, malgrado seu desejo pessoal por privacidade, não a terão de toda forma, sendo os possíveis prejuízos futuros e difusos –[26] a exemplo de um futuro vazamento de dados.

Os autores verificam que a política de proteção de dados pessoais tem se posicionado no sentido de empoderar os indivíduos – tomando-os como principais interessados (*stakeholders*) na tutela de sua privacidade e dados – a despeito de certo niilismo em relação à viabilidade de uma efetiva proteção. Essa proteção tem se manifestado em uma abordagem individualista, ou seja, voltada à revisão de políticas de privacidade extensas, manifestação do consentimento e, eventualmente, o manejo do direito de acesso ou à deleção dos dados tratados.

Todavia, tal abordagem individualista está sujeita às heurísticas e vieses clássicos[27] que atingem o indivíduo, alcançando efeitos cada vez menores, pelo que Farfield e Engels propõem uma abordagem mais voltada à interação de grupos de indivíduos:[28]

---

an online site or service, for example. This imposes a cost on me, based on the personal information I have given up, and it imposes a cost on everyone because I have contributed to the overall lack of privacy in the culture. Yet as long as the sum of my direct costs and my share of the social costs (resulting from my own release of private information) is less than the private benefit I gain, I will choose to give up information to access the site or service. Thus, it makes sense to examine privacy as a social construct, subject to the problems of social production.185 Indeed, we contend that privacy is a public good as that term is strictly defined in the economics literature. Privacy will fall prey to social dilemmas. In weighing important decisions about privacy, individual and group incentives diverge. And without measured intervention, individuals' fully informed privacy decisions tend to reduce overall privacy, even if everyone cherishes privacy equally and intensely".

[26] FAIRFIELD, Joshua A. T.; ENGEL, Christoph. Privacy as a public good. *Duke LJ*, v. 65, 2015. p. 425.

[27] Fala-se no "paradoxo da privacidade", os indivíduos declaram se preocupar com sua privacidade quando questionados, mas falham em agir quando necessário. Para maiores informações, *vide*: GERBER, Nina; GERBER, Paul; VOLKAMER, Melanie. Explaining the privacy paradox: A GERBER, Nina; GERBER, Paul; VOLKAMER, Melanie. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, v. 77, p. 226-261, 2018.

[28] FAIRFIELD, Joshua A. T.; ENGEL, Christoph. Privacy as a public good. *Duke LJ*, v. 65, 2015. p. 457. Tradução livre pelo autor. No original: "This Article proposes giving groups tools for this struggle. Policymakers should consider the size, composition, and cohesion of online groups when they attempt to create an environment conducive to privacy protection. Tools should not be centered on individual rights of review and deletion,

> Os responsáveis pelas políticas de proteção de dados – públicos e particulares – deveriam enfocar no tamanho, composição e coesão de grupos online ao tentar criar um ambiente condutor para a proteção da privacidade. Tais ferramentas não devem enfocar em simples revisão e deleção, que já se mostraram pouco efetivas. Em verdade, deveriam enfocar na comunicação de grupos, sanções e no fomento de gamificação[29] e no senso de comunidade.

Portanto, assim como a propriedade individual, extremada ou livre de parâmetros como a função social, falha em tutelar bens comuns e caros à sociedade – a proteção de dados pessoais e da privacidade também depende de mecanismos sociais e jurídicos mais sofisticados que o empoderamento dos indivíduos para consentirem ou não no tratamento de seus dados. A proposta dos autores supramencionados enfoca em estratégias de grupo para evitar maior intervenção regulatória estatal ou mantê-la em um mínimo possível.

Dennis Hircht, a seu turno, critica a abordagem anterior, apontando uma omissão importante na análise: a ausência das grandes corporações na análise do problema da privacidade e do consentimento emanado por indivíduos e/ou grupos de indivíduos. Segundo este autor, o centro do problema estaria nos principais interessados em explorar a privacidade e a proteção de dados como bens comuns, interiorizando os benefícios e externalizando os custos. As corporações cumpririam esse papel na economia da informação.

Embora reconheça a contribuição de Fairfield e Engels na superação de um marco regulatório excessivamente focado no indivíduo (mediante avisos e políticas de privacidade), em favor de modelos que favoreçam a ação coletiva (reitere-se, focados, na sanção, comunicação de grupos e gamificação), Hircht entende que tais medidas não seriam suficientes:[30]

---

which have proven largely ineffective. Rather, tools should focus on group communication, sanction, and fostering a sense of repeat play and community. Even the way that we speak about the nature of the problem can have an impact on whether people cooperate to produce the public good of privacy".

29 Nota de tradução: o original tratava de *repeat play*, como interações sucessivas entre os titulares de dados pessoais e seus direitos, com finais indeterminados, de maneira a criar uma experiência no titular acerca da defesa de seus interesses relacionados à privacidade e proteção de dados.

30 HIRSCH, Dennis D. Privacy, public goods, and the tragedy of the trust commons: a response to professors Fairfield and Engel. *Duke LJ Online*, v. 65, 2015. p. 67. Tradução livre pelo autor. No original: "The overuse of personal information is leading to a tragedy of the commons but it is not the one that Fairfield and Engel identify. Instead, it is a tragedy of the trust commons. All economies depend on trust. 'We trust that merchants will accept the small, green pieces of paper that we've earned in exchange for goods and services. We trust that airplanes will arrive safely and to the correct airport. We trust that professionals in our service will act in our best interest…' The information economy is no different. When we engage in a digital transaction, visit a Web site, enter a search query, or make a purchase from an online store, we trust the provider to supply us with goods and services that will not hurt us, just as we do in the brick-and-mortar economy".

> A exploração excessiva de dados pessoais está levando a uma tragédia dos comuns, mas não uma do tipo que Fairfield e Engel identificam. Na verdade, é uma tragédia da confiança comum. Todas as economias dependem de confiança. Confiamos que comerciante aceitarão pequenos pedaços de papel verde que recebemos em troca de bens e serviços. Confiamos que aviões chegarão segura e pontualmente. Confiamos que profissionais a nosso serviço atuarão em nosso melhor interesse... A economia da informação não é diferente. Quando nos engajamos numa transação digital, visitamos um site na *Web*, fazemos uma busca, ou procuramos um produto virtualmente, confiamos que o controlador de dados nos oferecerá produtos e serviços que não nos prejudicarão, assim como na economia tradicional.

Em um cenário hipotético, caso a confiança em torno das transações baseadas em privacidade e proteção de dados seja perdida, as pessoas podem começar a reter tais dados pessoais ou mesmo passar a oferecer dados falsos ou incompletos, gerando uma crise de confiança semelhante à crise de 2008 nos mercados financeiros. No cenário atual, porém, uma tragédia de anticomuns nesse contexto parece improvável, mas certamente não se apresenta impossível.

A título de exemplo, diferentes pessoas utilizaram a proteção de dados pessoais conferida pela legislação para dados médicos, considerados sensíveis, como uma maneira de recusar informações sobre a participação ou não em campanhas de vacinação durante a pandemia de Covid-19.[31]

A economia da informação, portanto, baseia-se em confiança digital, que dá ensejo a transações baseadas nos dados pessoais dos cidadãos – essa confiança sim seria um bem de livre acesso e parcialmente competitivo (no sentido de que, em havendo sucessivas violações e vazamentos, os titulares de tais dados podem começar a retê-los ou não os compartilhar adequadamente).

Embora não opte por um modelo particular, Hircht relaciona modelos regulatórios que contemplam as corporações, baseados na autorregulação das empresas, regulamentação estatal ou modelos mistos combinando ambos.

Outra forma de classificar tais modelos seria baseada no *design* do tratamento de dados, exigindo tipos específicos de aviso de privacidade para determinados tipos de tratamento de dados; ou na *performance* de segurança do tratamento, que determinam que as empresas evitem certos tipos ou níveis de risco, mas deixam-nas livres para escolher como atingir tais níveis de segurança.[32]

---

[31] HALDER, Steve. Is it a HIPAA Violation to Ask for Proof of Vaccine Status? *HIPAA Journal*, Dec. 25, 2021. Disponível em: https://www.hipaajournal.com/is-it-a-hipaa-violation-to-ask-for-proof-of-vaccine-status/. Acesso em: 28 jun. 2022.

[32] HIRSCH, Dennis D. Privacy, public goods, and the tragedy of the trust commons: a response to professors Fairfield and Engel. *Duke LJ Online*, v. 65, 2015. p. 12-13.

Em 2021, nos 40 anos da Convenção nº 108, contemplando os avanços europeus na regulação da privacidade e proteção de dados pessoais, Mayer-Schönberger[33] propôs que o próximo marco regulatório para fomentar a confiança na economia da informação seria a garantia de *accountability*, ou seja, da responsabilidade de todos os envolvidos nesse complexo normativo que vem sendo instalado no mundo há décadas:

> Há uma última razão para mudar nossa atenção para enfocar em responsabilidade, e isso se relaciona a todos nós. Se dizemos a pessoas que elas têm poder em teoria, mas na prática percebem que são frequentemente vítimas de abusos, não agentes de mudança, elas normalmente se afastam e desconfiam do uso de dados pessoais.

O autor ainda ressalva que, sem confiança nas instituições e na capacidade coletiva de criar mecanismos de tutela eficaz para a proteção dos dados pessoais, às vésperas do aniversário da Convenção nº 108, haveria o risco de se estar inaugurando uma nova era da ignorância.

Partindo destas premissas, vê-se que, malgrado acentuados avanços na regulação de privacidade e proteção de dados, ainda não se pode dar por acabada a missão regulatória, nem mesmo nos sistemas mais antigos, como o europeu.

Surge o questionamento de como países cuja preocupação com a proteção de dados foi mais tardia podem operacionalizar a tutela deste direito, constitucionalizado no caso brasileiro, gerando a confiança e a responsabilidade de que trata Mayer-Schönberger. A literatura apresenta algumas ideias nesse sentido.

4 Operacionalizando a privacidade e a proteção de dados pessoais

Na evolução dos marcos regulatórios, ficou bastante evidente a correlação entre a evolução das tecnologias e das normas correspondentes. Os telefones e computadores portáteis distribuíram os riscos e os benefícios da economia da informação em escala global e têm sido acompanhados por políticas de privacidade e técnicas de segurança cada vez mais sofisticadas.

Bruno Bioni, embora reconheça os esforços dos reguladores e da própria indústria em tornar o consentimento do titular de dados pessoais menos automático e mais consciente, critica fortemente a viabilidade de um modelo regulatório baseado em repetidas decisões do indivíduo acerca do tratamento de dados em cada *site*

[33] MAYER-SCHÖNBERGER, Viktor. Paradigm shift. *Computer Law and Security Review*, v. 40, 2020. p. 3.

ou aplicação que utiliza. Identifica permanecer na prática uma forte assimetria em controlador e titular de dados, havendo uma hipervulnerabilidade do segundo.[34]

O modelo regulatório de proteção de dados pessoais no país, para ser humanista e realizar os objetivos da Constituição Federal, precisa estar centrado na figura do titular dos dados pessoais. Logo, cabe à Administração Pública se pautar em dispositivos legais voltados ao desenvolvendo humano e numa "atuação planejada e, também, regulatória, firme na condução de comportamentos que possam se reverter em ganhos coletivos",[35] noutras palavras, no empoderamento do grupo de titulares na condição de cidadãos em rede, que estão no exercício de seu direito fundamental de ver protegidas suas projeções pessoais (como nome, endereço, dados sensíveis e diversos outros) no uso constante e inevitável das TICs.

Uma interessante proposta nesse sentido é mediante a utilização das chamadas *Privacy Enhancing Tecnologies* (PETs), tecnologias de aprimoramento da privacidade para facilitar a árvore de decisões do titular de dados como usuário dessas tecnologias.

O *World Wide Web Consortium* (W3C) é uma entidade privada que advoga a defesa de tecnologias de privacidade para preservação da autonomia e liberdade do usuário da internet. Nesse sentido, o órgão já propôs diferentes técnicas para facilitar a manifestação do consentimento pelo usuário:

a) Tecnologias *Do Not Track* (DNT) – o "não rastreio": partindo da ideia de *opt-in* e *opt-out*, tratar-se-ia de uma tecnologia vinculada aos navegadores de internet (Google Chrome, Firefox, Windows Edge e outros) para permitir ao usuário "aceitar" ou "recusar" os infinitos *cookies* e outros rastreadores virtuais de suas atividades antes ou durante a navegação *no próprio navegador* e em caráter geral, não mais precisando reiterar essa decisão a cada acesso,[36] o próprio navegador comunicaria essa decisão a cada acesso, reduzindo a carga decisória do usuário.
b) A *Platform for Privacy Preferences* (P3P) ou Plataforma para Preferências de Privacidade – mais sofisticada que a primeira tecnologia proposta, mas também vinculada ao navegador utilizado para se acessar a internet, a P3P funciona como uma análise automatizada de políticas de privacidade. O usuário preencheria um breve questionário de suas preferências de privacidade e proteção de dados pessoais e a plataforma tomaria as decisões adequadas de acordo com a política de privacidade de cada *site* ou aplicação visitada.

[34] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 219-220.
[35] CASIMIRO, Lígia Maria Silva Melo de; CARVALHO, Harley. Para cidades justas, em rede e inteligentes: uma agenda pública pelo direito à cidade sustentável. *International Journal of Digital Law*, Belo Horizonte, ano 2, n. 1, p. 199-215, jan./abr. 2021. p. 201. DOI: 10.47975/IJDL/1casimiro.
[36] SINGER, David. Everything you need to know about "Do not track". *W3C Blog*, 26 ago. 2013. Disponível em: https://www.w3.org/2011/tracking-protection/drafts/dnt-for-users.html. Acesso em: 30 jun. 2022.

> Trata-se de um mecanismo mais sofisticado por não ser um simples *opt in* ou *opt out*, ou seja, o usuário ainda poderia ter a personalização de certas aplicações baseadas em seus dados pessoais, mas delimitar mais facilmente o escopo em que a captação deles ocorreria.[37]

Veja-se que as tecnologias acima propostas não são pretenciosas ou irrazoáveis e atuam com enfoque na facilitação do processo decisório pelo titular de dados pessoais, ou seja, reduzindo o esforço e aprimorando a árvore de decisões do titular do consentimento. Lamentavelmente, conforme Bruno Bioni esclarece, uma vez que não existe uma regulamentação que torne tais tecnologias compulsórias pelos navegadores de internet, sua adoção prática ou generalizada não tem ocorrido:[38]

> Tal como na experiência do DNT, a P3P esbarrou no mesmo problema de não ser executável. A ausência de uma ação regulatória que a tornasse cogente para os navegadores e as aplicações de Internet foi determinante para o seu insucesso. Assim, mais uma vez, o consumidor restou vulnerado nesse impasse regulatório, relegando-se uma promissora ferramenta que poderia executar eficientemente a sua autodeterminação informacional.

Dessa maneira, verifica-se que o próximo passo para gerar a confiança e a responsabilidade tratadas anteriormente no sentido de aprimorar a regulação da privacidade e proteção de dados, necessariamente, envolve não apenas a efetiva aplicação do quadro normativo instalado, mas empoderar os titulares de dados inclusive mediante aplicações de tecnologias como as PETs sugeridas acima.

Noutras palavras, não se mostra necessário afastar ou vulnerar o consentimento do tratamento de dados pelo titular, mas de facilitá-lo para que não se torne uma letra morta nas normas acerca do tema, mas um efetivo mecanismo de controle da economia da informação.

Outra interessante ideia para operacionalizar o direito fundamental à proteção de dados pessoais é fornecer para os controladores de dados uma forma clara e exata de conhecer seus deveres regulatórios, especialmente em casos complexos, bem como fornecer aos titulares de dados mecanismos claros para exercer seus direitos. O GDPR europeu estabeleceu essa técnica como uma *one-stop-shop* (OSS) ou "balcão único" regulatório.

O objetivo[39] é uniformizar como diferentes autoridades nacionais de proteção de dados de cada país-membro da União Europeia regulam as matérias, bem como

---

[37] W3C. *Plataform for Privacy Preferences (P3P) Project*. Disponível em: https://www.w3.org/P3P/. Acesso em: 30 jun. 2022.

[38] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 237.

[39] UNIÃO EUROPEIA. GDPR. *Considerando nº 127*. Disponível em: https://gdpr-text.com/pt/read/recital-127/. Acesso em: 30 jun. 2022.

apontar uma autoridade única para a qual o titular de dados poderá direcionar sua reclamação, a exemplo de uma situação em que um titular tem seu dado coletado na Itália, porém a sede do controlador fica na Suécia (no OSS europeu, a reclamação poderia ser aberta na Itália e haveria cooperação entre as autoridades de proteção dos dois países para processar e responder a uma reclamação de um titular).[40] O modelo poderia ser adaptado ao caso brasileiro.

Portanto, consistência por intermédio de padronização e uniformização é fundamental para operacionalizar a tutela do direito fundamental à proteção de dados pessoais.

5 Conclusões

O presente estudo teve como objetivo central analisar como o modelo da *tragédia dos comuns* pode auxiliar na crítica da regulação do tema e identificar melhorias e forma de operacionalizá-las.

Constatou-se que há farta e interessante literatura acerca dos aspectos econômicos da privacidade e proteção de dados pessoais, inicialmente como "bens econômicos" clássicos como elemento fundamental da confiança que movimenta a economia da informação.

A literatura aparenta ser unânime em criticar a concentração de responsabilidade depositada sobre os titulares de dados e a centralidade do consentimento para os diferentes modelos regulatórios. A crítica se justifica no sentido de que os indivíduos são sujeitos a vieses e heurísticas diversas que favorecem que a decisão tomada seja sempre pelo consentimento no tratamento de dados, em prejuízo de uma postura de autonomia ante o tratamento de dados pessoais.

Por outro lado, a depender da premissa econômica que se aceite, diferentes propostas de melhoria regulatórias são possíveis, desde medidas enfocadas em grupos de indivíduos de maneira a evitar mais regulamentação estatal, até medidas enfocadas em incluir as corporações no processo regulatório, seja mediante autorregulação, intervenção estatal ou combinações de ambas.

O fato é que a missão regulatória, a despeito dos avanços de décadas, segue incompleta – especialmente considerando os contínuos avanços tecnológicos e o processamento cada vez mais sofisticado de dados pessoais. Mostra-se necessária a responsabilização dos controladores de acordo com os normativos vigentes e o fomento da confiança dos titulares de dados.

[40] UNIÃO EUROPEIA. Comissão Europeia de Proteção de Dados Pessoais. *One-Stop-Shop Leaflet*. 2020. Disponível em: https://edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf. Acesso em: 29 jun. 2022.

Pôde-se constatar que existem propostas de soluções tecnológicas e institucionais para fomentar essa confiança, na figura das chamadas PETs, tecnologias de aprimoramento de privacidade – que se concentram em simplificar o processo decisório na manifestação do consentimento, automatizando-o, porém a difusão dessas tecnologias esbarra na ausência de adesão, por exemplo, dos navegadores de internet, por ausência de uma regulação vinculante acerca do tema. Da mesma maneira, a técnica do OSS adotada pela União Europeia mostrou um esforço de consistência para orientar controladores de dados pessoais e facilitar o exercício de direitos por titulares de dados.

A análise econômica da privacidade e da proteção de dados pessoais revelou-se na pesquisa como uma perspectiva valiosa para se identificar as lacunas e fraquezas do sistema regulatório, bem como um ponto de partida para contribuições. No caso brasileiro em particular, as PETs facilitariam o exercício do consentimento informado pelos titulares pessoais em um país que ainda está conhecendo a proteção à privacidade de dados como um novo direito fundamental.

A finalidade do modelo regulatório, entre outras, é evitar uma tragédia dos (anti)comuns em relação à privacidade, ou seja, o esvaziamento da confiança das pessoas na economia da informação, seja em decorrência de vazamentos de dados, seja pela percepção de que o consentimento exigido pela legislação não se reverte em um efetivo empoderamento dos indivíduos. Ao contrário do apontado por parte da literatura, a pesquisa constatou que uma crise de desconfiança envolvendo a privacidade não é um cenário tão improvável assim.

Referências

BANCO INTERAMERICANO DE DESENVOLVIMENTO; ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Cibersegurança*: riscos, avanços e o caminho a seguir na América Latina e no Caribe. Relatório de Cibersegurança. 2020. Disponível em: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. ed. 1. fev. 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais#:~:text=0%20Brasil%20n%C3%A3o%20%C3%A9%20signat%C3%A1rio,de%20prote%C3%A7%C3%A3o%20de%20dados%20pessoais. Acesso em: 10 jun. 2022.

BRASIL. *Código de Defesa do Consumidor*. Lei nº 8.078 de 11 de setembro de 1990. Ementa: Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 1º jun. 2022.

BRASIL. *Constituição da República Federativa do Brasil de 5 de outubro de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 jun. 2022.

BRASIL. *Lei de Acesso à Informação*. Lei nº 12.527 de 18 de novembro de 2011. Ementa: Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 1º jun. 2022.

BRASIL. *Lei Geral de Proteção de Dados*. Lei nº 13.709 de 14 de agosto de 2018. Ementa: Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1º jun. 2022.

BRASIL. *Marco Civil da Internet*. Lei nº 12.965 de 23 de abril de 2014. Ementa: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1º jun. 2022.

CASIMIRO, Lígia Maria Silva Melo de; CARVALHO, Harley. Para cidades justas, em rede e inteligentes: uma agenda pública pelo direito à cidade sustentável. *International Journal of Digital Law*, Belo Horizonte, ano 2, n. 1, p. 199-215, jan./abr. 2021. DOI: 10.47975/IJDL/1casimiro.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2005.

CERVANTES, Nélida Astezia Castro. *A influência do TRIPS no Programa da SIDA no Brasil*: uma investigação no âmbito da perspectiva neoinstitucional da teoria da escolha racional. Tese (Doutorado em Ciências Sociais) – Universidade de Lisboa, Lisboa, 2021. Disponível em: https://www.repository.utl.pt/handle/10400.5/21855. Acesso em: mar. 2023.

COSTA, Frederico Lustosa da. Bases teóricas e conceituais da reforma dos anos 1990: crítica do paradigma gerencialista. *Revista Brasileira de Administração Política*, 2.2.

DATA PROTECTION LAW OF THE WORLD. *Legislação*. Disponível em: https://www.dlapiperdataprotection.com/index.html. Acesso em: 2 jun. 2022.

DONEDA, Danilo César Maganhoto. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2020.

FAIRFIELD, Joshua A. T.; ENGEL, Christoph. Privacy as a public good. *Duke LJ*, v. 65, p. 385, 2015.

FEREJOHN, John; PASQUINO, Pasquale. The countermajoritarian opportunity. Universidade da Pensilvânia. *Pan Carey Law*, v. 13, p. 353, 2010.

GERBER, Nina; GERBER, Paul; VOLKAMER, Melanie. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, v. 77, p. 226-261, 2018.

HALDER, Steve. Is it a HIPAA Violation to Ask for Proof of Vaccine Status? *HIPAA Journal*, Dec. 25, 2021. Disponível em: https://www.hipaajournal.com/is-it-a-hipaa-violation-to-ask-for-proof-of-vaccine-status/. Acesso em: 28 jun. 2022.

HARDIN, Garrett. The tragedy of the commons: the population problem has no technical solution; it requires a fundamental extension in morality. *Science*, v. 162, n. 3859, p. 1243-1248, 1968.

HELLER, Michael. The tragedy of the anti-commons: property in the transition from Marx to Markets. *Harvard Law Review*, n. 111, jun. 1997.

HIRSCH, Dennis D. Privacy, public goods, and the tragedy of the trust commons: a response to professors Fairfield and Engel. *Duke LJ Online*, v. 65, 2015.

MATIAS, João Luis Nogueira; ROCHA, Rocha. *Repensando o direito de propriedade*. [s.l.]: [s.n.], 2006.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection. *In*: ROTENBERG, Marc; AGRE, Philip E. *Technology and privacy*: The new landscape. [s.l.]: [s.n.], 1998.

MAYER-SCHÖNBERGER, Viktor. Paradigm shift. *Computer Law and Security Review*, v. 40, 2020.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução de Danilo Doneda e Lucial Cabral Doneada. Rio de Janeiro: Renovar, 2008.

SENADO FEDERAL DO BRASIL. *Proposta de Emenda à Constituição nº 17/2019*. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline. Acesso em: 13 jun. 2022.

SINGER, David. Everything you need to know about "Do not track". *W3C Blog*, 26 ago. 2013. Disponível em: https://www.w3.org/2011/tracking-protection/drafts/dnt-for-users.html. Acesso em: 30 jun. 2022.

W3C. *Plataform for Privacy Preferences (P3P) Project*. Disponível em: https://www.w3.org/P3P/. Acesso em: 30 jun. 2022.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

MELO, Lígia Maria Silva; CERVANTES, Nélida Astezia de Castro; LESSA, William Magalhães. A regulamentação da proteção de dados pessoais e seus desafios no contexto da tragédia dos (anti)comuns – Evitando a tragédia da desconfiança. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 11-29, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.melo.

Informações adicionais

Additional information

Editores responsáveis	
Editor-Chefe	Emerson Gabardo
Editor-Adjunto	Lucas Bossoni Saikali

INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 05 · n. 02 · maio/agosto 2024 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.5.n.2

05

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

International Journal of Digital Law – IJDL
ISSN 2675-7087
DOI: 10.47975/digital.law.vol.5.n.2.gaso

Derechos de las personas mayores frente a la Administración Pública digital

Rights of the elderly in front of the digital public administration

Josep Ramon Fuentes Gasó*
I Universidad Rovira i Virgili (Tarragona, España)
josepramon.fuentes@urv.cat
https://orcid.org/0000-0001-5669-6009

Jessica Vivas Roso**
II Universidad Central de Venezuela (Caracas, Venezuela)
vivasrosoj@gmail.com
https://orcid.org/0000-0002-5530-3434

Recebido/Received: 24.09.2024 / September 24th, 2024
Aprovado/Approved: 24.10.2024 / October 24th, 2024

Como citar esse artigo/*How to cite this article*: FUENTES GASÓ, Josep Ramon; VIVAS ROSO, Jessica. Derechos de las personas mayores frente a la Administración Pública digital. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 33-58, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.gaso.

* Profesor Titular de Derecho Administrativo en la Universitat Rovira i Virgili (Tarragona, España). Doctor en derecho (1999) y Licenciado en derecho (1991) por la Universidad Autónoma de Barcelona (Barcelona, España). Miembro del Grupo de Investigación sobre Territorio, ciudadanía y sostenibilidad de la Universidad Rovira i Virgili en el Centro de Estudios en Derecho Ambiental de Tarragona (CEDAT). Participante en diferentes proyectos de investigación del Estado y de la Generalidad de Cataluña, en materia local y ambiental. Ha realizado estancias de investigación en diversos centros, como: Scuola per il perfezionamento del Dirritto Ammnistrativo de la Università degli Studi di Bologna, Italia (1991-1993); Forchungsinstitut für Öffentliche Verwaltung en Speyer, Alemania (1995, 2008); Università degli Studi di Lecce, Italia (2001, 2002, 2005 y 2006); y Université de Paris II. PHANTEON-ASSAS, París, Francia (2004). E-mail: josepramon.fuentes@urv.cat.

** Profesora de la Especialización en Derecho Administrativo y de la Especialización en Derecho Constitucional de la Universidad Central de Venezuela (Caracas, Venezuela). Doctora en Derecho por la Universidad de Coruña (Galicia, España), Master en Derecho de la Administración Pública por la Universidad Rovira i Virgili (Tarragona, España), Especialista en Gerencia del Sector Público por la Universidad Católica Andrés Bello (Caracas, Venezuela). Especialista en Derecho Administrativo por la Universidad Central de Venezuela (Caracas, Venezuela). Miembro de la Asociación Venezolana de Derecho Administrativo y miembro del Centro de Estudios sobre Control Fiscal (CECOFI). E-mail: vivasrosoj@gmail.com.

Resumen: En este trabajo se analiza la incidencia que las tecnologías de la información y la comunicación tienen en las personas mayores de 65 años y cómo éstas pueden convertirse en una amenaza para el disfrute efectivo de sus derechos fundamentales. Asimismo, estudia el impacto que la transformación digital de las administraciones públicas tiene en las personas mayores y cuáles son las acciones que deberán emprenderse para minimizar la brecha digital y aumentar el acercamiento entre las tecnologías de la información y la comunicación y las personas mayores de 65 años.

Palabras claves: derechos fundamentales; envejecimiento activo; administración pública digital; personas mayores; discriminación; exclusión social.

Abstract: This paper analyzes the impact that information and communication technologies have on people over 65 years of age and how they can become a threat to the effective enjoyment of their fundamental rights. It also studies the impact that the digital transformation of public administrations has on the elderly and what actions should be taken to minimize the digital divide and increase the rapprochement between information and communication technologies and people over 65 years of age.

Keywords: fundamental rights; active aging; digital public administration; senior citizens; discrimination; social exclusion.

1 Introducción

Las sociedades actuales y futuras se caracterizan por dos elementos: el envejecimiento de la población y el uso —cada vez mayor— de las tecnologías de la información y la comunicación. Cada uno de ellos trae consigo retos y complejidades propias que deben ser atendidas por las distintas instituciones del Estado con miras a minimizar los riesgos de pobreza, desigualdad, brechas y exclusión y garantizar el disfrute efectivo de los derechos fundamentales.[1]

Ambas circunstancias cobran especial interés en el Estado español, ya que su población es la segunda que más envejece a escala mundial[2] y las estimaciones para los próximos años demuestran que en el 2033 las personas de 65 años y más supondrán el 25,2% del total de la población española,[3] y que dicha cifra aumentará al 40% en el 2050, convirtiéndose así en el país con la población más envejecida

1 *Vid. In totum.* FUENTES i GASÓ; Josep Ramon; VIVAS ROSO, Jessica. Transformación digital de las administraciones públicas, brecha digital y envejecimiento activo. En: GIFREU i FONT, Judith (coord.). *El envejecimiento activo como nuevo reto para los gobiernos locales*: La construcción jurídica de servicios públicos y espacios amigables para las personas mayores. Barcelona: Aranzadi, 2024. p. 475-495.

2 GONZÁLEZ GARCÍA, Erika; MARTÍNEZ HEREDIA, Nazaret. Personas mayores y TIC: oportunidades para estar conectados. *RES: Revista de Educación Social*, Barcelona, núm. 24, p. 1128. 2017.

3 HAZ GÓMEZ, Francisco Eduardo; MANZANERA ROMÁN, Salvador. Administración electrónica y personas mayores: retos metodológicos para el estudio de la exclusión digital entre la población mayor de edad. En: IZAOLA ARGÜESO, Amaia (coord.), *Actas del VIII Congreso de la Red Española de Política Social*: Cuidar la vida, garantizar la inclusión, convivir en diversidad: consensos y retos. Bilbao: Servicio Editorial de la Universidad del País Vasco, 2022. p. 1855-1868.

del mundo.[4] Adicionalmente, las tecnologías de la información y la comunicación (TIC's) han transformado múltiples ámbitos de la vida de las personas. Con el uso generalizado de internet, el aumento de las redes sociales y el reciente auge de la inteligencia artificial han surgido nuevas herramientas digitales para que el ser humano se organice, se comunice, se educe, enseñe y aprenda, cambiando a su vez la sociedad en la que se desenvuelve y las ciudades en las que habitan, transitan y crecen personal y profesionalmente.

Ello cobra especial relevancia en España, país que adelanta un proceso de transformación digital de las administraciones públicas que, por una parte, ha limitado el contacto personal entre los ciudadanos y sus instituciones y, por otra, ha aumentado, cada vez más, el número de trámites y servicios que se solicitan mediante herramientas telemáticas cuando su población mayor de 65 años es migrante digital, es decir, han vivido sin las tecnologías de la información y la comunicación, y ahora se ven en la necesidad de adaptarse a ellas, ya que el diálogo con sus hijos y sus nietos, las fotos, la música, las noticias y muchos trámites de su vida cotidiana —incluyendo los que se realizan ante las distintas administraciones públicas— se están canalizando a través de formatos digitales.[5]

Esta necesidad de adaptarse a las tecnologías de la comunicación y la información se aceleró a partir del año 2020 con la pandemia de Covid-19, cuando el distanciamiento social se convirtió en uno de los mecanismos más seguros para estar "a salvo".[6] Ello contribuyó a que se ejerciera una mayor presión en el uso y aprovechamiento de las tecnologías de la información y la comunicación,[7] evidenciando, entre otras cosas, que tener un buen teléfono móvil no significa que sepamos usarlo y aprovechar todas las oportunidades que nos ofrece.[8]

Ello ha traído como consecuencia que el proceso de adaptación y acercamiento de las personas mayores de 65 años a las nuevas tecnologías de la información y la comunicación sea lento y tenga dificultades en su implementación, ya que —como indicábamos previamente— la población mayor que actualmente habita en España no creció con las tecnologías de la información y, en muchos casos, desconocen

4 VIÑARÁS-ABAD, Mónica; PRETEL-JIMÉNEZ, Marilé; QUESADA-GONZÁLEZ, Carlos. E-commerce, social media and social inclusion A typology of users over 60 years of age in Spain. *Comunicación y Sociedad*, Navarra, vol. 35, núm. 3, pp. 141-142. 2022.

5 ETCHEMENDY, Ernestina; CASTILLA, Diana; BAÑOS RIVERA, Rosa María; BOTELLA ARBONA, Cristina. Sistema Mayordomo: la puerta de entrada de nuestros mayores a las nuevas tecnologías. *Ariadna: Cultura, Educación y Tecnología,* Castellón, vol. 1, núm. 1, p. 34. 2013.

6 SÁNCHEZ VALLE, María; LLORENTE BARROSO, Carmen. Desafíos de la administración electrónica para la inclusión de las personas mayores en la sociedad digital. *Revista Española de la Transparencia*, Madrid, núm. 16, p. 222. 2023.

7 CASTILLO RIQUELME, Víctor; CIFUENTES AGUAYO, Edgar; ÓRDENES ÓRDENES, Danitza; GATICA PARRA, Josefa. Depresión y aislamiento social en personas mayores, análisis del rol de la participación tecnológica. *Revista de Investigación en Psicología*, Lima, vol. 26, núm. 1, p. 79. 2023.

8 DINANT, Inès; SOLA, Ángel. TIC por el envejecimiento activo en Asturias: formación tecnológica para mejorar la calidad de vida de las personas mayores. + *Calidad,* Oviedo, núm. 26, p. 10. 2022.

su funcionamiento,[9] lo que ha generado situaciones de: amenaza a su integración social; aislamiento — lo que deriva en angustias, depresiones, deterioros cognitivos y de salud— ;[10] poco o ningún acceso a recursos disponibles de utilidad lúdica, deportiva o de salud, como por ejemplo vídeos de actividad física y juegos para el fortalecimiento de la memoria;[11] así como limitaciones en el acceso a cada vez más servicios públicos, con la consecuente merma en el disfrute de los derechos sociales de este grupo de personas.[12]

Por ello, este trabajo analiza la incidencia que las tecnologías de la información y la comunicación tienen en las personas mayores de 65 años y cómo éstas pueden convertirse en una amenaza para el disfrute efectivo de sus derechos fundamentales. Asimismo, estudia el impacto que la transformación digital de las administraciones públicas tiene en las personas mayores y cuáles son las acciones que deberán emprenderse para minimizar la brecha digital y aumentar el acercamiento entre las tecnologías de la información y la comunicación y las personas mayores de 65 años.

2 Las tecnologías de la información y la comunicación y su incidencia en las personas mayores

La aparición de las tecnologías de la información y la comunicación ha traído como consecuencia una mejora sustancial de la calidad de vida de las personas y ha dado paso al surgimiento de nuevas realidades como la telemedicina, el teletrabajo, las plataformas digitales, las videoconferencias o el comercio electrónico. Asimismo, ha eliminado muchas de las barreras de la comunicación y ha simplificado en buena medida nuestras actividades cotidianas.

Según explican Agudo Prado et al., el acceso a los ordenadores y a internet contribuye al desarrollo de nuevos lazos sociales y abre nuevas ventanas de conexión con el resto del mundo, dándole a las personas acceso permanente a la cultura y a la educación e implicándolas en actividades de cooperación social.[13] Por otra parte, evita el distanciamiento generacional entre los distintos grupos poblacionales,

9 GONZÁLEZ OÑATE, Cristina, y FANJUL PEYRÓ, Carlos. Aplicaciones móviles para personas mayores: un estudio sobre su estrategia actual. *Aula Abierta,* Oviedo, vol. 47, núm. 1, p. 108. 2018.

10 BUNBURY BUSTILLO, Eva; PÉREZ CALLE, Ricardo Diego; OSUNA ACEDO, Sara. Las competencias digitales en personas mayores: de amenaza a oportunidad. *Vivat Academia*, Madrid, núm. 155, p. 190. 2022.

11 BUNBURY BUSTILLO, Eva; PÉREZ CALLE, Ricardo Diego; OSUNA ACEDO, Sara. Las competencias digitales en personas mayores: de amenaza a oportunidad, *op. cit.*, p. 190.

12 HAZ GÓMEZ, Francisco Eduardo; MANZANERA ROMÁN, Salvador. Administración electrónica y personas mayores: retos metodológicos para el estudio de la exclusión digital entre la población mayor de edad, *op. cit.*, p. 1855.

13 AGUDO PRADO, Susana; PASCUAL SEVILLANO, María Ángeles; FOMBONA CADAVIECO, Javier. Usos de las herramientas digitales entre las personas mayores. *Comunicar: Revista Científica de Comunicación y Educación*, Sollihul, núm. 39, p. 195. 2012.

pero, muy especialmente, contribuye a que las personas mayores no se sientan desplazadas en el mundo actual.[14]

Concretamente, respecto de las personas mayores, tal como afirman Casado Muñoz et al., su participación activa en entornos tecnológicos contribuye a la mejora de su salud y su calidad de vida, y esto es debido a que: 1) se favorece la autonomía y la creatividad; 2) se crean nuevas redes de interacción con otras personas y con ello se evita el aislamiento y la soledad no deseados; 3) se posibilita el acceso a servicios de salud, culturales y educativos, entre otros, de forma remota; 4) se disminuyen los problemas relacionados con la salud mental, ya que las personas mayores que se involucran en entornos tecnológicos demuestran más integración y participación social; y 5) la actividad social a través del uso de tecnologías de la información y la comunicación no es incompatible con la actividad social presencial.[15]

La incorporación de las personas mayores en el uso de las tecnologías de la información y la comunicación contribuye al envejecimiento activo, término que ha sido definido por la Organización Mundial de la Salud[16] como aquel proceso que busca optimizar las oportunidades de salud, participación y seguridad de las personas mayores con la finalidad de mejorar su calidad de vida a medida que envejecen. Es un proceso que abarca —además de los aspectos mencionados— la participación de este grupo poblacional en la sociedad y su integración social, entendiendo que el envejecimiento es parte del proceso de desarrollo de toda persona en el que se cuenta con los mismos derechos a la cultura, al ocio, a la integración social, a la salud, a la participación ciudadana, entre otros.

Las tecnologías de la información y la comunicación facilitan, en cualquier persona, su desarrollo personal y social, pero en las personas mayores optimizan su calidad de vida en el ámbito técnico, económico, político y cultural.[17] Adicionalmente, contribuyen a crear un entorno rico en estímulos que aumenta las posibilidades de contar con un estado de salud sano física, emocional y psicosocialmente.[18]

---

14 AGUDO PRADO, Susana; PASCUAL SEVILLANO, María Ángeles; FOMBONA CADAVIECO, Javier. Usos de las herramientas digitales entre las personas mayores, *op. cit.*, p. 195.

15 CASADO MUÑOZ, Raquel; LEZCANO BARBERO, Fernando; RODRÍGUEZ CONDE, María José. Envejecimiento activo y acceso a las tecnologías: Un estudio empírico evolutivo. *Comunicar*: *Revista Científica de Comunicación y Educación*, Sollihul, núm. 45, p. 38. 2015.

16 ORGANIZACIÓN MUNDIAL DE LA SALUD. Envejecimiento activo: un marco político. *Revista Española de Geriatría y Gerontología*, Barcelona, vol. 37, núm. 2, p. 79. 2002.

17 CRUZ-DÍAZ, Rocío; ORDÓÑEZ-SIERRA, Rosario; ROMÁN GARCÍA, Sara; PAVÓN RABASCO, Francisco. Buenas prácticas que desarrollan la competencia mediática en entornos socioeducativos. En: FUENTE COBO, Carmen; GARCÍA GALERA, María del Carmen; CAMILLI TRUJILLO, Celia Rosa (coords.), *La educación mediática en España*: artículos seleccionados. Madrid, Universitas, 2018. p. 330.

18 CRUZ-DÍAZ, Rocío; REBOLLEDO GÁMEZ, Teresa. Herramientas tecnológicas y colaboración con terapias alternativas: el profesional de la educación social ante el envejecimiento y la discapacidad intelectual. En: ROIG VILA, Rosabel (coord.), *Tecnología, innovación e investigación en los procesos de enseñanza-aprendizaje*. Barcelona, Ediciones Octaedro, 2016. p. 307.

Ahora bien, ese acercamiento entre las personas mayores y las herramientas digitales no se logra "por arte de magia" o "de la noche a la mañana". Crear un entorno digital que resulte estimulante para las personas mayores de 65 años y que les permita incorporarse activamente en el mismo pasa por realizar un adecuado análisis de la información que se les facilita y diseñar políticas dirigidas a lograr un entorno adaptado a sus necesidades.[19]

El uso de las tecnologías de la información y la comunicación pone a prueba la posibilidad de adaptación de las personas mayores, que generalmente se perciben como ajenas al entorno digital. De hecho, como afirman Castillo Riquelme et al., las personas mayores representan uno de los grupos poblacionales con menor integración a la esfera digital, aun cuando las políticas públicas elaboradas por los Estados han promovido el uso de ordenadores y otros dispositivos móviles.[20] Por ello, debe procurarse que cuenten con un entorno rico en estímulos, en el que se incorporen las nuevas tecnologías como un elemento que contribuye a la mejora de la calidad de vida de este grupo poblacional.[21]

Además, es necesario desarrollar estrategias de acción y políticas públicas que permitan comprender que el envejecimiento es una etapa más de la vida de las personas, en la que continúa el proceso de aprendizaje, de crecimiento y enriquecimiento personal,[22] donde se debe eliminar las barreras en el acceso a las tecnologías de la información y la comunicación, simplificando su uso y haciéndolo universal,[23] con miras a lograr una mayor interacción social y mejorar la calidad de vida de este grupo de personas..

3 Brecha digital como riesgo para el envejecimiento activo

Según explican Sunkel y Ullmann, el concepto de brecha digital se utilizó por primera vez en los años noventa para hacer referencia a la distancia que se estaba creando entre los países, los grupos sociales y las personas que tenían acceso a las tecnologías digitales y los que no lo tenían.[24] Se trataba de una nueva desigualdad social que estaba íntimamente relacionada con problemas estructurales de la

19 AGUDO PRADO, Susana; PASCUAL SEVILLANO, María Ángeles; FOMBONA CADAVIECO, Javier. Usos de las herramientas digitales entre las personas mayores, *op. cit.*, p. 194.

20 CASTILLO RIQUELME, Víctor; CIFUENTES AGUAYO, Edgar; ÓRDENES ÓRDENES, Danitza; GATICA PARRA, Josefa. Depresión y aislamiento social en personas mayores, análisis del rol de la participación tecnológica, *op. cit.*, p. 80.

21 SÁNCHEZ FUENTES, David; EIZMENDI LORIZ; Gorka; AZCOITIA ARRECHE, José Miguel. Envejecimiento y nuevas tecnologías. *Revista Española de Geriatría y Gerontología*, Barcelona, vol. 41, núm. 2, p. 57. 2006.

22 AGUDO PRADO, Susana; PASCUAL SEVILLANO, María Ángeles; FOMBONA CADAVIECO, Javier. Usos de las herramientas digitales entre las personas mayores, *op. cit.*, p. 194.

23 SÁNCHEZ FUENTES, David; EIZMENDI LORIZ; Gorka; AZCOITIA ARRECHE, José Miguel. Envejecimiento y nuevas tecnologías, *op. cit.*, p. 58.

24 SUNKEL, Guillermo; ULLMANN, Heidi. Las personas mayores de América Latina en la era digital: superación de la brecha digital. *Revista de la CEPAL*, Vitacura, núm. 127, p. 247. 2019.

sociedad mundial, tales como la pobreza, la exclusión, el desempleo, la precarización del trabajo o la inequidad en la distribución de la riqueza, entre otros.[25]

Para Fernández Campomanes y Fueyo Gutiérrez, el concepto de brecha digital ha existido de forma paralela al de sociedad de la información y lo definen como "las diferencias entre quienes están conectados y conectadas y quienes no lo están";[26] una diferencia que crea fracturas entre los distintos grupos sociales y/o etarios y que debe considerar los distintos niveles de alfabetización y capacidad tecnológica de las personas.[27]

Ahora bien, existen distintas maneras de analizar y estudiar la brecha digital. Así, por ejemplo, González García y Martínez Heredia hacen referencia a dos tipos de brecha digital, la primaria y la secundaria, entendiendo que la brecha digital primaria se relaciona con la desigualdad en el acceso a las tecnologías de la información y la comunicación entre ricos y pobres y que la secundaria se refiere a la desigualdad de competencias y habilidades al acceso de las nuevas tecnologías[28]. Mientras que Arias Fernández et al.,[29] Villarejo Ramos et al.,[30] Fernández Campomanes y Fueyo Gutiérrez[31] y Gómez Navarro et al.,[32] entre otros, analizan la brecha digital desde tres niveles: el primero sería el acceso; el segundo, el uso; y el tercero, la apropiación o calidad en el uso.

La brecha digital en el acceso se centra en los obstáculos para acceder a la red, que puede comprender dificultades económicas o de formación y conocimientos.[33] De acuerdo con Gómez Navarro et al., son varios elementos los que se pueden analizar desde el punto de vista del acceso. Entre ellos se encuentran: en primer

---

25 GÓMEZ NAVARRO, Dulce Angélica; ALVARADO LÓPEZ, Raúl Arturo; MARTÍNEZ DOMÍNGUEZ, Marlen; DÍAZ DE LEÓN CASTAÑEDA, Christian. La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México. *Entreciencias: Diálogos en la Sociedad del Conocimiento*, Ciudad de México, vol. 6, núm. 16, p. 48. 2018.

26 FERNÁNDEZ CAMPOMANES, María; FUEYO GUTIÉRREZ, Aquilina. Redes sociales y mujeres mayores: estudio sobre la influencia de las redes sociales en la calidad de vida. *Revista Mediterránea de Comunicación*, Alicante, vol. 5, núm. 1, p. 159. 2014.

27 SEVILLA CARO, Maricela; SALGADO SOTO, María del Consuelo; OSUNA MILLÁN, Nora del Carmen. Envejecimiento activo. Las TIC en la vida del adulto mayor. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, Guadalajara, vol. 6, núm. 11, p. 577. 2015.

28 GONZÁLEZ GARCÍA, Erika; MARTÍNEZ HEREDIA, Nazaret. Personas mayores y TIC: oportunidades para estar conectados, *op. cit.*, p. 1131.

29 ARIAS FERNÁNDEZ, Enrique; LIRIO CASTRO, Juan; ALONSO GONZÁLEZ, David; HERRANZ AGUAYO, Inmaculada. Acceso y uso de las TIC de las mujeres mayores de la Europa comunitaria. *Prisma Social: Revista de Investigación Social*, Madrid, núm. 21, p. 284. 2018.

30 VILLAREJO RAMOS, Ángel Francisco; RONDÁN CATALUÑA, Francisco Javier; REVILLA-CAMACHO, María Ángeles. Tipología de compradores online mayores de 55 años. *Innovar: Revista de Ciencias Administrativas y Sociales*, Bogotá, vol. 26, núm. 59, p. 62. 2016.

31 FERNÁNDEZ CAMPOMANES, María; FUEYO GUTIÉRREZ, Aquilina. Redes sociales y mujeres mayores: estudio sobre la influencia de las redes sociales en la calidad de vida, *op. cit.*, p. 160.

32 GÓMEZ NAVARRO, Dulce Angélica; ALVARADO LÓPEZ, Raúl Arturo; MARTÍNEZ DOMÍNGUEZ, Marlen; DÍAZ DE LEÓN CASTAÑEDA, Christian. La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México, *op. cit.*, p. 49

33 RAGNEDDA, Massimo. The Third Digital Divide: A Weberian Approach to Digital Inequalities. Nueva York: Routledge, 2017. p. 15.

lugar, el acceso motivacional, es decir, el interés o no de las personas en el uso de las tecnologías de la información y la comunicación. En este tipo de acceso pueden influir factores sociales, culturales, mentales y psicológicos; en segundo lugar, el acceso físico o material relacionado con la disponibilidad de instrumentos y herramientas (hardware, software, aplicaciones y/o servicio de internet, entre otros); y, por último, el acceso a la alfabetización digital, es decir, contar con conocimientos y/o formación para adquirir habilidades digitales.[34]

Respecto a la brecha digital de uso, Fernández Campomanes y Fueyo Gutiérrez[35] explican que se trata de un concepto amplio y complejo que estudia cómo personas que se encuentran en igualdad de condiciones respecto del acceso aprovechan, en mayor o menor medida, las posibilidades que les ofrecen las tecnologías de la información y la comunicación. Es decir, este componente analiza en qué medida —frecuencia de uso— y para qué las personas hacen uso de las herramientas digitales. Generalmente, el análisis de este tipo de brecha digital se realiza mediante la comparación de los usuarios ocasionales con los usuarios habituales de las herramientas tecnológicas.[36]

En cuanto a la apropiación o calidad en el uso, nos referimos al grado de control y elección que posee la persona sobre las herramientas digitales y los contenidos a los que accede.[37] En este nivel, se incluyen los usos avanzados, es decir, cuando la persona accede a herramientas complejas que le proporcionan las tecnologías de la información y la comunicación.[38]

Las personas mayores de 65 años son un colectivo que se encuentra en riesgo de verse afectado por los distintos niveles y manifestaciones de la brecha digital, y dicho riesgo surge principalmente por el hecho que se trata de un grupo poblacional que nació y creció en una época donde no se habían desarrollado o apenas estaban surgiendo las tecnologías de la información y la comunicación —son inmigrantes digitales— , y aun cuando la mencionada brecha digital disminuirá en la medida que los adultos de hoy —nativos digitales— se conviertan en las personas mayores del mañana, la distancia y el desconocimiento de las personas de más de 65 años hoy día respecto de las tecnologías de la información y la comunicación es un hecho real.[39]

---

34 GÓMEZ NAVARRO, Dulce Angélica; ALVARADO LÓPEZ, Raúl Arturo; MARTÍNEZ DOMÍNGUEZ, Marlen; DÍAZ DE LEÓN CASTAÑEDA, Christian. La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México, *op. cit.*, p. 49

35 FERNÁNDEZ CAMPOMANES, María; FUEYO GUTIÉRREZ, Aquilina. Redes sociales y mujeres mayores: estudio sobre la influencia de las redes sociales en la calidad de vida, *op. cit.*, p. 160.

36 RAGNEDDA, Massimo. *The Third Digital Divide*: A Weberian Approach to Digital Inequalities, *op. cit.,* p. 15.

37 GÓMEZ NAVARRO, Dulce Angélica; ALVARADO LÓPEZ, Raúl Arturo; MARTÍNEZ DOMÍNGUEZ, Marlen; DÍAZ DE LEÓN CASTAÑEDA, Christian. La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México, *op. cit.*, p. 49

38 RAGNEDDA, Massimo. *The Third Digital Divide*: A Weberian Approach to Digital Inequalities, *op. cit.,* p. 15.

39 PERAL PERAL, Begoña; VILLAREJO RAMOS, Ángel Francisco; ARENAS GAITÁN, Jorge. Descifrando la brecha digital de los mayores. Panorama Social, Madrid, núm. 25, p. 78. 2017.

Generalmente, la brecha digital de las personas mayores se centra en la falta de competencias digitales, lo que las lleva a mantenerse al margen en el acceso, uso y apropiación de las nuevas tecnologías modernas.[40] Esta exclusión social, que deriva del distanciamiento o desvinculación con las tecnologías de la información y la comunicación, puede generar situaciones complejas de aislamiento, soledad no deseada y/o desintegración social.[41]

Como explica Olarte Encabo, la exclusión social, entendida como el proceso de separación de las personas y grupos sociales respecto de la sociedad y las oportunidades económicas, sociales, políticas, culturales y laborales a las que tienen derecho, se proyecta respecto de las tecnologías de la información y la comunicación cuando el sujeto o grupo de sujetos no tienen acceso a estas.[42] De allí que la exclusión digital se configure como un factor de desinformación y de disminución de oportunidades personales, lo que, en el caso de las personas mayores de 65 años, recobra especial importancia porque si no son capaces de responder a las exigencias sociales que derivan de las nuevas tecnologías puede romperse su vínculo con la sociedad.

Adicionalmente, no debemos olvidar que muchos países europeos han adelantado un proceso de digitalización y/o transformación digital como medio de reestructuración del estado del bienestar, y esta circunstancia, en el caso de las personas mayores de 65 años, ha generado que el acceso a los servicios de bienestar se deteriore. Tal como afirman Alexopoulou y Åström, el contacto entre los servicios de bienestar y los ciudadanos ha pasado de la comunicación interpersonal a la comunicación a través de plataformas en línea y ello ha generado que las personas que no tienen competencias digitales adecuadas no reciban los servicios de bienestar a los que tienen derecho.[43]

Arias Fernández et al., en el año 2017, realizaron un estudio sobre la brecha digital de las personas mayores entre 65 y 74 años en la UE y observaron que el 59%, en algún momento de su vida, ha utilizado un ordenador; que el 52% lo utilizó al menos una vez en el año del estudio, y que el 40% señaló no haber usado nunca un ordenador, lo que evidencia la gran brecha digital que existía en la UE para dicho año.[44]

---

40 HAZ GÓMEZ, Francisco Eduardo; MANZANERA ROMÁN, Salvador. Administración electrónica y personas mayores: retos metodológicos para el estudio de la exclusión digital entre la población mayor de edad, *op. cit.*, p. 1857.

41 OLARTE ENCABO, Sofía. Brecha digital, pobreza y exclusión social. *Temas laborales: Revista Andaluza de Trabajo y Bienestar Social*, Sevilla, núm. 138, p. 292. 2017.

42 OLARTE ENCABO, Sofía. Brecha digital, pobreza y exclusión social, *op. cit.*, p. 296.

43 ALEXOPOULOU, Sofia; ÅSTRÖM, Joachim. (2022). How the Responsibility of Digital Support for Older People is Allocated? The Swedish Welfare System at the Crossroads. Research on Ageing and Social Policy: (RASP), Barcelona, vol. 10, núm. 1, p. 52. 2022.

44 ARIAS FERNÁNDEZ, Enrique; LIRIO CASTRO, Juan; ALONSO GONZÁLEZ, David; HERRANZ AGUAYO, Inmaculada. Acceso y uso de las TIC de las mujeres mayores de la Europa comunitaria, *op. cit.*, p. 291.

Respecto de España, el estudio señala que para el año 2017, el 36% de las personas mayores entre 65 y 74 años había utilizado un ordenador en los últimos tres meses, porcentaje muy por debajo de la media europea, y que el 54% de personas mayores nunca lo había usado. Lo que permite concluir que la población mayor española cuenta con un bajo nivel en competencias digitales con respecto al resto de países europeos.[45]

Por otra parte, González Oñate et al., en el año 2015, compararon la relación de las personas mayores de 65 años de Reino Unido y España con las tecnologías de la información y la comunicación y concluyeron que muchas personas de este grupo poblacional se muestran reacias al uso de las nuevas tecnologías porque introducir su información personal en las páginas web les genera intranquilidad.[46] Sin embargo, este temor desaparece en cuanto descubren cuánto las tecnologías de la información y la comunicación pueden mejorar su calidad de vida.[47]

De allí que la brecha digital no solo constituye un riesgo para el envejecimiento activo, sino que también lo es para el efectivo disfrute de los derechos sociales de las personas mayores al impedir y/o dificultar el acceso a los servicios de bienestar. Por ello, debe trabajarse en la reducción y/o eliminación de la mencionada brecha como mecanismo para reducir la vulnerabilidad y evitar el aislamiento de las personas mayores.[48]

Para ello, es necesario no solamente mejorar el acceso de las personas mayores a las tecnologías de la información y la comunicación, sino, además, dotarlas de los conocimientos, herramientas y habilidades imprescindibles para que puedan comunicarse, opinar y construir conocimiento en la red. La inclusión de los mayores a las tecnologías de la información y la comunicación pasa por confiar en la red y mejorar la experiencia del usuario frente a las mismas.

> Todo ello implicará que los mayores puedan desarrollar sus capacidades y habilidades cognitivas necesarias para enfrentarse a aplicaciones tecnológicas más complejas y útiles, como la banca electrónica, los servicios sociales y de salud, los trámites con las administraciones

45 ARIAS FERNÁNDEZ, Enrique; LIRIO CASTRO, Juan; ALONSO GONZÁLEZ, David; HERRANZ AGUAYO, Inmaculada. Acceso y uso de las TIC de las mujeres mayores de la Europa comunitaria, *op. cit.*, p. 292.

46 GONZÁLEZ OÑATE, Cristina; FANJUL PEYRÓ, Carlos; CABEZUELO-LORENZO, Francisco. Uso, consumo y conocimiento de las nuevas tecnologías en personas mayores en Francia, Reino Unido y España. Comunicar: Revista Científica de Comunicación y Educación, Sollihul, núm. 45, p. 27. 2015.

47 ÁVILA-RODRÍGUEZ DE MIER, Belén; MARTÍN GARCÍA, Noemi. La frecuencia del uso de internet como determinante de la vulnerabilidad entre la población sénior: usuario habitual vs. no usuario habitual. *Revista Mediterránea de Comunicación*, Alicante, vol. 10, núm. 1, p. 16. 2019.

48 BUNBURY BUSTILLO, Eva; PÉREZ CALLE, Ricardo Diego; OSUNA ACEDO, Sara. Las competencias digitales en personas mayores: de amenaza a oportunidad, *op. cit.*, p. 178.

públicas, la consecución de información o la adquisición de productos y servicios, entre otros.[49]

4 Derechos de las personas mayores frente a la Administración Pública digital

Como hemos indicado previamente, las tecnologías de la información y la comunicación se utilizan hoy día en casi todas las facetas del ser humano, y la relación de este con las instituciones públicas no escapa de la influencia de las nuevas tecnologías. Dentro del sector público, estos instrumentos han servido para mejorar la prestación de los servicios, facilitar las relaciones con las personas e incluso entre administraciones públicas, haciendo que, en buena medida, la comunicación sea rápida, transparente, eficiente y participativa.[50]

La transformación digital de las instituciones públicas implica incorporar las tecnologías de la información y la comunicación en las distintas actividades de gestión, planificación y administración con miras a mejorar los servicios y la información ofrecida a las personas y organizaciones y a facilitar la creación de canales que permitan aumentar la transparencia y la participación ciudadana.[51]

De acuerdo con Maldonado Meléndez, una de las razones que ha influido en el uso de los medios electrónicos y la automatización de los procesos es la capacidad que tienen estas tecnologías de permitir una interacción inmediata entre el Estado y las personas.[52] Los cambios que se han producido en los distintos órganos y entes públicos a partir de la implementación de las tecnologías de la información y la comunicación han generado, además, la transformación de viejos paradigmas y han impulsado nuevas formas de relacionamiento entre los distintos sujetos.[53]

Así, hemos vivido un proceso de transformación digital, que no es otra cosa que la integración de las tecnologías en las distintas áreas, procedimientos y niveles de las administraciones públicas "cambiando la forma en la que operan y se relacionan

---

49 PERAL PERAL, Begoña; VILLAREJO RAMOS, Ángel Francisco; ARENAS GAITÁN, Jorge. Descifrando la brecha digital de los mayores, *op. cit.*, p. 78.

50 CERRILLO MARTÍNEZ, Agustí. La regulación de la administración electrónica local: el caso del Ayuntamiento de Barcelona. *Anuario del Gobierno Local*, Barcelona, núm. 1, p. 178. 2006.

51 SÁNCHEZ VALLE, María; LLORENTE BARROSO, Carmen. Desafíos de la administración electrónica para la inclusión de las personas mayores en la sociedad digital, *op. cit.*, p. 220.

52 MALDONADO MELÉNDEZ, Mirko. Del gobierno electrónico a la administración digital: las transformaciones digitales en Iberoamérica. *Anuario de la Red Eurolatinoamericana de Buen Gobierno y Buena Administración*, Buenos Aires, núm. 3, p. 3. 2023. Disponible en: <https://ijeditores.com/pop.php?option=articulo&Hash=ea8464e399a5e99ac727fc8f1b77540f>. Consultado el: 15 de agosto de 2024.

53 CASTILLO BLANCO, Federico. El tránsito a una administración digital y robotizada: el necesario cambio del modelo de administración y empleo público. *Revista Iberoamericana de Gobierno Local*, Granada, núm. 19, p. 28. 2021.

con el ciudadano, reelaborando procedimientos, servicios digitales y estrategias amigables para el ciudadano".[54]

Este proceso, tal como afirma Sobrino García requiere, entre otras cosas, un tráfico y tratamiento masivo de datos e información que genera sobre las distintas administraciones públicas un sinfín de retos entre los se encuentran: la reutilización de la información pública; el tratamiento de los datos personales y el respecto de la privacidad de las personas, la inclusión de grupos vulnerables, la participación ciudadana, entre otros.[55]

Es un proceso que ha requerido la creación de un marco normativo que permita su implementación, así como la reformulación de los procedimientos y las organizaciones, garantizando seguridad jurídica y el ejercicio de los derechos y deberes de las personas.[56]

En España, el proceso de transformación digital de las instituciones públicas comenzó con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que incorporó la obligación que las administraciones públicas "impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos" en su actuación diaria (artículo 45).

Seguidamente, encontramos la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que, en palabras de Cotino Hueso, se configuró como un verdadero salto hacia adelante "que miró al horizonte de la Administración, pero también la perspectiva de la ciudadanía"[57] y, de acuerdo con Rando Burgos:

> [J]ustifica su promulgación en la creación de un marco jurídico que facilite la extensión y utilización de estas tecnologías, con el reto principal de la implantación de las Tecnologías de la Información y las Comunicaciones (TIC), para la sociedad en general y para la Administración en particular, de generar la confianza suficiente que elimine o minimice los riesgos asociados a su utilización.[58]

---

54 MALDONADO MELÉNDEZ, Mirko. Del gobierno electrónico a la administración digital: las transformaciones digitales en Iberoamérica, *op. cit.*, p. 4.

55 SOBRINO GARCÍA, Itziar. Las 'smart cities' y la inteligencia artificial. Nuevos retos de las administraciones públicas en la gobernanza inteligente. En: SOBRINO GARCÍA, Itziar (coord.), *Justicia, administración y derecho:* nuevos retos del derecho en el siglo XXI. Pamplona: Thomson Reuters Aranzadi, 2021, p. 160.

56 CERRILLO MARTÍNEZ, Agustí. La regulación de la administración electrónica local: el caso del Ayuntamiento de Barcelona, *op. cit.*, p. 179.

57 COTINO HUESO, Lorenzo. El nuevo reglamento de Administración electrónica, que no innova en tiempos de transformación digital. *Revista Catalana de Dret Públic*, Barcelona, núm. 63, p. 120. 2021.

58 RANDO BURGOS, Esther. Nuevos retos en la Administración del siglo XXI: digitalización, inteligencia artificial y transformación administrativa. Disponible en: <https://laadministracionaldia.inap.es/noticia.asp?id=1514543>. Consultado el: 30 de agosto de 2024.

En efecto, esta Ley permitió dar los primeros pasos en la creación de páginas web institucionales y sedes electrónicas, impulsando, además, los certificados de firma electrónica, el DNI electrónico y el expediente electrónico.[59]

Posteriormente, se aprueban la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que, de acuerdo con Martínez Gutiérrez, insertan en el corazón del ordenamiento jurídico español el modelo de administración electrónica.[60] Estas leyes, entre otras cosas, reconocieron el derecho a comunicarse a través de un Punto de Acceso General Electrónico de la Administración, así como el derecho a ser asistidos en el uso de medios electrónicos. Adicionalmente, reguló los sistemas de identificación y firma electrónica, la representación del interesado y los registros electrónicos de apoderamientos.[61]

Con este marco normativo como referencia, los distintos órganos y entes del sector público iniciaron los procesos de adecuación de sus plataformas y procesos a la era digital. Sin embargo, no se trata de un proceso exento de baches, retrasos e inconvenientes, sobre todo si lo vemos desde la mirada de las personas mayores de 65 años. En efecto, aun cuando los distintos servicios telemáticos que ofrecen las administraciones públicas se han extendido de manera regular entre la población, el uso que las personas mayores de 65 años realizan de la administración electrónica sigue siendo muy limitado.[62]

Por ejemplo, según datos del Instituto Nacional de Estadística (INE) correspondientes al año 2023, solo el 37,5% de las personas entre 65 y 74 años han mantenido algún contacto o interacción con la Administración en los últimos 12 meses. El 27,5% la han utilizado para obtener información oficial de páginas web de la Administración, enviar formularios cumplimentados online como el pago de impuestos y la solicitud de citas médicas (26,5%), así como para descargar formularios oficiales (21,1%).[63]

---

59 BALLESTER ESPINOSA, Adrián. La transformación digital forzosa en la Administración Pública: cómo la tecnología ayudará en un futuro cercano a los gobiernos en la toma de decisiones. *Telos: Cuadernos de Comunicación e Innovación*, Madrid, núm. 117, p. 147. 2021.

60 MARTÍNEZ GUTIÉRREZ, Rubén. Elementos para la configuración de la administración digital. *Revista de Derecho Administrativo,* Lima. núm. 20, p. 214. 2021.

61 HAZ GÓMEZ, Francisco Eduardo; MANZANERA ROMÁN, Salvador. Administración electrónica y personas mayores: retos metodológicos para el estudio de la exclusión digital entre la población mayor de edad, *op. cit.*, p. 1856-1857. Martínez Gutiérrez cuestiona que se haya regulado de forma separada los distintos aspectos que intervienen en el proceso de transformación digital de las administraciones públicas. Para el autor, ambas normas regulan de forma separada aspectos que se encuentran íntimamente relacionados como la sede y el registro electrónico, cuando, con el estado de avance de la administración electrónica que derivaba de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, se hubiese esperado una mejor regulación legal. *Vid.* MARTÍNEZ GUTIÉRREZ, Rubén. Elementos para la configuración de la administración digital, *op. cit.*, p. 214.

62 SÁNCHEZ VALLE, María; LLORENTE BARROSO, Carmen. Desafíos de la administración electrónica para la inclusión de las personas mayores en la sociedad digital, *op. cit.*, p. 218.

63 SANZ, Elena. La brecha digital en los mayores: solo un 37,5% interactúa con la administración electrónica. Disponible en: <https://theconversation.com/la-brecha-digital-en-los-mayores-solo-un-37-5-interactua-con-la-administracion-electronica-222315>. Consultado el: 30 de agosto de 2024.

Por otro lado, un 11,2% de los usuarios entre 65 y 74 años afirmaron que no enviaron algunos de los formularios previamente mencionados a través de Internet, a pesar de tener la necesidad de presentar tales documentos.

Otro estudio realizado por el Observatorio Nacional de Tecnología y Sociedad, en el año 2021, evidenció que un 60% de las personas con más de 64 años utiliza los sistemas de identificación digital para realizar algún tipo de consulta, proceso o gestión administrativa (declaración de la renta, consultar notificaciones o comunicaciones, realizar pagos telemáticos, etc.). Se trata de un porcentaje menor que el de usuarios con edades entre los 24 y los 35 años, donde el porcentaje asciende al 87%.[64]

Y un tercer estudio elaborado por el Real Patronato sobre Discapacidad en el año 2017 daba cuenta de que las personas mayores de 65 años encontraban dificultades para consultar su Cl@ve PIN, dado que solo contaban con un tiempo de seguridad de 10 minutos para acceder al trámite y en muchas ocasiones algunos de los usuarios han tenido que realizar varias veces la operación, al haber superado los 10 minutos previstos para realizar la consulta.[65]

Los datos parecen evidenciar que, a pesar de los avances de las administraciones públicas frente a la era digital, no existe una incorporación efectiva y positiva de las personas entre 65 y 74 años en el uso de las tecnologías de la información y comunicación, lo que les afecta no solo la realización de los trámites *online*, sino el acceso a servicios públicos o a las prestaciones económicas de la seguridad social.

De acuerdo con Sánchez-Valle et al.[66] son diversos los motivos que pueden impedir el acceso de las personas mayores a las tecnologías de la información y la comunicación y a las plataformas electrónicas de las administraciones públicas, entre los que se pueden mencionar: en primer lugar, no disponer de un ordenador o dispositivo que les permita el acceso a internet; en segundo lugar, el diseño de las páginas web de las administraciones públicas es complejo, o con una navegabilidad y usabilidad poco intuitivas; y por último, la falta de confianza en los trámites en línea.[67]

Estas circunstancias han generado que, a la par de una normativa que promueva la transformación digital de las administraciones públicas, también se haya desarrollado un marco jurídico que permita facilitar y mejorar el acceso de las personas mayores a las nuevas tecnologías. Entre ellas podemos mencionar:

---

64 OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD. *Estudio sobre digitalización de la Administración.* Madrid: Ministerio de Asuntos Económicos y Transformación Digital, 2021. p. 6.

65 REAL PATRONATO SOBRE DISCAPACIDAD. *Estudio de accesibilidad de los trámites con la Administración Pública en España*. Madrid: Ministerio de Sanidad, Consumo y Bienestar Social, 2017. p. 47.

66 SÁNCHEZ-VALLE, María; VINARÁS ABAD, Mónica; LLORENTE-BARROSO, Carmen. Empowering the Elderly and Promoting Active Ageing Through the Internet: The Benefit of e-inclusion Programmes. In: WITHIN KOLLAK, Ingrid (ed.), *Safe at Home with Assistive Technology*. Cham: Springer International Publishing, 2017. p. 99.

67 SÁNCHEZ VALLE, María; LLORENTE BARROSO, Carmen. Desafíos de la administración electrónica para la inclusión de las personas mayores en la sociedad digital, *op. cit.*, p. 223.

1. La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, cuya disposición adicional quinta establecía que las administraciones públicas debían adoptar las medidas necesarias para que la información disponible en sus páginas web pueda ser accesible a personas con discapacidad y de edad avanzada, de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos. El plazo de adecuación vencía el 31 de diciembre de 2005.[68]
2. El Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social. En su disposición adicional segunda establece que las personas mayores tendrán prioridad en el acceso a iniciativas, programas y acciones de infoinclusión y de extensión de la sociedad de la información que desarrollen las administraciones públicas.
3. La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, que prevé que los medios electrónicos que utilicen los órganos y entes del sector público deberán ser accesibles para las personas con discapacidad de acuerdo con las normas técnicas existentes en la materia. Además, deberán adoptar las medidas adecuadas para permitir que los documentos destinados a personas con discapacidad estén disponibles en formatos que tengan en cuenta las posibilidades de reutilización por parte de dichas personas (artículo 5.8).
4. La Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, en su disposición adicional undécima prevé que las administraciones públicas promoverán el impulso, el desarrollo y la aplicación de los estándares de accesibilidad para personas con discapacidad y diseño para todos, en todos los elementos y procesos basados en las nuevas tecnologías de la sociedad de la información.
5. El Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, que en su artículo 5 establece que las medidas contenidas en la Ley para garantizar la igualdad de oportunidades, la no discriminación y la accesibilidad universal de las personas se aplicarán en los siguientes ámbitos: a) Telecomunicaciones y sociedad de la información, b) Espacios públicos urbanizados, infraestructuras y

[68] Esta disposición fue derogada por la disposición derogatoria única c) de la Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos.

edificación, c) Transportes, d) Bienes y servicios a disposición del público, e) Relaciones con las Administraciones públicas, f) Administración de justicia, g) Participación en la vida pública y en los procesos electorales, h) Patrimonio cultural, y; i) Empleo.

6. El Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. Su artículo 5 prevé que las entidades incluidas en su ámbito de aplicación[69] deberán contar con sitios web y aplicaciones para dispositivos móviles que sean accesibles para sus personas usuarias, especialmente para las personas mayores y personas con discapacidad, de forma tal que sus contenidos sean perceptibles, operables, comprensibles y robustos. De igual forma dispone que la accesibilidad deberá ser considerada en el proceso de diseño, gestión, mantenimiento y actualización de contenidos de los sitios web y las aplicaciones para dispositivos móviles, debiendo, en la medida de sus posibilidades, aumentar la accesibilidad de los sitios web y las aplicaciones para dispositivos móviles.

Este marco normativo tiene como finalidad permitirles a las administraciones públicas afrontar los retos que derivan de sus procesos de transformación digital para garantizar los derechos de las personas mayores de 65. Respecto de dichos derechos, presentamos algunas consideraciones que deben ser tomadas en todo momento por las administraciones públicas en sus procesos de transformación y digitalización:

4.1 No discriminación

La transformación digital de las administraciones públicas puede generar procesos de exclusión y/o aislamiento respecto de los diferentes bienes y servicios que ofrecen los órganos y entes públicos. Las razones para dicha exclusión pueden derivar de diferentes motivos: falta de confianza; falta de conocimientos o información necesaria sobre el funcionamiento de los trámites, pasos a seguir y requisitos requeridos; carencia de dispositivos electrónicos necesarios para la realización del trámite (computadora o teléfono móvil inteligente); carencia o deficiencias en el servicio de internet; entre otros.

En este punto, es necesario recordar las palabras de Caballero Álvarez, quien afirma que a partir de la pandemia de Covid-19 han surgido “nuevas pobrezas”,

[69] De acuerdo con el artículo 2, el ámbito subjetivo de aplicación comprende: la Administración General del Estado; las administraciones de las comunidades autónomas; las entidades que integran la Administración Local; el sector público institucional, en los términos establecidos en el artículo 2.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones públicas; las asociaciones constituidas por las administraciones, entes, organismos y entidades que integran el sector público; y la Administración de Justicia.

como, por ejemplo, las relacionadas con la brecha digital, y es que "[h]ay familias que no son pobres en el sentido tradicional de la expresión pero que solo tienen un ordenador para todos los miembros de la familia, que tienen que compartir simultáneamente para trabajar y estudiar. Tenemos que añadir un nuevo esfuerzo y nuevas consideraciones".[70]

En un entorno tecnológico ajeno y no natural para las personas mayores de 65 años, éstas son expuestas a situaciones de vulnerabilidad por parte de las administraciones públicas, más aún cuando los portales web y aplicaciones móviles no atienden a estándares de accesibilidad y diseño para todos, lo cual puede limitar las relaciones de este grupo de personas con las administraciones públicas, el sistema de salud, el sistema financiero, los servicios culturales, de entretenimiento, de comunicación con otras personas, entre otros.

Aunado a ello, herramientas tecnológicas poco amigables para las personas mayores los puede llevar a una pérdida de su autonomía e incluso poner en riesgo la seguridad de sus datos personales (por ejemplo, claves de acceso), al tener que acudir a terceras personas (hijos, nietos, amistades) que posean un mayor y mejor conocimiento tecnológico para realizar tareas sencillas como pedir una cita médica, realizar el pago de un servicio o cualquier transacción bancaria. En definitiva, las discrimina y limita su capacidad de obrar.[71]

Para minimizar el impacto que pueda tener la transformación digital de las administraciones públicas, éstas deben implementar acciones para reducir la brecha entre las personas mayores de 65 años y las distintas plataformas tecnológicas del sector público. Entre dichas acciones se pueden mencionar: herramientas tecnológicas amigables, capacitación permanente para las personas mayores, aumentar el plazo para la realización de los trámites, entre otros.[72] La idea es

---

70 CABALLERO ÁLVAREZ, Abel. (2020). "Nuevas pobrezas" a raíz de la pandemia. En DE FRUTOS, Javier; ARIAS LERA, Alejandro; LOSOVIZ, Lucia; BERNAL, Paola (coords.), *El rol de los gobiernos locales en la lucha contra la pobreza infantil en el contexto de la emergencia de la COVID-19*. Madrid: Ministerio de Sanidad, Consumo y Bienestar Social, 2020. p. 13.

71 Un estudio realizado por el grupo de trabajo Brecha Digital y Personas Mayores en el año 2021 evidenció que no es muy frecuente el uso de los servicios en línea que ofrece la Administración en España entre las personas mayores de 60 años. Según el informe, el 59% de los mayores utilizan la administración electrónica para solicitar una cita médica, hacer la declaración de la renta o renovar un documento oficial y consideran que es complicado navegar por las páginas web de la Administración debido a que el lenguaje que utilizan es demasiado complejo, tienen mucho contenido y la terminología es muy técnica y complicada. *Vid.* GRUPO DE INVESTIGACIÓN BRECHA DIGITAL Y PERSONAS MAYORES. *Seniors digitales:* Informe sobre el uso del comercio y la administración electrónica en España. Madrid: CEU Ediciones, 2021. p. 19. En este mismo sentido, Sánchez Valle y Llorente Barroso afirman que el principal freno para utilizar estos servicios es el temor a equivocarse, a tener que facilitar demasiados datos personales y a la dificultad para acordarse de las claves de acceso a las distintas páginas web. *Vid.* SÁNCHEZ VALLE, María; LLORENTE BARROSO, Carmen. Desafíos de la administración electrónica para la inclusión de las personas mayores en la sociedad digital, *op. cit.*, p. 221.

72 FUNDACIÓN COTEC. *Administración electrónica y personas mayores*: Mejoras en el acceso y uso de la Administración electrónica por parte de las personas mayores. Madrid: Universidad de Murcia, 2021. p. 9.

que las tecnologías de la información y la comunicación sean una herramienta de inclusión y no de exclusión y discriminación.[73]

4.2 Acceso a los servicios no digitales

Un segundo elemento que deben considerar las administraciones públicas en sus procesos de transformación digital es garantizar el efectivo acceso a los servicios que ofrecen, y es que, las políticas públicas que se ejecutan a favor de las personas mayores suelen tener como centro de actuación los servicios sociales que se orientan hacia la prevención de riesgos, la atención de necesidades y la promoción del bienestar del individuo.[74]

Las administraciones públicas han fomentado, cada vez en mayor medida, el acceso y uso de estos servicios a través de plataformas en línea, sin tomar en consideración los retos que enfrentan las personas mayores para la utilización de las tecnologías de la información y la comunicación.[75] Ello trae como consecuencia que aquellas personas que se encuentren poco o nada familiarizadas con las tecnologías de la información y la comunicación, no accedan ni a la información ni a los servicios de bienestar a los que tienen derecho, mermando su calidad de vida.

En efecto, tal como afirma Beltrán Castellanos, aquellas personas que no sepan o no puedan utilizar los medios electrónicos que ha dispuesto la Administración, pero que estén obligados a ello, pueden verse limitados e incluso privados de ejercer sus derechos y acceder a los beneficios del Estado del bienestar como, por ejemplo, acceder a una subvención, solicitar asistencia sociosanitaria, psicosocial o de otra naturaleza, todo lo cual pudo haber solicitado a través de algún mecanismo

---

73 De acuerdo con Bunbury Bustillo et al., para ello se debe considerar: 1. Los contenidos, es decir, las personas mayores, deben contar con información que se ajuste a sus necesidades e intereses, así como información suficiente y accesible que aumente sus posibilidades de mantener el contacto con otras personas, participar en eventos, administrar su vida y atender sus necesidades personales. 2. Adecuar a sus aptitudes físicas e intelectuales la información que consumen y los canales de comunicación que utilizan. Por ejemplo, en aquellos casos donde la persona requiera introducir claves y otros datos en sitios web (de instituciones bancarias o de administraciones públicas), dichas páginas deben considerar que la destreza y rapidez de una persona mayor para introducir dicha clave es menor que la de una persona joven o adulta y, por tanto, requerirá que la página web le otorgue un tiempo mayor para completar el proceso (introducir la clave), puesto que, de lo contrario, se estarían generando miedos y temores frente al uso de las tecnologías de la información y la comunicación, y; 3. Superar la brecha digital. *Vid.* BUNBURY BUSTILLO, Eva; PÉREZ CALLE, Ricardo Diego; OSUNA ACEDO, Sara. Las competencias digitales en personas mayores: de amenaza a oportunidad, *op. cit.*, p. 177-178.

74 DOMÍNGUEZ MARTÍN, Mónica. Políticas públicas y configuración de los servicios de protección y atención a las personas mayores. El protagonismo de los municipios. *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, Madrid, núm. 25, p. 253. 2021. EGEA DE HARO, Alfonso. La definición y localización de la política de mayores. En: DÍEZ SASTRE, Silvia; RODRÍGUEZ DE SANTIAGO, José María (dirs.), *Ciudades envejecidas*: El derecho y la política local para la protección y cuidado de las personas mayores. Navarra: Aranzadi, 2021. p. 35.

75 *Vid.* SÁNCHEZ VALLE, María; LLORENTE BARROSO, Carmen. Desafíos de la administración electrónica para la inclusión de las personas mayores en la sociedad digital, *op. cit.*, p. 220.

tradicional (acudir a la sede de la Administración a solicitar la atención o ayuda correspondiente).[76]

Por ello, tal como afirman Viñarás-Abad et al., las administraciones públicas tienen la obligación de hacer accesibles sus servicios digitales debiendo "garantizar a todos los colectivos, y especialmente a los más vulnerables, un uso que responda a las necesidades y expectativas de los mismos".[77]

Para ello se plantean, al menos, dos posibles acciones a seguir: 1. Ofrecer en todo momento alternativas no automatizadas para el acceso de a los servicios de las administraciones públicas; 2. Implementar sistemas de asistencia virtual automatizada con un enfoque inclusivo. Es decir, que contemplen, por lo menos, los siguientes aspectos: a) intuición; b) accesibilidad; c) lenguaje natural; d) datos personales; e) transparencia y f) rol de los seres humanos.[78]

4.3 Protección de datos personales

Un tercer elemento a considerar en el proceso de transformación digital es el relativo al tratamiento de los datos personales. La realización de trámites, solicitudes y/o cualquier otra actividad por plataformas electrónicas trae consigo la recolección de una cantidad importante de información sobre las personas que se puede expresar de distintas formas (numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, entre otros).

Las administraciones públicas deben asegurarles a las personas mayores de 65 años que sus datos personales serán tratados en estricto cumplimiento del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas

---

76 BELTRÁN CASTELLANOS, José Miguel. *La brecha digital en las relaciones de la ciudadanía con las administraciones públicas.* Valencia: Tirant lo Blanch, 2024. p. 106.

77 VIÑARÁS-ABAD, Mónica; ABAD-ALCALÁ, Leopoldo; LLORENTE-BARROSO, Carmen; SÁNCHEZ-VALLE, María; PRETEL-JIMÉNEZ, Marilé. Administración electrónica y e-inclusión de las personas mayores. *Revista Latina de Comunicación Social*, vol. 72, núm. 2, pp. 217. 2017.

78 STRINGHINI, Antonella. Asistencia virtual automatizada e inclusiva para optimizar la relación de la ciudadanía con la Administración Pública, *op. cit* p. 124-125. STRINGHINI explica cada uno de estos elementos de la siguiente forma: 1. Intuición. Los asistentes virtuales deben ser intuitivos, es decir; debe ser utilizada por todas las personas, independientemente, de su grado de alfabetización, edad, y condiciones sociales, económicas y culturales. 2. Accesibilidad. Se debe poder interactuar con los asistentes virtuales a través de textos, voz y/o imágenes. 3. Lenguaje natural. Los asistentes virtuales deben relacionarse utilizando un lenguaje que sea natural a la forma como se expresa una persona; más aún en materia de trámites y procedimientos administrativos, donde es más útil un lenguaje claro y simple que pueda entender cualquier persona, y no un lenguaje técnico y engorroso que solo es natural para los especialistas en determinada materia. 4. Datos personales. Los asistentes virtuales deben informar en todo momento a las personas sobre el tratamiento que se le dará a los datos personales y las condiciones de seguridad de los mismos. 5. Transparencia. El asistente virtual debe explicarle a la persona que se trata de un robot y no es una persona la que se encuentra detrás del chat. Además, no debe suplantar, manipular ni perturbar la capacidad de las personas de formarse y mantener opiniones o de recibir y expresar ideas. 6. Rol de los seres humanos. Se debe ofrecer la posibilidad de hablar con una persona humana que preste sus servicios a las administraciones públicas.

en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales, debiendo implementar acciones como el consentimiento previo para la recogida y tratamiento de los datos.

Es decir; para generar confianza y facilitar el acercamiento entre las personas mayores de 65 años y las administraciones públicas a través de las tecnologías de la información y al comunicación es fundamental que se les informe sobre el tratamiento que se le dará a los datos personales y las condiciones de seguridad de los mismos, todo ello en términos claros y sencillos que permitan la comprensión del uso que se le dará a los datos de estas personas.[79]

4.4 Asistencia en el uso de las herramientas digitales

Para Martínez Gutiérrez[80] y Beltrán Castellanos[81] uno de los derechos que cobra relevancia en la lucha contra la brecha digital y la promoción del envejecimiento activo es el relativo a la asistencia de las personas para el acceso a cualquier tramitación administrativa y que tiene como contrapartida la obligación de las administraciones públicas de garantizar que dichas personas se puedan relacionar con ésta a través de medios electrónicos.

Dicha obligación tiene su fundamento en el artículo 12 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas que prevé que los órganos y entes del sector público deben poner a disposición de las personas "los canales de acceso que sean necesarios, así como los sistemas y aplicaciones que en cada caso se determinen".

Respecto de las personas mayores de 65 años, es importante destacar que cuando la Ley hace referencia a "los canales de acceso que sean necesarios" estos no siempre deberán ser electrónicos o digitales, por el contrario, tomando en consideración las especiales características de este grupo de personas, que pueden incluso desconocer cómo hacer uso de un dispositivo o medio electrónico, es necesario que las administraciones públicas brinden asistencia personalizada, ya sea para enseñarle a la persona a utilizar la herramienta, dispositivo o aplicación

79 STRINGHINI, Antonella. Asistencia virtual automatizada e inclusiva para optimizar la relación de la ciudadanía con la Administración Pública. *International Journal of Digital Law*, Belo Horizonte, año 1, núm. 1, p. 126. 2020 124-125.

80 MARTÍNEZ GUTIÉRREZ, Rubén. "Administración electrónica e inclusión digital en las entidades locales medianas y pequeñas: Brecha digital, servicios públicos y nuevos modelos de atención a la ciudadanía". En: FONDEVILA ANTOLÍN, Jorge (dir.), *Transformación digital en las medianas y pequeñas entidades locales: retos en clave de eficiencia y sostenibilidad*. Madrid: Wolters Kluwer Legal & Regulatory España, S.A, 2022. p. 115.

81 BELTRÁN CASTELLANOS, José Miguel. *La brecha digital en las relaciones de la ciudadanía con las administraciones públicas*, *op. cit.*, p. 122.

electrónica que se trate o para permitirle acceder a cualquier trámite administrativo sin hacer uso de dichas herramientas tecnológicas.

5 Conclusiones

El envejecimiento es un proceso complejo que requiere afrontar, no solo cambios físicos, sino que es necesario, además, desarrollar nuevas capacidades y adquirir nuevos conocimientos, más aún cuando actualmente pueden identificarse, al menos, dos tipos de generaciones: los nativos y los inmigrantes digitales. Los nativos digitales son aquellas personas que nacen en un ambiente en el que las tecnologías de la información y la comunicación forman parte de su vida diaria y no se imaginan la vida sin ellas; mientras que los migrantes digitales son aquellas personas que nacieron en una época donde las mencionadas tecnologías eran limitadas o se encontraban muy poco desarrolladas y no están acostumbradas a relacionarse día a día con ellas.[82]

Las tecnologías de la información y la comunicación, si bien han demostrado que proporcionan múltiples beneficios a las personas y su relación con las instituciones públicas, también plantean retos importantes, sobre todo frente a las personas mayores y el envejecimiento. Que dichas tecnologías se conviertan en un aliado o en un enemigo de nuestros mayores dependerá de cómo los distintos órganos y entes públicos aborden el problema de la brecha digital.

Debemos tener presente que el objetivo de las tecnologías de la información y la comunicación es dejar de ser un elemento de exclusión para convertirse en un mecanismo de integración social y de enriquecimiento mutuo entre las diferentes generaciones que cohabitan en una misma comunidad.[83] Un instrumento que puede contribuir a abordar los retos del envejecimiento: la prevención de la dependencia, la prevención del aislamiento y la soledad no deseada, la promoción del envejecimiento activo, la vida en el entorno propio, entre otros.[84] Por ello, los órganos y entes públicos deben garantizar que los servicios que ofrecen a las personas, aun cuando deban ajustarse a las nuevas tecnologías, también deban considerar a los no nativos digitales. Asimismo, deberán promover la formación digital y garantizar que toda persona tenga la oportunidad de adaptarse a la administración pública digital.[85]

---

82 GONZÁLEZ GARCÍA, Erika; MARTÍNEZ HEREDIA, Nazaret. Personas mayores y TIC: oportunidades para estar conectados, *op. cit.*, p. 1131.

83 RODRÍGUEZ RÚA, Adela Augusta; GONZÁLEZ RODRÍGUEZ, Rubén. Un paso más hacia la autogestión digital: proyecto para la autonomía y la inclusión de las personas mayores. *Humanismo y Trabajo Social*, León, núm. 17, p. 188. 2017.

84 SÁNCHEZ FUENTES, David; EIZMENDI LORIZ; Gorka; AZCOITIA ARRECHE, José Miguel. Envejecimiento y nuevas tecnologías, *op. cit.*, p. 64.

85 BARRIO ANDRÉS, Moisés. *Los derechos digitales y su regulación en España, la Unión Europea e Iberoamérica*. A Coruña: Editorial Colex, 2023. p. 81.

En España existe un marco jurídico que promueve la transformación digital y la inclusión de las personas en el uso de las tecnologías de la información y la comunicación. Asimismo, la pandemia de Covid-19 demostró que las personas mayores son capaces de adaptarse y reinventarse, pero deben ser acompañadas en dicho proceso y las instituciones públicas juegan un rol fundamental en ello. La vejez es tan solo una etapa más en la vida en la que se puede continuar aprendiendo, mejorando y creciendo emocional y socialmente.

Las administraciones públicas deben estar al servicio de la personas y no al revés, por ello tienen la obligación de remover los obstáculos que puedan derivar de la implementación de las tecnologías de la comunicación y la información en sus tareas diarias, para permitirle a las personas mayores de 65 años el disfrute efectivo de sus derechos, el acceso a los servicios públicos y a las prestaciones del sistema de seguridad social, evitando la discriminación, el aislamiento y la exclusión social.

Referencias

AGUDO PRADO, Susana; PASCUAL SEVILLANO, María Ángeles; FOMBONA CADAVIECO, Javier. Usos de las herramientas digitales entre las personas mayores. *Comunicar: Revista Científica de Comunicación y Educación*, Sollihul, núm. 39, pág. 193-201. 2012.

ALEXOPOULOU, Sofia; ÅSTRÖM, Joachim. (2022). How the Responsibility of Digital Support for Older People is Allocated? The Swedish Welfare System at the Crossroads. *Research on Ageing and Social Policy: (RASP)*, Barcelona, vol. 10, núm. 1, pág. 48-76. 2022.

ARIAS FERNÁNDEZ, Enrique; LIRIO CASTRO, Juan; ALONSO GONZÁLEZ, David; HERRANZ AGUAYO, Inmaculada. Acceso y uso de las TIC de las mujeres mayores de la Europa comunitaria. *Prisma Social: Revista de Investigación Social*, Madrid, núm. 21, pág. 282-315. 2018.

ÁVILA-RODRÍGUEZ DE MIER, Belén; MARTÍN GARCÍA, Noemi. La frecuencia del uso de internet como determinante de la vulnerabilidad entre la población sénior: usuario habitual vs. no usuario habitual. *Revista Mediterránea de Comunicación*, Alicante, vol. 10, núm. 1, pág. 13-26. 2019.

BALLESTER ESPINOSA, Adrián. La transformación digital forzosa en la Administración Pública: cómo la tecnología ayudará en un futuro cercano a los gobiernos en la toma de decisiones. *Telos: Cuadernos de Comunicación e Innovación*, Madrid, núm. 117, pág. 146-151. 2021.

BARRIO ANDRÉS, Moisés. *Los derechos digitales y su regulación en España, la Unión Europea e Iberoamérica*. A Coruña: Editorial Colex, 2023. 156p.

BELTRÁN CASTELLANOS, José Miguel. *La brecha digital en las relaciones de la ciudadanía con las administraciones públicas.* Valencia: Tirant lo Blanch, 2024. 276p.

BUNBURY BUSTILLO, Eva; PÉREZ CALLE, Ricardo Diego; OSUNA ACEDO, Sara. Las competencias digitales en personas mayores: de amenaza a oportunidad. *Vivat Academia*, Madrid, núm. 155, pág. 173-195. 2022.

CABALLERO ÁLVAREZ, Abel. (2020). "Nuevas pobrezas" a raíz de la pandemia. En DE FRUTOS, Javier; ARIAS LERA, Alejandro; LOSOVIZ, Lucia; BERNAL, Paola (coords.), *El rol de los gobiernos locales en la lucha contra la pobreza infantil en el contexto de la emergencia de la COVID-19.* Madrid: Ministerio de Sanidad, Consumo y Bienestar Social, 2020. p. 11-13.

CAMILLI TRUJILLO, Celia Rosa (coords.), *La educación mediática en España*: artículos seleccionados. Madrid, Universitas, 2018. p. 321-338.

CASADO MUÑOZ, Raquel; LEZCANO BARBERO, Fernando; RODRÍGUEZ CONDE, María José. Envejecimiento activo y acceso a las tecnologías: Un estudio empírico evolutivo. *Comunicar: Revista Científica de Comunicación y Educación*, Sollihul, núm. 45, pág. 37-46. 2015.

CASTILLO BLANCO, Federico. El tránsito a una administración digital y robotizada: el necesario cambio del modelo de administración y empleo público. *Revista Iberoamericana de Gobierno Local*, Granada, núm. 19, pág. 1-33. 2021.

CASTILLO RIQUELME, Víctor; CIFUENTES AGUAYO, Edgar; ÓRDENES ÓRDENES, Danitza; GATICA PARRA, Josefa. Depresión y aislamiento social en personas mayores, análisis del rol de la participación tecnológica. *Revista de Investigación en Psicología*, Lima, vol. 26, núm. 1, pág. 77-96. 2023.

CERRILLO MARTÍNEZ, Agustí. La regulación de la administración electrónica local: el caso del Ayuntamiento de Barcelona. *Anuario del Gobierno Local*, Barcelona, núm. 1, pág. 179-214. 2006.

COTINO HUESO, Lorenzo. El nuevo reglamento de Administración electrónica, que no innova en tiempos de transformación digital. *Revista Catalana de Dret Públic*, Barcelona, núm. 63, pág. 118-136. 2021.

CRUZ-DÍAZ, Rocío; ORDÓÑEZ-SIERRA, Rosario; ROMÁN GARCÍA, Sara; PAVÓN RABASCO, Francisco. Buenas prácticas que desarrollan la competencia mediática en entornos socioeducativos. En: FUENTE COBO, Carmen; GARCÍA GALERA, María del Carmen;

CRUZ-DÍAZ, Rocío; REBOLLEDO GÁMEZ, Teresa. Herramientas tecnológicas y colaboración con terapias alternativas: el profesional de la educación social ante el envejecimiento y la discapacidad intelectual. En: ROIG VILA, Rosabel (coord.), *Tecnología, innovación e investigación en los procesos de enseñanza-aprendizaje.* Barcelona, Ediciones Octaedro, 2016. p. 304-312.

DINANT, Inès; SOLA, Ángel. TIC por el envejecimiento activo en Asturias: formación tecnológica para mejorar la calidad de vida de las personas mayores. + *Calidad*, Oviedo, núm. 26, pág. 9-30. 2022.

DOMÍNGUEZ MARTÍN, Mónica. Políticas públicas y configuración de los servicios de protección y atención a las personas mayores. El protagonismo de los municipios. *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, Madrid, núm. 25, pág. 249-279. 2021.

EGEA DE HARO, Alfonso. La definición y localización de la política de mayores. En: DÍEZ SASTRE, Silvia; RODRÍGUEZ DE SANTIAGO, José María (dirs.), *Ciudades envejecidas*: El derecho y la política local para la protección y cuidado de las personas mayores. Navarra: Aranzadi, 2021. p. 21-60.

ETCHEMENDY, Ernestina; CASTILLA, Diana; BAÑOS RIVERA, Rosa María; BOTELLA ARBONA, Cristina. Sistema Mayordomo: la puerta de entrada de nuestros mayores a las nuevas tecnologías. *Ariadna: Cultura, Educación y Tecnología*, Castellón, vol. 1, núm. 1, pág 33-38. 2013.

FERNÁNDEZ CAMPOMANES, María; FUEYO GUTIÉRREZ, Aquilina. Redes sociales y mujeres mayores: estudio sobre la influencia de las redes sociales en la calidad de vida. *Revista Mediterránea de Comunicación*, Alicante, vol. 5, núm. 1, pág. 157-177. 2014.

FUENTES i GASÓ; Josep Ramon; VIVAS ROSO, Jessica. Transformación digital de las administraciones públicas, brecha digital y envejecimiento activo. En: GIFREU i FONT, Judith (coord.). *El envejecimiento activo como nuevo reto para los gobiernos locales*: La construcción jurídica de servicios públicos y espacios amigables para las personas mayores. Barcelona: Aranzadi, 2024. p. 475-495.

FUNDACIÓN COTEC. *Administración electrónica y personas mayores*: Mejoras en el acceso y uso de la Administración electrónica por parte de las personas mayores. Madrid: Universidad de Murcia, 2021. 56 p.

GOBIERNO DE ESPAÑA. *II Plan Nacional de Accesibilidad. Universal. España, país accesible*. Madrid: Ministerio de Derechos Sociales y Agenda 2030, 2023. 101p.

GÓMEZ NAVARRO, Dulce Angélica; ALVARADO LÓPEZ, Raúl Arturo; MARTÍNEZ DOMÍNGUEZ, Marlen; DÍAZ DE LEÓN CASTAÑEDA, Christian. La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México. *Entreciencias: Diálogos en la Sociedad del Conocimiento*, Ciudad de México, vol. 6, núm. 16, pág. 49-64. 2018.

GONZÁLEZ GARCÍA, Erika; MARTÍNEZ HEREDIA, Nazaret. Personas mayores y TIC: oportunidades para estar conectados. *RES: Revista de Educación Social*, Barcelona, núm. 24, pág. 1128-1141. 2017.

GONZÁLEZ OÑATE, Cristina, y FANJUL PEYRÓ, Carlos. Aplicaciones móviles para personas mayores: un estudio sobre su estrategia actual. *Aula Abierta*, Oviedo, vol. 47, núm. 1, pág. 107-112. 2018.

GONZÁLEZ OÑATE, Cristina; FANJUL PEYRÓ, Carlos; CABEZUELO-LORENZO, Francisco. Uso, consumo y conocimiento de las nuevas tecnologías en personas mayores en Francia, Reino Unido y España. *Comunicar: Revista Científica de Comunicación y Educación*, Sollihul, núm. 45, pág. 19-28. 2015.

GRUPO DE INVESTIGACIÓN BRECHA DIGITAL Y PERSONAS MAYORES. *Séniors digitales:* Informe sobre el uso del comercio y la administración electrónica en España. Madrid: CEU Ediciones, 2021. 76p.

HAZ GÓMEZ, Francisco Eduardo; MANZANERA ROMÁN, Salvador. Administración electrónica y personas mayores: retos metodológicos para el estudio de la exclusión digital entre la población mayor de edad. En: IZAOLA ARGÜESO, Amaia (coord.), *Actas del VIII Congreso de la Red Española de Política Social:* Cuidar la vida, garantizar la inclusión, convivir en diversidad: consensos y retos. Bilbao: Servicio Editorial de la Universidad del País Vasco, 2022. p. 1855-1868.

MALDONADO MELÉNDEZ, Mirko. Del gobierno electrónico a la administración digital: las transformaciones digitales en Iberoamérica. *Anuario de la Red Eurolatinoamericana de Buen Gobierno y Buena Administración*, Buenos Aires, núm. 3, pág. 1-22. 2023. Disponible en: https://ijeditores.com/pop.php?option=articulo&Hash=ea8464e399a5e99ac727fc8f1b77540f. Consultado el: 15 de agosto de 2024.

MARTÍNEZ GUTIÉRREZ, Rubén. "Administración electrónica e inclusión digital en las entidades locales medianas y pequeñas: Brecha digital, servicios públicos y nuevos modelos de atención a la ciudadanía". En: FONDEVILA ANTOLÍN, Jorge (dir.), *Transformación digital en las medianas y pequeñas entidades locales: retos en clave de eficiencia y sostenibilidad*. Madrid: Wolters Kluwer Legal & Regulatory España, S.A, 2022. pp. 99-124.

MARTÍNEZ GUTIÉRREZ, Rubén. Elementos para la configuración de la administración digital. *Revista de Derecho Administrativo*, Lima. núm. 20, pág. 212-233. 2021.

OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD. *Estudio sobre digitalización de la Administración.* Madrid: Ministerio de Asuntos Económicos y Transformación Digital, 2021. 25p.

OLARTE ENCABO, Sofía. Brecha digital, pobreza y exclusión social. *Temas laborales: Revista Andaluza de Trabajo y Bienestar Social*, Sevilla, núm. 138, pág. 285-313. 2017.

ORGANIZACIÓN MUNDIAL DE LA SALUD. Envejecimiento activo: un marco político. *Revista Española de Geriatría y Gerontología*, Barcelona, vol. 37, núm. 2, pág. 74-105. 2002.

PERAL PERAL, Begoña; VILLAREJO RAMOS, Ángel Francisco; ARENAS GAITÁN, Jorge. Descifrando la brecha digital de los mayores. *Panorama Social*, Madrid, núm. 25, pág. 67-82. 2017.

RAGNEDDA, Massimo. *The Third Digital Divide:* A Weberian Approach to Digital Inequalities. Nueva York: Routledge, 2017. 128p.

RANDO BURGOS, Esther. Nuevos retos en la Administración del siglo XXI: digitalización, inteligencia artificial y transformación administrativa. Disponible en: <https://laadministracionaldia.inap.es/noticia.asp?id=1514543>. Consultado el: 30 de agosto de 2024.

REAL PATRONATO SOBRE DISCAPACIDAD. *Estudio de accesibilidad de los trámites con la Administración Pública en España*. Madrid: Ministerio de Sanidad, Consumo y Bienestar Social, 2017. 124p.

RODRÍGUEZ RÚA, Adela Augusta; GONZÁLEZ RODRÍGUEZ, Rubén. Un paso más hacia la autogestión digital: proyecto para la autonomía y la inclusión de las personas mayores. *Humanismo y Trabajo Social*, León, núm. 17, pág. 173-191. 2017.

SÁNCHEZ FUENTES, David; EIZMENDI LORIZ; Gorka; AZCOITIA ARRECHE, José Miguel. Envejecimiento y nuevas tecnologías. *Revista Española de Geriatría y Gerontología*, Barcelona, vol. 41, núm. 2, pág. 57-75. 2006.

SÁNCHEZ VALLE, María; LLORENTE BARROSO, Carmen. Desafíos de la administración electrónica para la inclusión de las personas mayores en la sociedad digital. *Revista Española de la Transparencia*, Madrid, núm. 16, pp. 217-243. 2023.

SÁNCHEZ-VALLE, María; VINARÁS ABAD, Mónica; LLORENTE-BARROSO, Carmen. Empowering the Elderly and Promoting Active Ageing Through the Internet: The Benefit of e-inclusion Programmes. In: WITHIN KOLLAK, Ingrid (ed.), *Safe at Home with Assistive Technology.* Cham: Springer International Publishing, 2017. p. 95-108.

SANZ, Elena. La brecha digital en los mayores: solo un 37,5% interactúa con la administración electrónica. Disponible en: <https://theconversation.com/la-brecha-digital-en-los-mayores-solo-un-37-5-interactua-con-la-administracion-electronica-222315>. Consultado el: 30 de agosto de 2024.

SEVILLA CARO, Maricela; SALGADO SOTO, María del Consuelo; OSUNA MILLÁN, Nora del Carmen. Envejecimiento activo. Las TIC en la vida del adulto mayor. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, Guadalajara, vol. 6, núm. 11, pág. 574-587. 2015.

SOBRINO GARCÍA, Itziar. Las 'smart cities' y la inteligencia artificial. Nuevos retos de las administraciones públicas en la gobernanza inteligente. En: SOBRINO GARCÍA, Itziar (coord.), *Justicia, administración y derecho:* nuevos retos del derecho en el siglo XXI. Pamplona: Thomson Reuters Aranzadi, 2021, p. 157-177.

STRINGHINI, Antonella. Asistencia virtual automatizada e inclusiva para optimizar la relación de la ciudadanía con la Administración Pública. *International Journal of Digital Law*, Belo Horizonte, año 1, núm. 1, pág. 117-128. 2020.

SUNKEL, Guillermo; ULLMANN, Heidi. Las personas mayores de América Latina en la era digital: superación de la brecha digital. *Revista de la CEPAL*, Vitacura, núm. 127, pág. 243-268. 2019.

VILLAREJO RAMOS, Ángel Francisco; RONDÁN CATALUÑA, Francisco Javier; REVILLA-CAMACHO, María Ángeles. Tipología de compradores online mayores de 55 años. *Innovar: Revista de Ciencias Administrativas y Sociales*, Bogotá, vol. 26, núm. 59, pág. 61-72. 2016.

VIÑARÁS-ABAD, Mónica; ABAD-ALCALÁ, Leopoldo; LLORENTE-BARROSO, Carmen; SÁNCHEZ-VALLE, María; PRETEL-JIMÉNEZ, Marilé. Administración electrónica y e-inclusión de las personas mayores. *Revista Latina de Comunicación Social*, vol. 72, núm. 2, pp. 197-219. 2017.

VIÑARÁS-ABAD, Mónica; PRETEL-JIMÉNEZ, Marilé; QUESADA-GONZÁLEZ, Carlos. E-commerce, social media and social inclusion A typology of users over 60 years of age in Spain. *Comunicación y Sociedad*, Navarra, vol. 35, núm. 3, pp. 141-154. 2022.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

FUENTES GASÓ, Josep Ramon; VIVAS ROSO, Jessica. Derechos de las personas mayores frente a la Administración Pública digital. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 33-58, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.gaso.

Informações adicionais

Additional information

INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 05 · n. 02 · maio/agosto 2024 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.5.n.2

05

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

International Journal of Digital Law – IJDL
ISSN 2675-7087
DOI: 10.47975/digital.law.vol.5.n.2.alonso

La libertad de expresión en plataformas digitales amenazada en la UE: los casos Twitter y Telegram

Freedom of expression on digital platforms threatened in the EU: the Twitter and Telegram cases

José María Pernas Alonso*
I Universidad Autónoma de Madrid (Madrid, España)
jmpernas@icam.es
https://orcid.org/0000-0002-6738-6601

Recebido/Received: 28.08.2024/ August 28th, 2024
Aprovado/Approved: 01.11.2024 / November 1st, 2024

Resumen: El 18 de diciembre de 2023 la Comisión Europea inició una investigación contra Twitter (actual X), con base en la llamada Ley de Servicios Digitales de la Unión Europea (UE). En agosto de 2024 se ha conocido la detención por el Estado francés del fundador de Telegram, Pável Dúrov, por no aceptar la restricción de contenidos exigida en dicha red social. Todas estas acciones conducen a analizar si el valor de la libertad y el derecho de libertad de expresión están en peligro en la UE y su caracterización en la Carta de Derechos Fundamentales la UE (CDFUE) y en la jurisprudencia del Tribunal de Justicia de la UE (TJUE) y del Tribunal Europeo de Derechos Humanos (TEDH).

Palabras-clave: Libertad de expresión; servicios digitales; derechos fundamentales; Unión Europea; plataformas digitales.

Abstract: The 18th of December 2023 the European Commission started an administrative procedure against Twitter (currently called X), based on the European Digital Services Act. In August 2024 the French Police has arrested the founder of Telegram, Pável Dúrov, for non-accepting the content restriction in the abovementioned platform. All these public actions led us to analyze if the value of liberty and the freedom of expression right are being respected and protected in the European Union, based on the regulation established on the EU Chart for Fundamental Rights and the jurisprudence of the European Court of Justice and the European Court of Human Rights.

Como citar esse artigo/*How to cite this article*: PERNAS ALONSO, José María. La libertad de expresión en plataformas digitales amenazada en la UE: los casos Twitter y Telegram. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 61-78, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.alonso.

* Doctor en Derecho, Gobierno y Políticas Públicas por la Universidad Autónoma de Madrid (Madrid, España). Licenciado en Derecho (2007) y Ciencias Políticas y de la Administración (2008) por la Universidad Pontificia Comillas de Madrid. Abogado colegiado ICAM (2007). Abogado. E-mail: jmpernas@icam.es.

Keywords: Freedom of expression; digital services; fundamental rights; European Union; digital platforms.

1 Introducción

Cuando el 18 de diciembre de 2023 la Comisión Europea inició un procedimiento contra la red social Twitter (actualmente X),[1] por vulnerar la Ley Europea de Servicios Digitales (LESD),[2] pocos juristas osaron mencionar que dicha actuación pudiera ser contraria a los derechos fundamentales consagrados en la CDFUE. Sin embargo, la reciente detención por Francia del fundador de Telegram, otra plataforma digital, está poniendo en cuestión si en la UE se está garantizando el valor de la libertad y el derecho a la libertad de expresión, que son la base del Estado liberal democrático y de los propios valores del artículo 2 del Tratado de la UE (TUE).[3]

En este estudió analizaremos las motivaciones de la UE para incoar ese procedimiento de investigación frente a Twitter (actualmente X), en función de la regulación de la LESD. También las motivaciones de un juez francés para ordenar la detención del Fundador de Telegram, para comprobar que versan sobre la misma exigencia de moderar contenidos o supervisarlos para atribuir a sujetos privados las responsabilidades en materia de prevención de comisión de supuestos hechos delictivos. Se analizará si esas potestades de la Comisión Europea son proporcionadas y respetuosas del valor de la libertad y del derecho a la libertad de expresión en un régimen democrático conforme a la jurisprudencia del TJUE y del TEDH y del TC español. Se finaliza con una reflexión sobre los derechos individuales como antecedentes del poder político y las bases morales de la democracia.

1 COMISIÓN EUROPEA. *La Comisión incoa un procedimiento formal contra X en virtud de la Ley de Servicios Digitales.* Comunicado de Prensa. Disponible en: <https://ec.europa.eu/commission/presscorner/detail/es/ip_23_6709>. Acceso el: 28 ago. 2024.

2 Ley compuesta principalmente por el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE, de directa aplicación a todos los Estados miembros. En adelante, designaremos a ese conjunto normativo como LESD.

3 "La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Estos valores son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres".

2 El procedimiento de investigación iniciado por la Comisión Europea contra Twitter

En el Comunicado de Prensa de 18 de diciembre de 2023 titulado "La Comisión incoa un procedimiento formal contra X en virtud de la Ley de Servicios Digitales", la Comisión Europea justificó la iniciación de un procedimiento contra Twitter (X) con base en los siguientes hechos y artículos de la LESD (énfasis añadido):

> La Comisión Europea ha incoado un procedimiento formal para evaluar si X podría haber infringido la Ley de Servicios Digitales en ámbitos relacionados con *la gestión de riesgos, la moderación de contenidos, las interfaces engañosas, la transparencia de la publicidad y el acceso de los investigadores a los datos.*
>
> Sobre la base de la investigación preliminar realizada hasta la fecha, y concretamente un análisis del informe de evaluación de riesgos presentado por X en septiembre, del informe de transparencia de X publicado el 3 de noviembre y de las respuestas de X a una solicitud formal de información, que, entre otras cosas, se refería a la difusión de contenidos ilícitos en el contexto de los ataques terroristas de Hamás contra Israel, la Comisión ha decidido incoar un procedimiento formal de infracción contra X en virtud de la Ley de Servicios Digitales.
> El procedimiento se centrará en lo siguiente:
> El cumplimiento de las obligaciones de la Ley de Servicios Digitales relacionadas con la *lucha contra la difusión de contenidos ilícitos en la UE*, y en particular en relación con la evaluación de riesgos y las medidas de mitigación adoptadas por X para contrarrestar la difusión de contenidos ilícitos en la UE, así como el funcionamiento del mecanismo de notificación y acción en relación con los contenidos ilícitos en la UE dispuesto por la Ley de Servicios Digitales, también a la luz de los recursos de moderación de contenidos de X.
> La eficacia de las medidas adoptadas para luchar contra *la manipulación de la información en la plataforma*, sobre todo la eficacia del denominado sistema de notas comunitarias de X en la UE y la eficacia de las políticas conexas para mitigar los *riesgos desde el punto de vista del discurso cívico y los procesos electorales.*
> Las medidas adoptadas por X para aumentar la transparencia de su plataforma. La investigación se refiere a presuntas *deficiencias a la hora de conceder a los investigadores acceso a los datos de acceso público de X*, conforme a lo dispuesto en el artículo 40 de la Ley de Servicios Digitales, así como a deficiencias en el repositorio de anuncios de X.
> Un presunto *diseño engañoso de la interfaz de usuario*, sobre todo en relación con las marcas de verificación vinculadas a determinados productos de suscripción, las llamadas marcas azules.

> Si se demuestran, estos incumplimientos constituirían infracciones del artículo 34, apartados 1 y 2, del artículo 35, apartado 1, del artículo 16, apartados 5 y 6, del artículo 25, apartado 1, del artículo 39 y del artículo 40, apartado 12, de la Ley de Servicios Digitales. La Comisión se dispone ahora a realizar una investigación pormenorizada con carácter prioritario. La incoación de un procedimiento formal de infracción no prejuzga su resultado.
> Se trata del primer procedimiento formal iniciado por la Comisión para hacer cumplir el primer marco horizontal a escala de la UE en materia de responsabilidad de las plataformas en línea, tan solo tres años después de su propuesta.

Recientemente hemos conocido que la Comisión Europea ha remitido a Meta un requerimiento de información amparada en dicha LESD.[4]

Como veremos, las imputaciones realizadas por la Comisión Europea a la red social Twitter son bastantes similares a las que imputa el Estado francés al fundador de Télegram, detenido en agosto de 2024: *la gestión de riesgos, la moderación de contenidos, las interfaces engañosas, la transparencia de la publicidad y el acceso de los investigadores a los datos.* Estamos ante una limitación de la libertad, valor supremo de las Constituciones nacionales de los estados miembros de la UE y reconocido en la CDFUE y en Convenio Europeo de Derechos Humanos (CEDH) y de la libertad de expresión.

Como demostraremos, la garantía de un Estado democrático se basa en el respeto de los derechos individuales innatos al individuo, y por ende de una serie de valores morales, por lo que no cabe utilizar presunciones para limitar dichos derechos individuales (entre los cuales la libertad de expresión es de los fundantes del Estado liberal democrático en el siglo XIX en Europa).

Si se analizan las motivaciones de la Comisión Europea (resaltadas en negrita por mi parte en el Comunicado de Prensa citado), se comprueba que estamos ante conceptos jurídicos indeterminados, es decir que pueden ser utilizados de forma arbitraria para minar la libertad y la libertad de expresión:

- Contenidos ilícitos en la UE:
- Manipulación de la información en la plataforma.
- deficiencias a la hora de conceder a los investigadores acceso a los datos de acceso público de X.
- diseño engañoso de la interfaz de usuario.

[4] COMISIÓN EUROPEA. *"La Comisión Europea envía una solicitud de información a Meta en virtud de la Ley de Servicios Digitales"*. Comunicado de Prensa. Disponible en: <https://digital-strategy.ec.europa.eu/es/news/commission-sends-request-information-meta-under-digital-services-act-2>. Acceso el: 28 ago. 2024.

Además, las potestades administrativas de autotutela declarativa y ejecutiva sobre supervisión de actividades privadas entrañan riesgos para los derechos individuales. Por eso, el Tribunal Supremo de los EE.UU. ha considerado en su reciente sentencia SEC v. Jarkosy,[5] que una agencia administrativa como la Securities and Exchange Commission no puede ejecutar multas contra una empresa supervisada sin que un jurado lo confirme, dado que lo contrario sería vulnerar la Séptima Enmienda de la Constitución de los EE.UU.

3 La ley de servicios digitales de la UE y la libertad de expresión

Es preciso analizar si la LESD contiene normas que permitan a la Comisión Europea limitar, mediante procedimientos administrativos, la libertad de expresión y el valor de la libertad. Es decir, si la Comisión Europea tiene autotutela declarativa, y sobre todo ejecutiva, para suspender la actividad de plataformas digitales.

En primer lugar, hay que tener en cuenta que la LESD establece un régimen especial de sujeción a grandes plataformas digitales, al que no están sujetos otras plataformas con menor facturación o difusión. Así, X (antes llamada Twitter) fue designada plataforma en línea de muy gran tamaño el 25 de abril de 2023 en virtud de la Ley de Servicios Digitales de la UE, tras su declaración de tener 112 millones de usuarios activos mensuales en la UE, según lo notificado a la Comisión el 17 de febrero de 2023.

Como plataforma en línea de muy gran tamaño, X ha tenido que cumplir una serie de obligaciones establecidas en la Ley de Servicios Digitales transcurridos cuatro meses tras su designación.

Recordemos que el Reglamento Europeo de Servicios Digitales entró en vigor el 17 de febrero de 2024, aunque desde finales de 2023 se aplican a plataformas designadas por la Comisión Europea con más de 45 millones de usuarios en la UE. Este Reglamento Europeo (que es una Ley de directo cumplimiento para los Estados Miembros), que establece obligaciones de información a grandes plataformas,[6] en concreto las siguientes:[7]

---

5 SUPREME COURT OF THE UNITED STATES. *Securities and Exchange Commission v. Jarkesy et al*. Disponible en: <https://www.supremecourt.gov/opinions/23pdf/22-859_1924.pdf>.

6 Autores como Valiente Martínez entienden que con este Reglamento europeo "se está exigiendo a las redes sociales que lleven a su máximo alcance el procedimiento de 'notice and takedown', pero de una forma mucho más generalista y no sólo para proteger los derechos de autor. Esta política, tan alejada de la doctrina de los puertos seguros, no carece de defensores; al fin y al cabo, el Derecho debe brindar protección jurídico-constitucional a quienes emplean las redes sociales. Además, si otros medios de difusión afrontan distintos escenarios de responsabilidad, ya sea administrativa, civil o aun penal, no parece sostenible la exención de los ISP´s.". VALIENTE MARTÍNEZ, Francisco. La libertad de expresión y las redes sociales: de la doctrina de los puertos seguros a la moderación de contenidos. *Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos*, n. 48, enero 2023, p. 196, 2023.

7 Según argumentario de la Comisión Europea disponible en: <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_es>.

> - "Las plataformas en línea y los motores de búsqueda de muy gran tamaño plantean especiales riesgos en cuanto a difusión de contenidos ilícitos y nocivos para la sociedad. Se contemplan normas específicas para las plataformas que lleguen a más del 10 % de los 450 millones de consumidores europeos. La lista de plataformas designadas está disponible en DSA: Plataformas en línea muy grandes y motores de búsqueda
> - Las plataformas en línea reúnen a vendedores y consumidores, tales como mercados en línea, tiendas de aplicaciones, plataformas de economía colaborativa y plataformas de medios sociales.
> - Servicios de alojamiento de datos como la nube y los servicios de alojamiento web (incluidas también las plataformas en línea).
> Los servicios de intermediación ofrecen infraestructuras de red: proveedores de acceso a internet y registradores de nombres de dominio (incluidos también los servicios de alojamiento de datos)."

Por eso la LESD (o *Digital Services Act*), clasifica plataformas o motores de búsqueda que tienen más de 45 millones de usuarios al mes en la UE como plataformas en línea de muy gran tamaño (VLOP) o motores de búsqueda en línea de muy gran tamaño (VLOSEs).[8] La Comisión desginó VLOP o VLOSE sobre la base de los números de usuario proporcionados por las plataformas y los motores de búsqueda, que, independientemente de su tamaño, estaban obligados a publicar antes del 17 de febrero de 2023.

Las Obligaciones para VLOPs y VLOSEs según la LESD serían los siguientes:

- establecer un punto de contacto para las autoridades y los usuarios
- denunciar delitos penales
- tener términos y condiciones fáciles de usar
- ser transparentes en lo que respecta a la publicidad, los sistemas de recomendación o las decisiones de moderación del contenido
- También deben seguir las reglas que se centran solo en los VLOP y VLOSEs debido a su tamaño y el impacto potencial que pueden tener en la sociedad. Esto significa que deben identificar, analizar y evaluar los riesgos sistémicos que están vinculados a sus servicios. Deben examinar, en particular, los riesgos relacionados con:
  - contenidos ilícitos
  - derechos fundamentales, como la libertad de expresión, la libertad y el pluralismo de los medios de comunicación, la discriminación, la protección de los consumidores y los derechos de los niños

[8] Lista de VLOP y VLOPSEs designados por la Comisión Europea disponible en: <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>.

  - seguridad pública y procesos electorales
  - violencia de género, salud pública, protección de menores y bienestar mental y físico
  - Una vez identificados los riesgos y notificados a la Comisión para su supervisión, los VLOP y los VLOSE están obligados a adoptar medidas que mitiguen estos riesgos. Esto podría significar adaptar el diseño o el funcionamiento de sus servicios o cambiar sus sistemas de recomendación. También podrían consistir en reforzar la plataforma internamente con más recursos para identificar mejor los riesgos sistémicos.
- Establecer una función de cumplimiento interno que garantice que los riesgos identificados se mitiguen
- Ser auditado por un auditor independiente al menos una vez al año y adoptar medidas que respondan a las recomendaciones del auditor.
- Compartir sus datos con la Comisión y las autoridades nacionales para que puedan supervisar y evaluar el cumplimiento de la norma DSA
- permitir a los investigadores examinados acceder a los datos de la plataforma cuando la investigación contribuya a la detección, identificación y comprensión de los riesgos sistémicos en la UE
- proporcionar una opción en sus sistemas de recomendación que no se basa en la creación de perfiles de usuario
- disponer de un repositorio de anuncios a disposición del público

Según el Comunicado de Prensa de la Comisión Europea, Twitter podría estar incumpliendo varios artículos de la LESD.

En primer lugar, las obligaciones del artículo 34, apartados 1 y 2, y el artículo 35, apartado 1, dado que como plataforma de gran tamaño estaría obligada a detectar, analizar y evaluar con diligencia cualquier riesgo sistémico en la Unión derivado del diseño o el funcionamiento de su servicio y sus sistemas conexos, o del uso que se haga de sus servicios. Al realizar evaluaciones de riesgos, las plataformas en línea de muy gran tamaño deben tener en cuenta varios factores que influyen en los riesgos sistémicos, tales como los sistemas de recomendación, los sistemas de publicidad o la manipulación intencionada del servicio, por ejemplo, mediante el uso no auténtico o la explotación automatizada del servicio, así como la amplificación y la difusión potencialmente rápida y amplia de contenidos ilícitos y de información incompatible con sus condiciones.

La Comisión Europea presume así que “Las plataformas en línea de muy gran tamaño están obligadas a establecer medidas de mitigación razonables, proporcionadas y eficaces, adaptadas a los riesgos sistémicos concretos detectados”.

Además, según el Comunicado de Prensa sobre la investigación respecto a Twitter:

> De conformidad con el artículo 16, apartados 5 y 6, las plataformas en línea deben *notificar sin demora indebida la decisión de moderación de contenidos a las personas físicas o entidades,* facilitando información sobre las posibilidades de reparación en relación con tal decisión; las plataformas deben adoptar esas decisiones de manera oportuna, diligente, no arbitraria y objetiva.
>
> De conformidad con el artículo 25, apartado 1, los prestadores de plataformas en línea no deben diseñar, organizar o gestionar sus interfaces en línea de manera que engañen o manipulen a sus usuarios, o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas.
>
> De conformidad con el artículo 39, las plataformas en línea de muy gran tamaño deben compilar y hacer público, a través de una herramienta consultable y fiable, un repositorio que contenga anuncios en sus plataformas, hasta un año después de la presentación del anuncio por última vez, de manera que la información sea exacta y completa.
>
> De conformidad con el artículo 40, apartado 12, las plataformas en línea de muy gran tamaño *deben facilitar a los investigadores un acceso efectivo a los datos de las plataformas.*

Como vemos la argumentación de la Comisión Europea es prolija pero plagaba de conceptos jurídicos indeterminados, y por ende arbitrarios, que no han sido todavía interpretados por el TJUE. En todo caso, he subrayado en negrita frases que acreditan que la Comisión Europea está exigiendo a las plataformas digitales que moderen las opiniones de los usuarios (“*notificar sin demora indebida la decisión de moderación de contenidos a las personas físicas o entidades”),* y que *“deben facilitar a los investigadores un acceso efectivo a los datos de las plataformas”*.

Estamos por tanto ante la imposición de obligaciones genéricas y sin límite (desproporcionadas) para que sujetos privados limiten la libertad de expresión y la libertad de los individuos (sin orden judicial que lo autorice), y además a que den acceso sin límite y sin orden judicial previa a las autoridades europeas sobre datos u opiniones vertidas en las plataformas por los ciudadanos o empresas.

A ello se añade que en los artículos 9 y 10 del Reglamento Europeo 2022/2065 (directamente aplicable y parte de la LESD), no determinan claramente si deben ser las autoridades judiciales o administrativas las que ordenen la suspensión de medios o canales de difusión de contenidos ilícitos o la entrega de información (conversaciones privadas y datos personales de ciudadanos) (énfasis añadido):

> Artículo 9
>
> Órdenes de actuación contra contenidos ilícitos
>
> *1. Cuando reciban una orden de actuación contra uno o varios elementos concretos de contenido ilícito, dictada por las autoridades judiciales o administrativas nacionales pertinentes*, sobre la base del Derecho de la Unión aplicable o del Derecho nacional aplicable en cumplimiento del Derecho de la Unión, los prestadores de servicios intermediarios informarán a la autoridad que haya dictado la orden, o a cualquier otra autoridad especificada en la orden, de cualquier curso dado a la orden sin dilación indebida, especificando si se ha dado curso a la orden y cuándo." [...]
>
> Artículo 10
>
> Órdenes de entrega de información
>
> 1. *Cuando reciban una orden de proporcionar información específica sobre uno o varios destinatarios individuales del servicio, dictada por las autoridades judiciales o administrativas nacionales pertinentes*, sobre la base del Derecho de la Unión aplicable o del Derecho nacional aplicable en cumplimiento del Derecho de la Unión, los prestadores de servicios intermediarios informarán, sin dilación indebida, a la autoridad que haya dictado la orden o a cualquier otra autoridad especificada en la orden, de su recepción, y del curso dado a la orden, especificando si se ha dado curso a la orden y cuándo."

Aunque enigmáticamente se diga en el apartado 6 de ambos artículo 9 y 10 del Reglamento 2022/2065 que "*Las condiciones y los requisitos establecidos en el presente artículo se entenderán sin perjuicio del Derecho procesal penal y civil nacional"*, ello no despeja la duda de si dicho Reglamento está permitiendo que una autoridad administrativa (sin verificación judicial), limite el derecho fundamental a la libertad de expresión de medios o plataformas digitales y de los propios usuarios, lo cual es muy grave, pues ninguna Ley europea puede estar por encima de textos de rango constitucional o fundacional como la Constituciones de los Estados miembros, el TUE, la CEDF, el CEDH y la jurisprudencia que los interpreta.

Estamos por tanto ante un traslado genérico y sin orden judicial a sujetos privados (las grandes plataformas como *Twitter* o *Telegram*) de potestades de intervención de comunicaciones y de restricción de libertades. Ante la negativa de Twitter a inmiscuirse en derechos individuales, la Comisión Europea ha iniciado un procedimiento sancionador contra dicha plataforma digital.

No cabe mayor ejemplo de traslado a sujetos privados de potestades públicas de restricción de derechos fundamentales, cuando esa restricción solo puede venir ordenada por una orden judicial apegada a la Constitución o CDFUE, y siempre que haya una prueba suficiente. No puede la UE establecer obligaciones genéricas a sujetos privados de restricciones sobre derechos individuales, puesto que eso sería

como enmendar la propia libertad de los sujetos privados para interactuar en un Estado democrático de Derecho.

4 Los motivos para la detención en Francia del fundador de Telegram

La detención en agosto de 2024 del fundador de la red Telegram por parte de la policía francesa fue argumentada por el Estado francés con base en razones de prevención de delitos de odio y terrorismo.[9]

Cabe recordar que en marzo de 2024 también un juez español interrumpió temporalmente el funcionamiento de Telegram en España,[10] con base en que cuatro de los principales grupos de comunicación del país (Mediaset, Atresmedia, Movistar y Egeda) denunciaran que la aplicación difundía contenidos generados por ellos y protegidos por derechos de autor sin autorización de los creadores. El juez había pedido a Telegram que enviara cierta información para el caso en julio de 2023 y ordenó el bloqueo de la aplicación después de que la empresa no respondiera. Pero la orden judicial fue revocada por Auto de la Audiencia Nacional de 25 de marzo de 2024,[11] después de que se criticara que era desproporcionada y podía causar perjuicios a millones de usuarios.

Según el citado Auto de la Audiencia Nacional, analizando la LESD:

> Al efecto, ya no solo para evitar aquel "pulso" sino por lo que aquí interesa para poder obtener esa información será cuestión a resolver por el legislador y que sin duda lo hará -por exigencia europea- a tenor de la denominada Ley de Servicios Digitales y Ley de Mercados Digitales, cuyos objetivos principales son : Crear un espacio digital más seguro en el que se protejan los derechos fundamentales de todos los usuarios de servicios digitales y establecer unas condiciones de competencia equitativas para fomentar la innovación, el crecimiento y la competitividad, tanto en el mercado único europeo como a escala mundial. Y así se dice: Por ejemplo, algunas grandes plataformas controlan ecosistemas importantes en la economía

9 Detención efectuada por orden judicial preventiva, con base en la falta de moderadores en Telegram, que permite la utilización de dicha plataforma digital para la realización de actividades criminales. Véase: MATURANA, Jesús. *Pavel Durov, fundador de Telegram, detenido en París por permitir actividades delictivas en la App.* Euronews. Disponible en: <https://es.euronews.com/next/2024/08/25/pavel-durov-fundador-de-telegram-detenido-en-paris-implicaciones-para-la-libertad-en-inter>. Acceso el: 28 ago. 2024.

10 EUROPA PRESS. *Un juez pide a las operadoras suspender Telegram en España.* ElDerecho.com. Disponible en: <https://elderecho.com/un-juez-pide-a-las-operadoras-suspender-telegram-en-espana>. Acceso el: 28 ago. 2024.

11 PODER JUDICIAL ESPAÑA. Audiencia Nacional Juzgado Central de Instrucción Cinco D. Previas 52/2023. Madrid, 2024. Disponible en: <https://www.newtral.es/wp-content/uploads/2024/03/AUTO-ALZANDO-SUSPENSION-TELEGRAM-25.03.2024.pdf?x95607>.

> digital. Han surgido como guardianes en los mercados digitales, con el poder de actuar como fabricantes de reglas privadas.
>
> Al efecto exige:
> Establecer un punto de contacto para autoridades y usuarios, denunciar delitos penales tener términos y condiciones fáciles de usar, ser transparente en lo que respecta a la publicidad, los sistemas de recomendación o las decisiones de moderación de contenidos. También deben seguir las reglas que se centran únicamente en los VLOP y VLOSE debido a su tamaño y el impacto potencial que pueden tener en la sociedad. Esto significa que deben identificar, analizar y evaluar los riesgos sistémicos vinculados a sus servicios. Deberían prestar atención, en particular, a los riesgos relacionados con contenido ilegal, derechos fundamentales, como la libertad de expresión, la libertad y el pluralismo de los medios de comunicación, la discriminación, la protección del consumidor y los derechos del niño. seguridad pública y procesos electorales, violencia de género, salud pública, protección de menores y bienestar físico y mental, etc.
> Por tanto, Telegram, como el resto de las grandes plataformas, tendrán obligatoriamente que responder por el punto de contacto en Europa para, como en el presente caso, requerirle la información precisa.

Como analizamos en apartado anterior, Telegram podría ser caracterizada, con base en la LESD, como guardiana de los mercados digitales, y por ende, tal y como ha realizado la Comisión Europea en el procedimiento contra Twitter, imponérsela obligaciones perpetuas de moderación de contenidos y suministro de información sobre conversaciones privadas de ciudadanos y personas jurídicas.

5 Interpretación del derecho a la libertad de expresión dada por el TC español y por el TEDH y el TJUE al CEDH y a la CDFUE

Aunque ya hemos demostrado que el proceso administrativo iniciado por la Comisión Europea contra Twitter parte de aplicar la LESD concibiendo a las grandes plataformas como sujetos obligados a restringir la libertad de expresión y suministrar sin límite datos de los usuarios, es preciso analizar los textos de rango constitucional vigentes en Europa y la jurisprudencia que los interpreta, para sostener así que no puede una LESD ser interpretada, sin orden judicial motivada, para subvertir derechos individuales que anteceden a la creación del poder político.[12]

[12] Derechos inalienables como ya sostuvieran Francisco de Vitoria en su "De potestate civilii" (1528), Juan de Mariana en "De rege et regis institutione" (1599) o; o Francisco Suárez (1548-1617) en sus obras Defensio Fidei («Defensa de la fe»), en De legibus («Sobre las leyes»), enDe Bello(«Sobre la guerra»), o John Locke en su Segundo Tratado Sobre el Gobierno Civil (1690), o Hamilton en el número 78 de El Federalista (1790), lo que ya se estipula en la Constitución de EE.UU. (1787).

Toda esa limitación basada en razones de orden público, cuya prueba es meramente indiciaria, no podemos admitirla en un Estado democrático de Derecho, teniendo en cuenta la desproporcionalidad que conlleva al exigir a sujetos privados una permanente moderación de contenidos (censura) y acceso de datos sobre conversaciones privados a autoridades públicas. Siguiendo a Fernández Segado,[13] en cuanto a los requisitos que la jurisprudencia del TEDH exige para limitar la libertad de expresión, no cabe que la Comisión Europea o un Estado aludan a potenciales amenazas de estados extranjeros para exigir una entrega en masa de información sobre conversaciones privadas o una moderación de contenidos constante de las plataformas digitales.

El artículo 10 de la CEDH determina que (énfasis añadido):

> 1. Todas las personas tienen derecho a la libertad de expresión. *Este derecho deberá incluir la libertad de mantener opiniones y de recibir e impartir información e ideas sin interferencias de la autoridad pública e independientemente de las fronteras*. Este artículo no deberá evitar que los Estados requieran las licencias de empresas de radio, televisión o cine.
>
> 2. El ejercicio de estas libertades, dado que conlleva obligaciones y responsabilidades, podrá estar sujeto a las formalidades, condiciones, restricciones o multas tal y como estén prescritas por la ley y *sean necesarias en una sociedad democrática, en interés de la seguridad nacional, integridad territorial o seguridad pública, para la prevención del desorden o del crimen, para la protección de la salud o de la moral, para la protección de la reputación o de los derechos de otros, para evitar la revelación de información recibida confidencialmente, o para mantener la autoridad e imparcialidad del poder judicial.*"

El artículo 10 de la CEDH caracteriza así a la libertad de expresión como un derecho fundamental que solo puede ser restringido por razones de seguridad nacional, integridad territorial o seguridad pública, así como prevención del crimen.

Por su parte, el artículo 11 de la CEDF configura el derecho a la libertad de expresión de la siguiente manera:

[13] "a) El adjetivo «necesario» implica la existencia de una «necesidad social imperiosa» o «imprevista». b) Esta «necesidad» ha de constatarse en el marco de una sociedad democrática, lo que implica que el artículo 10 ampara no sólo las informaciones o ideas favorables, inofensivas o indiferentes, sino también las que puedan chocar, inquietar u ofender al Estado o a una fracción cualquiera de la población, pues así lo demanda el pluralismo, la tolerancia y el espíritu de apertura, sin los cuales no existe una «sociedad democrática»; será igualmente, de conformidad con este espíritu plural y tolerante y con esta mentalidad abierta, como deberán interpretarse las restricciones a la libertad de expresión". FERNANDEZ SEGADO, Francisco. La libertad de expresión en la doctrina del Tribunal Europeo de Derechos Humanos. *Revista de Estudios Políticos (Nueva Época)*, Madrid. n. 70. octubre-diciembre 1990, p. 123.

> 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.
>
> 2. Se respetan la libertad de los medios de comunicación y su pluralismo

Como la jurisprudencia y doctrina han establecido, y también por ejemplo el art. 20 de la Constitución española,[14] solo mediante orden judicial es posible restringir los derechos fundamentales, de modo que no cabe la censura previa ni por tanto obligaciones de actuación ilimitadas a sujetos privados para moderar o limitar opiniones, sin orden judicial que lo exija.

Además, el TJUE y el TEDH han reconocido que el vertido de opiniones en redes sociales o plataformas digitales es un ejercicio relevante de la libertad de expresión que debe gozar del máximo rango de protección, lo que también se aplica a los medios o plataformas a través de los que se difunden dichas opiniones (Telegram o Twitter por ejemplo), "*considerándose que cualquier restricción a estos medios afecta al derecho a recibir y comunicar información*".[15]

De hecho, la jurisprudencia del TEDH determina que ese derecho fundamental se aplica tanto al particular que recibe o expresa información como al medio en

[14] 1. Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción. b) A la producción y creación literaria, artística, científica y técnica. c) A la libertad de cátedra. d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades. 2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa. 3. La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España. 4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia. 5. Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.

[15] Como resumen de la jurisprudencia cabe citar las palabras del TJUE, que también acoge jurisprudencia del TEDH, en el considerando 46 de la sentencia del asunto C-401/19: "En efecto, según la jurisprudencia del Tribunal Europeo de Derechos Humanos, el artículo 10 del CEDH garantiza la libertad de expresión y de información a toda persona y se refiere no solo al contenido de la información, sino también a los medios a través de los que se difunde, considerándose que cualquier restricción a estos medios afecta al derecho a recibir y comunicar información. Como dicho Tribunal ha declarado, Internet es actualmente uno de los principales medios para el ejercicio por los individuos de su derecho a la libertad de expresión y de información. Los sitios de Internet y en particular las plataformas de intercambio de contenido en línea contribuyen enormemente, merced a su accesibilidad y a su capacidad para conservar y difundir grandes cantidades de datos, a mejorar el acceso del público a los asuntos de actualidad y, de manera general, a facilitar la comunicación de la información y la posibilidad de los individuos de expresarse en Internet constituye una herramienta sin precedentes para el ejercicio de la libertad de expresión (véanse, en este sentido, TEDH, sentencias de 1 de diciembre de 2015, Cengiz y otros c. Turquía, CE:ECHR:2015:1201JUD004822610, §52, y de 23 de junio de 2020, Vladimir Kharitonov c. Rusia, CE:ECHR:2020:0623JUD001079514, §33 y jurisprudencia citada)."

el que se inserta tal información.[16] Y la jurisprudencia del TEDH entiende que la libre expresión de opiniones no permite a Turquía en casos de guerra requisar publicaciones basadas en el orden público, sin una prueba suficiente. Por tanto, la jurisprudencia del TEDH permite utilizar excepciones a la libertad de expresión de forma excepcional y siempre con un criterio (*favor libertatis)* en favor de la libertad de expresión, de suerte que es el poder público, en prueba suficiente realizada por una autoridad independiente (judicial), el que debe probar que hay indicios suficientes. Siempre bajo el principio de proporcionalidad e idoneidad de la restricción, es decir que la medida sea idónea para garantizar derechos individuales y proporcionada (no una obligación de moderación o censura permanente). No es lícito por tanto utilizar potestades genéricas e ilimitadas para exigir a las plataformas una restricción de contenidos[17] o un suministro constante de información sobre conversaciones privadas.

Es verdad que la libertad de expresión a veces puede entrar en colisión con otros derechos fundamentales como el derecho al honor, a la intimidad o a la propia imagen,[18] pero en todo caso solo los tribunales pueden restringir la libertad

---

16 Como resumen Freixes Sanjuan, "el TEDH entiende los soportes técnicos a través de los cuales se difunden los contenidos en forma amplia, como así lo demuestra el hecho de que en el Asunto Müller y otros contra Suiza y otros realice esta reflexión al incluir dentro de la libertad de expresión las «informaciones e ideas de forma artística»; que, en los Asuntos Barthold contra Alemania, Casado Coca contra España , «Marktintern» Verlag GmbH y Klaus Beermann contra Alemania y Jacubowsky contra Dinamarca", incluya la publicidad comercial en el ámbito de la libertad de expresión e información; y que en los Asuntos Groppera Radio y otros contra Suiza, Autronic AG contra Suiza y Informationsverein Lentia y otros contra Austria, , incluyera la denominada libertad de antena en el ámbito de la libertad de expresión." FREIXES SANJUÁN, Teresa. El Tribunal Europeo de Derechos Humanos y las libertades de la comunicación, *Revista de Derecho Comunitario Europeo*, Madrid, n. 15 año 7, mayo-agosto 2003, p. 466.

17 Así resume Costa, J.P. la jurisprudencia del TEDH en relación con las excepciones del art. 10 del CEDH para limitar la libertad de expresión: "el Tribunal se niega a ir demasiado lejos al tener en cuenta los intereses del orden público. Así en 1999 el Tribunal dictó numerosas e importantes sentencias en demandas dirigidas contra Turquía (asuntos Sürek y otros). A través de una jurisprudencia matizada, resultado del conjunto de estas sentencias, el Tribunal considera que, incluso en el contexto de una guerra civil enmascarada como la del sudeste de Turquía, la libertad de expresión debe prevalecer, salvo cuando los artículos, las declaraciones o las obras constituyan una clara incitación a la escalada de la violencia. En el ejercicio de su control de proporcionalidad, el Tribunal tiene en cuenta igualmente la naturaleza y el 'quantum' de las penas impuestas a las personas perseguidas. Estos asuntos han dado lugar a trece sentencias del Tribunal: en once de ellas, ha determinado la violación del artículo 10 por parte de Turquía; mientras que en las otras dos ha estimado la no violación." COSTA, Jean-Paul. La libertad de expresión según la jurisprudencia del Tribunal Europeo de Derechos Humanos de Estrasburgo. *Persona y derecho: revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos*, n. 44, Madrid, 2001, p. 248-249.

18 Como el TC ha analizado en consolidada jurisprudencia, son los tribunales los que siempre deben realizar la ponderación sobre qué derecho fundamental debe prevalecer. Así, existen unas pautas, puestas de relieve en especial por la jurisprudencia, que será necesario tener presentes a la hora de analizar cualquier conflicto entre los derechos del artículo 18.1 y los del artículo 20: a) En ningún caso resultará admisible el insulto o las calificaciones claramente difamatorias (SSTC 204/2001, de 15 de octubre; 20/2002, de 28 de enero; STC 181/2006; STC 9/2007); b) El cargo u ocupación de la persona afectada será un factor a analizar, teniendo en cuenta que los cargos públicos o las personas que por su profesión se ven expuestas al público tendrán que soportar un grado mayor de crítica o de afectación a su intimidad que las personas que no cuenten con esa exposición al público (STC 101/2003, de 2 de junio); c) Las expresiones o informaciones habrán de contrastarse con los usos sociales, de forma tal que, por ejemplo, expresiones en el pasado consideradas injuriosas pueden haber perdido ese carácter o determinadas informaciones que antes pudieran haberse considerado atentatorias del honor o la intimidad ahora resultan inocuas; d) No se desvelarán innecesariamente aspectos de la vida privada o de la intimidad que no

de expresión mediante órdenes judiciales,[19] sin que una LESD ni la Comisión Europea puedan establecer obligaciones genéricas e ilimitadas de moderación de contenidos o de suministro de datos sobre conversaciones privadas que se realizan en plataformas o redes como Twitter o Telegram.

6 Conclusión: solo desde el respeto a los derechos naturales de os individuos podremos mantener la vigencia de la democracia

La constatación de que la Comisión Europea o un Estado miembro como Francia están ejerciendo potestades de investigación y sanción para exigir a plataformas privadas labores de restricción de libertades de forma genérica y sin limitación,

resulten relevantes para la información (STC 185/2002, de 14 de octubre; 127/2003, de 30 de junio). Sin embargo, más allá de estos aspectos de carácter subjetivo el Tribunal Constitucional ha destacado el carácter prevalente o preferente de la libertad de información por su capacidad para formar una opinión pública libre, indisolublemente unida al pluralismo político propio del Estado democrático (STC 21/2000, de 31 de enero; SSTC 9 y 235/2007). No obstante, es necesario tener presente que esa prevalencia no juega de forma automática sino sólo en supuestos en los que no concurran otros factores, como pueda ser la presunción de inocencia (STC 219/1992, de 3 de diciembre), en los que la ponderación lleve a primar intimidad, honor o propia imagen sobre las libertades de expresión o, en particular, de información (STC, por sólo citar una, 158/2003, de 15 de septiembre).

19 Como avizoraba Boix Palop en 2016, esta regulación europea, aunque se vista de excepcionalidad, se va iba a convertir en la regla: *"Se trataría, con todo, se nos dirá, de supuestos excepcionales previstos para la represión de conductas muy concretas y que además están tipificados únicamente para supuestos donde hay riesgo para la seguridad y orden públicos. Sin embargo, ello no parece una razón de peso para quebrar el tradicional reparto sobre los contenidos expresivos, que reprimía estas conductas por medio de la actuación de los jueces y tribunales. Los riesgos para la libertad de expresión y el pluralismo, al operar de este modo, son evidentes y permiten intuir una paulatina extensión futura de estas posibilidades de intervención administrativa sobre los contenidos en las redes sociales apelando a diversos títulos jurídicos que justificarían estas intromisiones.* [...] *obviando el hecho de que Internet es un medio de suyo más libre, plural, abierto... y no sometido a ese control administrativo, lo que probablemente debiera reconducir la fiscalización sobre el mismo a unos controles más en la línea de lo que ha sido la convicción tradicional, con base en el art. 20.5 CE, de que solo una autoridad judicial podía tomar este tipo de decisiones. No debe olvidarse, además, que el art. 20.2 CE establece también la prohibición de la censura previa, de modo que hay quien entiende que, por definición, y de la combinación de ambos artículos, se deduce un importante mandato al legislador en el sentido de no ceder excesivos espacios a la Administración en el control de contenidos expresivos (Betancor Rodríguez, 2007). Esta posible extensión, que permitiría controlar los contenidos audiovisuales que se comparten/difunden por medio de las redes sociales (y no olvidemos que cada vez más los grandes operadores tienen perfiles en las redes desde donde promocionan y enlazan sus productos y aspiran a captar audiencia) nos situaría ya de lleno en una quiebra absoluta de los equilibrios tradicionales en punto a quién controla los excesos expresivos, añadiendo a otros entes, además del juez, con capacidad para realizar esta labor. Se trata de una posibilidad ciertamente peligrosa desde la perspectiva proliberal que este trabajo viene defendiendo y que colocaría al Estado en una posición muy ventajosa en sus intentos de disciplinar la expresión de los ciudadanos en las redes (Boix Palop, 2011c: 218-222; Teruel Lozano, 2014). La conclusión, en definitiva, al menos en este punto, no puede ser sino clara y particularmente inquietante. Con diversas razones de tipo técnico (que no viene al caso ahora discutir o cuestionar, por razones de espacio y de orientación de este trabajo) podemos constatar ya a estas alturas la aparición y consolidación respecto de las formas de comunicación en Internet de mecanismos e instancias de control antes inexistentes respecto de contenidos o informaciones que, cuando lo son en otros formatos, nadie tenía (ni tiene) dudas de que solo podían ser cuestionadas, en su caso, por la autoridad judicial"*. BOIX PALOP, Andrés. La construcción de los límites a la libertad de expresión en las redes sociales. *Revista de Estudios Políticos*, n. 173, julio-septiembre 2016, p. 55-112.

plasma un quiebre en el clásico esquema de los derechos fundamentales de libertad que solo podían estar restringidos por el poder judicial y en casos concretos.

En la práctica supone que la Comisión Europea y otros Estados europeos entienden que el Estado está por encima de los derechos individuales,[20] utilizando simplemente razones de prevención genéricas. Sin embargo, anteponer el poder público a los derechos individuales es un error. La democracia liberal se basa en una idea moral, que el individuo nace con unos derechos individuales naturales, y que por ende cualquier ente público solo puede tener sentido si respeta esos derechos (básicamente, libertad, vida y propiedad).[21]

Como hemos analizado, los textos constitucionales, empezando por la Constitución de EE.UU. de 1787 (Primera Enmienda), el artículo 20 de la Constitución española, el artículo 10 de la CEDH o el artículo 11 de la CEDF, garantizan la libertad de expresión, además de la libertad como valor fundamental del orden democrático. Por eso la jurisprudencia, tanto del TC español, como del TEDH o del TJUE, no permite la intervención de publicaciones o la limitación de la libertad de expresión de forma genérica sin orden judicial previa que acredite la idoneidad y proporcionalidad de la medida.

Las actuaciones de la Comisión Europea para exigir una limitación genérica e indefinida de las expresiones vertidas por ciudadanos en plataformas digitales

---

20 Ejemplo de esta peligrosa de alimentar el leviatán estatal es el artículo de Vázquez, Víctor, "¿Qué hacer frente al discurso abyecto?", El Mundo, 25 de agosto de 2024. Según este profesor: "Frente a cualquier problema relacionado con el discurso en la red, se puede apelar sin más, bien por ortodoxia liberal, bien por pereza intelectual, a los presupuestos optimistas del liberalismo clásico. Es decir, optar por el simple alegato a favor de la libertad de expresión, asumiendo que cualquier discurso u ofensa fracasará si se combate con mejores argumentos. No creo que sea tan fácil. Desde luego, no sabemos si Stuart Mill o el juez Holmes sostendrían exactamente los mismos postulados sobre la libertad de expresión y el mercado de las ideas a la luz de tecnología actual y de la propia sociología de las redes sociales, o si asumirían, como hace el legislador europeo, que el discurso en la red requiere de una regulación jurídica singular frente a ciertos riesgos. [...] No nos movemos aquí en la complejidad de definir qué es desinformación, riesgo sistémico, ni tampoco resulta necesario hacer conjeturas sobre cuán contagiosa es la animadversión que transmiten ciertos mensajes. Se trata de actuar con herramientas penales básicas para la defensa de la integridad física y moral, el honor o la vida. Todo esto sin olvidar, claro, que el derecho no puede sustituir nuestra responsabilidad cívica de hacer frente a lo abyecto."

21 Como explicaba el Presidente de Argentina Javier Milei, en una conferencia en Madrid al recibir el Premio Juan de Mariana el 21 de junio de 2024: "Pero no es solamente la cuestión de la economía. Nosotros interpretamos la economía desde una cuestión moral. El diseño de la política económica tiene que ver con una cuestión fundamentalmente moral, es decir, cuáles son los valores que están detrás de eso. Y claramente, frente a eso, nada puede contra el liberalismo. El liberalismo Por eso, recurrentemente, en nuestros actos de campaña cerrábamos con la definición de liberalismo de Alberto Benegas Lynch (hijo), con algunas mutaciones que yo le hice: el liberalismo es el respeto irrestricto del proyecto de vida del prójimo, basado en el principio de no agresión y en la defensa del derecho a la vida, a la libertad y a la propiedad. Sus instituciones son la propiedad privada, los mercados libres de intervención estatal, la libre competencia (pero en el sentido austríaco, no en el sentido neoclásico), la división del trabajo, la cooperación social, y donde solamente se puede ser exitoso sirviendo al prójimo con bienes de mejor calidad y de mejor precio. En ese sentido, eso es un marco rector, y nosotros como objetivo tenemos que hacer que Argentina vuelva a ser grande nuevamente. La única forma de lograr eso es que Argentina vuelva a ser libre nuevamente. Y eso es lo que marca el norte." Disponible en: <https://juandemariana.org/ijm-actualidad/analisis-diario/discurso-de-recepcion-del-premio-juan-de-mariana-de-javier-milei/>.

(la denominada "moderación de contenidos), así como la remisión ilimitada de datos sobre conversaciones privadas de ciudadanos a la Comisión Europea y otras autoridades públicas, está socavando esas libertades fundamentales que anteceden al poder político. Las autoridades europeas, esgrimiendo motivos indeterminados de orden público, y sin órdenes judiciales previas, se estarían situando por encima de la CEDF y de los valores supremos de la UE del art. 2 del TUE. No cabe que ninguna LESD sea coartada para que las autoridades europeas vulneren derechos fundamentales consagrados en el TUE y en la CEDF, así como en las Constituciones nacionales de los Estados miembros.

Estamos por tanto ante la batalla de nuestro tiempo: exigir el respeto a los derechos individuales de los individuos y a la separación de poderes que permita a los jueces ser el único poder capaz de restringirlos bajos sólidas razones y siempre que esté justificado por fines constitucionales y de manera proporcionada. Estas actuaciones de la Comisión Europea o de otros Estados miembros[22] atestiguan que el momento de la batalla por la democracia y los derechos individuales ya está aquí.

Referencias bibliográficas

BOIX PALOP, Andrés. La construcción de los límites a la libertad de expresión en las redes sociales. *Revista de Estudios Políticos*, Madrid, n. 173, julio-septiembre 2016, p. 55-112

COMISIÓN EUROPEA. *La Comisión Europea envía una solicitud de información a Meta en virtud de la Ley de Servicios Digitales.* Comunicado de Prensa. Disponible en: <https://digital-strategy.ec.europa.eu/es/news/commission-sends-request-information-meta-under-digital-services-act-2>. Acceso el: 28 ago. 2024.

COMISIÓN EUROPEA. *La Comisión incoa un procedimiento formal contra X en virtud de la Ley de Servicios Digitales.* Comunicado de Prensa. Disponible en: <https://ec.europa.eu/commission/presscorner/detail/es/ip_23_6709>. Acceso el: 28 ago. 2024.

COSTA, Jean-Paul. La libertad de expresión según la jurisprudencia del Tribunal Europeo de Derechos Humanos de Estrasburgo. *Persona y derecho: revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos*, n. 44, Madrid, 2001.

FERNANDEZ SEGADO, Francisco. La libertad de expresión en la doctrina del Tribunal Europeo de Derechos Humanos. *Revista de Estudios Políticos (Nueva Época)*, Madrid. n. 70. octubre-diciembre 1990, p. 93-124.

FREIXES SANJUÁN, Teresa. El Tribunal Europeo de Derechos Humanos y las libertades de la comunicación, *Revista de Derecho Comunitario Europeo*, Madrid, n. 15 año 7, mayo-agosto 2003, p. 463-497.

[22] Como la Ley Orgánica 1/2024 de Amnistía en España, por la que el Parlamento española anula centenares de sentencias y actuaciones judiciales al declarar no perseguible cualquier actuación que persiga la independencia de Cataluña, anulando la separación de poderes. O la reforma del art. 49 de la Constitución española sobre discapacidad, que establece una desigualdad de trato en favor de mujeres discapacitadas frente a los hombres discapacitados, reforma publicada en el Boletín Oficial del Estado, núm. 43, de 17 de febrero de 2024, páginas 19462 a 19471 (10 págs.)

OPORTO, Pablo Font. El núcleo de la doctrina de Francisco Suárez sobre la resistencia y el tiranicidio. *Pensamiento Revista de Investigación e Información Filosófica*, Madrid, v. 69 n. 60, septiembre-diciembre, 2013, p. 493–521.

VALIENTE MARTÍNEZ, Francisco. La libertad de expresión y las redes sociales: de la doctrina de los puertos seguros a la moderación de contenidos. Derechos y libertades: Revista de Filosofía del Derecho y derechos humanos, n. 48, 2023.

VÁZQUEZ, Víctor J. ¿Qué hacer frente al discurso abyecto?, *El Mundo*. Disponible en: <https://www.elmundo.es/espana/2024/08/25/66ca0b8921efa0a3298b45b4.html>.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

PERNAS ALONSO, José María. La libertad de expresión en plataformas digitales amenazada en la UE: los casos Twitter y Telegram. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 61-78, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.alonso.

Informações adicionais

Additional information

INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 05 · n. 02 · maio/agosto 2024 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.5.n.2

05

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

International Journal of Digital Law – IJDL
ISSN 2675-7087
DOI: 10.47975/digital.law.vol.5.n.2.leal

Segurança pública e inteligência artificial: novos paradigmas

Public security and artificial intelligence: new paradigms

Rogerio Gesta Leal*
Universidade de Santa Cruz do Sul (Santa Cruz do Sul, Rio Grande do Sul, Brasil)
rleal@unisc.br
https://orcid.org/0000-0003-1372-6348

Recebido em/Received: 31.08.2024 / August 31st, 2024
Aprovado em/Approved: 28.09.2024 / September 28th, 2024

Resumo: O objeto de estudo do presente trabalho é enfrentar a problemática das condições e possibilidades de políticas públicas de segurança com o uso de inteligência artificial e tecnologias de informação, levando em conta direitos e garantias fundamentais individuais e sociais demarcadas pelo Estado democrático de direito, nomeadamente no Brasil. A hipótese e proposta de enfrentamento destas questões se dá a partir do estabelecimento de marcos normativos claros e políticas de garantias por parte do Estado, a partir do que tais políticas podem se instituir e desenvolver, com permanente controle interno e externo, notadamente social.

Palavras-chave: Segurança pública; políticas públicas; direitos fundamentais; Estado de direito; controle de políticas públicas.

Abstract: The object of study of this work is to confront the problem of the conditions and possibilities of public security policies with the use of artificial intelligence and information technologies, taking into account fundamental individual and social rights and guarantees demarcated by the Democratic Rule of Law, namely in Brazil. The hypothesis and proposal for tackling these issues is based on the establishment of clear normative frameworks and guarantee policies by the State, from which such policies can be instituted and developed, with permanent internal and external control, notably social.

Como citar esse artigo/*How to cite this article*: LEAL, Rogério Gesta. Segurança pública e inteligência artificial – Novos paradigmas. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 81-99, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.leal.

* Professor Titular da Universidade de Santa Cruz do Sul (Santa Cruz do Sul-RS, Brasil) e da Fundação Superior do Ministério Público do Rio Grande do Sul – FMP (Porto Alegre-RS, Brasil), nos cursos de Mestrado e Doutorado em Direito. Doutor em Direito pela Universidade Federal de Santa Catarina – UFSC e pela Universidad Nacional de Buenos Aires. Mestre em Desenvolvimento Regional da Universidade de Santa Cruz – USC. Graduado em Direito pela Universidade de Santa Cruz do Sul. Desembargador do Tribunal de Justiça do Estado do Rio Grande do Sul. *E-mail*: rleal@unisc.br.

Keywords: Public security; Public policies; Fundamental rights; Rule of law; Control of public policies.

1 Notas introdutórias

É inegável que, em todas as áreas da vida, a inteligência artificial (IA) tem se mostrado cada vez mais presente e com mais funcionalidades, que facilitam nas tarefas do cotidiano.[1] Por apresentar sofisticação e otimização tecnológica, pode facilmente ser percebida como ferramenta que é destituída de erros, não apresentando preconceitos e estereótipos, características comumente atreladas ao ser humano. Todavia, se vivemos numa sociedade na qual tudo que (re)produzimos é atravessado por fatores históricos, de natureza cultural e social, por que as IAs – criadas pelo homem – também não replicariam estigmas relacionados à classe, raça, gênero, etnias, dentre outros?[2]

A *algoritmização da vida*,[3] que está presente nas redes sociais e *streamings*, e tem ganhado espaço em inúmeros campos, tem influenciado cada vez mais políticas de segurança pública. A despeito disto, problemas de discriminação e preconceito estrutural em determinadas políticas desta natureza continuam os mesmos, e o uso discriminatório e preconceituoso da IA não pode tirar a responsabilidade do Estado no ponto (porque, se houve erro, foi culpa do algoritmo, e não de quem programou).[4]

É interessante perceber esse paralelo: por um lado, a tecnologia é colocada como solução, mas ao mesmo tempo a sociedade civil em diferentes momentos vai contestar isso.

---

1 Um exemplo claro é o uso da inteligência artificial na tomada de decisões judiciais e administrativas: VALLE, Vivian Lima López; FUENTES I GASÓ, Josep Ramón; AJUS, Attílio Martins. Decisão judicial assistida por inteligência artificial e o Sistema Victor do Supremo Tribunal Federal. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 2, e252, maio/ago. 2023. DOI: 10.5380/rinc.v10i2.92598; BITENCOURT, Caroline Müller; MARTINS, Luisa Helena Nicknig. A inteligência artificial nos órgãos constitucionais de controle de contas da administração pública brasileira. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 3, e253, set./dez. 2023. DOI: 10.5380/rinc.v10i3.93650; TOLEDO, Claudia; PESSOA, Daniel. O uso de inteligência artificial na tomada de decisão judicial. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 1, e237, jan./abr. 2023. DOI: 10.5380/rinc.v10i1.86319; SIERRA CADENA, Grenfieth de Jesus. Implementación de la Inteligencia Artificial en las Altas Cortes de Colombia: los casos de la Corte Constitucional y el Consejo de Estado. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 11, n. 1, e253, ene./jul. 2024. DOI 10.14409/redoeda.v11i1.13824.

2 SÁNCHEZ DÍAZ, María Fernanda. El impacto de la inteligencia artificial generativa en los derechos humanos. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 11, n. 1, e252, ene./jun. 2024. DOI: 10.14409/redoeda.v11i1.13612.

3 PUSCHEL, André Felipe Silva; RODRIGUES, Roberto Tessis; VALLE, Vivian Cristina Lima López. O dilema ético da decisão algorítmica na administração pública. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 90, p. 207-226, out./dez. 2022. DOI: 10.21056/aec.v22i90.1737.

4 RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. Personal data protection and State surveillance: the risks of digital discrimination and the Federal Supreme Court's vision. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 90, p. 63-85, out./dez. 2022. DOI: 10.21056/aec.v22i90.1658.

São estes cenários e seus riscos, assim como iniciativas para controlá-los, que este trabalho pretende abordar. Para tanto, elegemos como objetivos específicos: (i) demarcar as relações entre sociedade do conhecimento e sociedade da vigilância; (ii) as reações institucionais e políticas à sociedade de vigilância; (iii) propor premissas viabilizadoras de políticas de segurança pública democráticas para o uso de novas tecnologias com o uso de IA no âmbito da segurança pública.

Pretendemos utilizar neste trabalho o método dedutivo, testando nossas hipóteses com os fundamentos que passam a ser declinados. Utilizaremos, para tanto, técnica de pesquisa com documentação indireta, nomeadamente bibliográfica.

2 Sociedade do conhecimento x sociedade da vigilância

O termo "sociedade da informação" foi incorporado nos últimos anos no discurso político, acadêmico e midiático global. Manuel Castells afirma que esta sociedade é um novo sistema tecnológico, econômico e social; uma economia na qual o incremento de produtividade não depende do incremento quantitativo dos fatores de produção (capital, trabalho, recursos naturais), mas de aplicação de conhecimentos e informação na gestão, produção e distribuição, tanto nos processos como nos produtos.[5]

Estas sociedades se caracterizam por serem baseadas no conhecimento e nos esforços para converter informação em conhecimento. Quanto maior a quantidade de informação gerada por uma sociedade, maior será a necessidade de convertê-la em conhecimento.

Um aspecto de singular relevância no desenvolvimento das "sociedades da informação e do conhecimento", pois, é a *velocidade* com que a informação é gerada, transmitida e processada. Hoje, a informação pode ser obtida de forma praticamente instantânea e, muitas vezes, da mesma fonte que a produz, transcendendo fronteiras e limitações de espaço e tempo.

Embora existam várias interpretações sobre a amplitude e o significado do conceito desta sociedade, o certo é que nela são reconfiguradas as formas como todas as pessoas realizam a maior parte das suas atividades, a partir de novas formas de empreender e realizar ações quotidianas; portanto, podemos afirmar que ela é também síntese de mudanças de paradigmas estruturais em múltiplos campos da vida.[6]

---

5 CASTELS, Manuel. *La sociedad en red* – La era de la información. Economía, sociedad y cultura. Madrid: Alianza Editorial, 1997. v. 1. p. 67.

6 Tratamos de forma mais aprofundada disto no livro LEAL, Rogerio Gesta. *Segurança pública no Estado democrático de direito* – Avanços e recuos. São Paulo: Tirant lo Blanch, 2023.

Alvin Toffler, no início da década de 1980, antecipou com singular clareza o advento da sociedade da informação, lembrando que, há mais de 10 mil anos, a primeira onda introduziu mudanças importantes na história, impulsionada pela revolução agrícola, transformando as condições de vida dos primitivos caçadores e coletores, que formaram sociedades camponesas nas quais a produtividade dependia principalmente da demonstração de força humana e animal, bem como do sol, vento e água. Os beneficiários desta transformação foram aqueles que entenderam que a nova organização estaria focada no campo.[7]

Com a segunda onda, a revolução industrial desencadeou mudanças profundas na história,[8] dando origem a uma nova civilização centrada na indústria e na produção em grande escala. A produtividade dependia da relação que o homem estabelecia com as máquinas. Aqueles que não compreenderam o significado e o alcance da racionalidade imposta pela nova ordem ficaram para trás, significativamente limitados nas suas capacidades de produção.

A terceira onda introduz, por sua vez, uma nova sociedade, que se assenta na informação, no conhecimento e na criatividade. Nestas sociedades, a produtividade depende do desenvolvimento de novas tecnologias, que – afirma Toffler – permitiriam ao homem fazer menos e pensar mais. Ou seja, o desenvolvimento de tecnologias avançadas de informação e comunicação permite a configuração de novo espaço social, como um terceiro ambiente, marcado por inéditos modelos de mercados, culturas e percepções do mundo.[9]

Imaginava-se que, neste novo mundo de possibilidades infinitas de conhecimento/ilustração, a racionalidade humana chegaria a um nível de excelência que seria capaz de desenvolver a vida e relações humanas de forma mais civilizada e sustentavelmente, com harmonia, justiça social e *segurança.* Ledo engano!

Um inédito *marco paradigmático de colapso* desta sociedade do conhecimento/informação: os ataques terroristas do 11.9.2001 das torres gêmeas, de New York (EUA), inauguraram o que podemos chamar de quarta onda civilizatória: a Era Panóptica da Sociedade da Vigilância.

Quando imaginávamos que as novas tecnologias geradas pela sociedade da informação poderiam nos assegurar a prevenção de problemas das mais diversas ordens, estas têm se revelado impotentes diante de contínuas situações de emergências, riscos e perigos que vão se criando hodiernamente em todo o globo,

---

7 TOFFLER, Alvim. *La tercera ola*. México: Edivisión, 1981. p. 81.

8 MARTNEZ GARBIRAS, María Margarita; SÁNCHEZ-HUERTAS, Luis Fernando. Los atajos de la Cuarta Revolución Industrial a la democracia: una reflexión de lecciones aprendidas en clave de Lafont y Berlin. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 23, n. 94, p. 43-62, out./dez. 2023. DOI: 10.21056/aec.v23i94.1725.

9 Neste sentido DAVARRA RODRIGUEZ, Miguel Angel. *De las autopistas de la información a la sociedad virtual*. Madri: Aranzadi Editorial, 2008. p. 51 e seguintes.

provocadas por atos terroristas e de violência imensos, bem como por fatores ambientais, de consumo, energéticos, raciais, étnicos, biológicos, de criminalidades, dentre outros, atestando ser ilusória a crença de que, por meio do conhecimento e das inovações tecnológicas, nos libertaríamos de quaisquer medos, deixaríamos de ser criaturas e passaríamos a ser criadores da comunidade em que vivemos.[10]

Em outras palavras, medos e incertezas, como nos indica Mongardini, continuam a ser traços cada vez mais característicos de nossos quotidianos,[11] e bastou um vírus microscópico, gerador da Covid-19,[12] para voltarmos a nos encontrar sozinhos e desesperados! De repente regressamos ao tempo da terrível gripe espanhola,[13] com as mesmas máscaras, com os mesmos medos, mas sobretudo com os mesmos erros, como exemplo, o de não revelar à sociedade a propagação da doença em tempo certo; ou, pior ainda, o de comunicar notícias manipuladas e muitas vezes até falsas,[14] nomeadamente por redes sociais virtuais, justamente aquelas que poderiam em muito auxiliar os cenários trágicos que passamos.

---

10 Ver o excelente texto de Ver o excelente texto de HARARI, Yuval Noah. *Homo Deus*. Uma breve história do amanhã. São Paulo: Companhia das Letras, 2016. Ver igualmente o texto de DOMINICI, Piero. *La società dell'irresponsabilità*. Milano: Franco Angeli, 2015. p. 28 e seguintes.

11 MONGARDINI, Carlo. *Le dimensioni sociali della paura*. Milano: Franco Angeli, 2010. p. 46. Na mesma linha o excelente texto de ZOLO, Danilo. *Sula paura* – Fragilità, aggressività, potere. Milano: Feltrinelli Editore, 2011. p. 49 e seguintes. Neste texto o autor se pergunta: "perché così spesso la paura mi rendeva aggressivo e perché l'aggressività mia e la prepotenza degli altri erano strettamente intrecciate. Mi domandavo, in sostanza, qual era il rapporto fra la paura, l'aggressività e la violenza scatenata dai miei simili nel corso dei millenni" (p. 11). É importante debater esses temas, pois, muitas vezes, como cita o autor, lembrando de Arnold Gehlen: "Con grande abilità abbiamo sospinto la morte al di fuori del nostro campo visivo. La morte gioca dietro porte laccate di bianco".

12 Sobre os impactos jurídicos da Covid-19 nos direitos humanos e no direito administrativo, ver: CASTILLO ARJONA, Mónica. El fenómeno de la Covid-19 y sus efectos sociales en el derecho administrativo del siglo XXI. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 173-187, ene./jun. 2021. DOI: 10.14409/redoeda.v8i1.9548; SÁNCHEZ DIAZ, Maria Fernanda; ROMERO TELLO, Ana Guadalupe. Covid-19, Derechos Humanos y Estado frente al manejo de la Pandemia. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 233-254, ene. /jun. 2021. DOI 10.14409/redoeda.v8i1.9525; HERNANDES, Luiz Eduardo Camargo Outeiro; PIOVESAN, Flávia. Desafios judiciais em tempos de pandemia: fortalecendo o diálogo entre a Comissão Interamericana de Direitos Humanos e o Supremo Tribunal Brasileiro para a proteção dos direitos humanos. *Revista de Investigações Constitucionais*, Curitiba, v. 9, n. 2, p. 371-388, maio/ago. 2022. DOI: 10.5380/rinc.v9i2.86138; NÓBREGA, Marcos; HEINEN, Juliano. As forças que mudarão a Administração Pública pós-Covid: transparência 2.0, blockchain e smart contracts. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 21, n. 85, p. 217-230, jul./set. 2021. DOI: 10.21056/aec.v21i85.1405; RODRÍGUEZ-ARANA MUÑOZ, Jaime. Administrative Law and human dignity (on the post-pandemic reconstruction of Administrative Law). *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 88, p. 11-33, abr./jun. 2022. DOI: 10.21056/ aec.v22i88.1646; BOMTEMPO, Eugênio Morais; CARMONA, Paulo Cavichioli. A solidariedade social na pandemia de Covid-19. A*&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 89, p. 251-276, jul./set. 2022. DOI: 10.21056/aec.v22i89.1662.

13 A *gripe espanhola* foi causada por um vírus influenza que se espalhou pelo mundo entre 1918 e 1919, não se sabendo ao certo de onde partiu, tendo causado a morte de cerca de 50 milhões de pessoas, sendo que algumas estatísticas falem em até 100 milhões de mortos, conforme dados coletados no *site*: https://www.historiadomundo.com.br/idade-contemporanea/gripe-espanhola.htm. Acesso em: 22 mar. 2023.

14 VALLE, Vivian Cristina Lima López; RUIZ, Maria Guadalupe Fernandes; BÜTTNER, Marcielly. Fake news, influência na formação da opinião pública e impactos sobre a legitimidade da decisão pública. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 95, p. 73-97, jan./mar. 2024. DOI: 10.21056/aec.v24i95.1898.

Estes fatos têm nos demonstrado como a construção social dos riscos e perigos que nos cercam (entendidos como atributos socialmente construídos) tem fornecido bases teóricas e empíricas sólidas para o desenho de políticas muitas vezes autoritárias (inclusive de segurança pública). Daí porque autores como Ferrajoli insistem na tese de que o neoconstitucionalismo, para estar à altura destes novos desafios, deve construir garantias capazes de criar alternativas racionais e credíveis às previsões de um futuro caracterizado pela incerteza, violência, desigualdade e devastação ambiental.[15]

Mesmo que as Constituições contemporâneas tenham se ocupado de criar instrumentos de gestão de crises, é preciso permanentemente refletir sobre possível paradoxo de regimes democráticos que conseguem se autodestruir usando processos e procedimentos (por eles criados) de forma antidemocrática. Como nos dizem D'Agostini e Ferrera, em tempos de crise é fácil superestimar a necessidade de segurança e subestimar o valor da liberdade; e isto porque, sem segurança, não há liberdade.[16] Mas também é verdade que a história constitucional hodierna nos mostra claramente como a ruptura da proteção dos direitos e liberdades em nome da defesa da segurança está presente desde há muito.[17]

Por isto podemos dizer que a segurança, enquanto bem constitucional multifacetado e polissêmico, pode se dar em sentido material e ideal; objetivo e subjetivo; individual e coletivo; interno e externo, submetendo-se cada vez mais, e de forma ordinária, a juízos de ponderação com outros interesses de importância constitucional, mesmo além de ambientes de emergência tradicionais. Como nos diz Walzer, sem segurança nenhuma forma de representação política baseada no consenso é possível; e a liberdade, aqui, figura como aquela tranquilidade de espírito decorrente da convicção de se estar seguro.[18]

Por todas estas razões, a prevenção e a precaução tornaram-se, nos dias atuais, as *règles de droit*[19] por excelência, o mantra de todas políticas públicas

---

15 FERRAJOLI, Luigi. *La democrazia attraverso i diritti*. Roma: Laterza, 2013. p. 27.

16 D'AGOSTINI, Franca; FERRERA, Maurizio. *Le verità del potere* – Sei diritto aleatici. Roma: Einaudi, 2019. p. 81. Em verdade, a história já nos ensinou que por trás do aparente império da lei há sempre homens que governam e legislam, razão pela qual toda a norma jurídica está destinada a formalizar vontades/desejos e escolhas de poder.

17 No ponto ver o excelente texto de COLE, David. *Enemy Aliens* – double standards and constitutional freedoms in the war on terrorism. New York: The New Press, 2003. p. 77. No mesmo sentido o livro de CERI, Paolo. *La società vulnerabile* – Quale sicurezza, quale libertà. Roma/Bari: Laterza, 2003. p. 38 e seguintes.

18 WALZER, Michael. *La libertà e i suoi nemici nell'età della guerra al terrorismo*. Roma/Bari: Laterza, 2010. p. 43.

19 Como quer VERHOEVEN, Charles Leben. *Le principe de précaution* – Aspects de droit international et communautaire. Paris: Éditons Panthéon-Assas, 2022. p. 41. Lembra-nos o autor que o princípio da precaução intervém quando convém adotar as medidas adequadas, mesmo face a riscos não totalmente apurados cientificamente, diferindo-se, pois, do princípio da prevenção, que, no entanto, opera quando a informação científica sobre o perigo e a nocividade são certos, concordantes e conclusivos.

preocupadas em minimizar riscos, perigos e medos capazes de prevalecer sobre outros direitos, e conformar a ação da administração pública como um todo. E em nome de tudo isto foram se criando políticas públicas globais – físicas e virtuais – de segurança máxima contra riscos e perigos conhecidos e desconhecidos, mesmo que em detrimento de alguns direitos e garantias fundamentais individuais a duras penas conquistados, como privacidade e intimidade.

Lembremos que foi sob o pretexto de sua cruzada contra o terrorismo internacional que o governo do Presidente Bush promoveu, pós-11.9.2001, iniciativas legislativas que impuseram restrições significativas à liberdade de expressão e aos direitos relacionados com a privacidade pessoal, dentre as quais: Estatuto de Escuta Telefônica, Lei de Privacidade de Comunicações Eletrônicas, Lei de Fraude e Abuso de Computadores, Lei de Vigilância de Inteligência Estrangeira, Lei de Direitos e Privacidade de Educação Familiar, Lei de Lavagem de Dinheiro, Lei de Imigração e Nacionalidade, Lei de Sigilo Bancário, Lei de Direito à Privacidade Financeira, Lei Patriótica dos EUA, e Lei Antiterrorismo de 2001.[20]

Para exercer funções panópticas eficazes sobre a informações que circulam pela internet, o governo do Presidente Bush promoveu a adaptação do quadro regulamentar referido, nomeadamente por meio do *USA Patriotic Act*, concedendo amplos poderes às áreas de segurança do governo para fiscalizar as informações que circulam na internet, autorizando a interceptar todas as comunicações que considerassem "suspeitas".[21] Ao lado destas, criou também o programa CAPPS II (*Computer Assisted Passenger Pre-Screening*), pré-inspeção assistida por computador de passageiros.[22] Este sistema provém das informações que as companhias aéreas armazenam no registo dos passageiros, e inclui dados relativos às viagens realizadas, bem como possíveis antecedentes criminais e informações não especificadas.

Por outro lado, instrumentos de IA e novas tecnologias de acesso, coleta e gestão da informação podem ser, ao mesmo tempo, viabilizadores de espaços democráticos; mas também autoritário, basta vermos os regimes no Irã e da China, usando-as para suprimir a liberdade de expressão, aprimorar técnicas de vigilância, disseminar propaganda de ponta e pacificar suas populações com entretenimento

---

20 "Wiretap Statute, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Foreign Intelligence Surveillance Act, Family Education Rights and Privacy Act, Money Laundering Act, Immigration and Nationality Act, Bank Secrecy Act, Right to Financial Privacy Act, USA Patriotic Act, Anti-Terrorism Act 2001" – conforme informações do *site*: https://epic.org/privacy/terrorism/usapatriot/. Acesso em: 27 abr. 2024.

21 Já sabemos hoje que a internet pode, de fato, ser utilizada como meio capaz de desempenhar funções úteis de vigilância e controle individual e social, o que representa bem novo ciclo do panoptismo foucaultiano, conforme sua obra FOUCAULT, Michel. *Vigilar y castigar*. Nacimiento de la prisión. México: Siglo XXI, 1983. p. 43 e seguintes.

22 O sistema CAPPS está em funcionamento desde 1998 e provém dos ataques terroristas ocorridos durante os Jogos Olímpicos de Atlanta, em 1996, bem como do trágico desfecho do voo 800, da TWA, que em consequência de uma *avaria mecânica* colidiu com o Oceano Pacífico. Mais dados podem ser obtidos no *site*: https://www.gao.gov/products/gao-04-385. Acesso em: 27 abr. 2024.

digital alienante.[23] Para além disto, tem se formado um *capitalismo da vigilância*[24] a partir da IA e das redes sociais, com a instalação de grandes monopólios econômicos caracterizadores do que se tem chamado de *feudalismo tecnológico*,[25] o que se percebe em corporações como Facebook, Google, Amazon, Apple, Microsoft, Netflix, governantes autocráticos e sem controle de cidadãos que ocuparam um espaço que se pensava ser coletivo.[26]

Por conta disto é que a Lei dos Mercados Digitais, recentemente aprovada pela Europa, estabelece um conjunto de critérios objetivos claramente definidos para qualificar grandes plataformas *on-line* como *gatekeepers*,[27] visando garantir que elas se comportem de modo a respeitar direitos e garantias individuais e sociais.[28]

A despeito disto, é em nome da segurança pública contra atos de terrorismo e de criminalidade organizada que vários governos têm desenvolvido programas de vigilância de seus cidadãos ao redor do mundo, como nos informa Federico Kukso, ao referir que, na China, bancos, aeroportos, hotéis e até banheiros públicos verificam a identidade das pessoas inspecionando seus rostos, por meio do *software* chamado *Xue Liang* (olhos agudos), que analisa milhões de imagens para rastrear pessoas, detectar comportamentos suspeitos e até prever crimes.[29] Demonstra o autor iniciativas governamentais – isoladas ou em colaboração global – para acessar dados e informações privados e públicos, de pessoas físicas e jurídicas, em nome da segurança preventiva e curativa, sem qualquer informação e prestação de contas àqueles que são atingidos por suas políticas.[30]

---

23 Ver a interessante matéria publicada no *site*: https://www.poder360.com.br/poder-tech/tecnologia/leis-rigorosas-garantem-controle-social-na-internet-chinesa/. Acesso em: 30 abr. 2024.

24 Tema bem explorado por ZUBOFF, Shoshana. *The age of surveillance capitalism*. New York: Perseus Books, 2019. p. 61 e seguintes.

25 MOROZOV, Evgeny. *The net delusion*: the dark side of internet freedom. New York: Public Affairs, 2019. p. 38. Na mesma linha o livro de VAROUFAKIS, Yanis. *Technofeudalism*. London: Bodley Head, 2023. Para Varoufakis, as grandes empresas tecnológicas Meta, Amazon, Apple, Alphabet controlam a nossa atenção e medeiam as nossas transações, transformando os humanos em servos digitais que publicam, navegam e compram incessantemente nas suas plataformas. Em vez de perseguir os lucros que derivam do trabalho, os senhores da tecnologia, a quem ele chama de *cloudalistas*, extraem rendas.

26 Nos dias de hoje, já se fala de um novo mercado no qual é possível transferir dados pessoais em troca de benefícios de produtos personalizados. Desta forma, o usuário pode considerar a possibilidade de ceder os seus dados em troca da utilização daqueles (ainda mais quando a maioria cede os seus dados sem receber qualquer tipo de compensação por isso).

27 Entendidas como grandes plataformas digitais que fornecem um conjunto predefinido de serviços digitais, como motores de pesquisa *on-line* e lojas de aplicações e serviços de mensagens. Essas empresas têm: (i) posição econômica forte, com impacto significativo no mercado interno, operando em vários países da UE; (ii) forte posição de intermediação, o que significa que ligam grande base de utilizadores a grande número de empresas; (iii) posição consolidada e duradoura no mercado. A Comissão Europeia, em 6.9.2023, designou como *gatekeepers*: Alphabet, Amazon, Apple, ByteDance e Meta, Microsoft.

28 Ver notícia no *site*: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en. Acesso em: 29 abr. 2024.

29 Ver a matéria publicada no *site*: https://wtm.inf.br/artigos/170-milhoes-de-cameras-monitoram-possiveis-terroristas-na-china/. Acesso em: 30 abr. 2024.

30 KUKSO, Federico. Una historia de control. *In*: STANCANELLI, Pablo. *El Atlas de la revolución digital* – Del sueño libertario al capitalismo de vigilancia. Buenos Aires: Capital Intelectual, 2019. p. 12. Lembra o

Lembremos ainda da ferramenta de espionagem digital chamada *Pegasus*, criada pela empresa israelense NSO Group, usada para grampear *smartphones*, computadores e redes de comunicação e gestão de dados de forma global, tudo isto em nome da promoção da segurança da democracia e dos povos democráticos.[31]

E mais, estes recursos tecnológicos utilizados pelo setor público (Estado) e privado (mercado), por se valerem, em regra, de *software* com códigos fechados, impossibilitam níveis de transparência e visibilidade dos elementos constitutivos neurais de suas operações, inviabilizando controles sociais, políticos e jurídicos mais eficazes.[32]

Por conta destes cenários, tem se tornado cada vez mais comum falarmos na emergência de uma sociedade da vigilância e de uma democracia vigiada, chegando ao ponto de alguns jornalistas afirmarem que privacidade e intimidade configuram já direitos e garantias em certa medida ultrapassados, nomeadamente em tempos de níveis de insegurança global crescente.[33] Daí porque haver muita preocupação disseminada no tecido social em face das dinâmicas de quotidiana expansão incontrolável da vigilância comunitária, que conta com arquitetura e logística sem precedentes na história da civilização, basta atentarmos para o contingente de câmeras de monitoramento em espaços públicos e privados os mais diversos (lojas, bancos, praças públicas, ruas etc.).[34]

---

autor que estes sistemas também podem ser usados para rastrear objetivos políticos escusos envolvendo ofensivas contra dissidentes ou opositores e críticos e governos de ocasião.

31 Ver a excelente matéria publicada no *site* das empresas Globo: https://g1.globo.com/economia/tecnologia/noticia/2021/07/19/entenda-o-que-e-o-pegasus-software-de-espionagem-que-teria-sido-usado-para-invadir-smartphones-de-milhares-de-pessoas.ghtml. Acesso em: 25 abr. 2023, dando conta de que, uma vez instalado, o Pegasus permite que os invasores tenham acesso a qualquer tipo de dado disponível no aparelho invadido, inclusive o uso do microfone e câmera, razão pela qual é vendido a várias agências governamentais para coletar dados de agentes suspeitos de crimes e terrorismo.

32 O FBI, nos EUA, desde há muito utiliza *softwares* de configuração fechada os mais diversos para espionar pessoas físicas e jurídicas em nome da segurança pública nacional, e isto bem antes dos atentados às Torres Gêmeas de 2001, basta lembrarmos os programas Omnivore (1991) e Carnivore (1997), que monitoravam correios eletrônicos e comunicações eletrônicas – mais tarde substituídos por *softwares* disponíveis no mercado. Neste sentido ver a matéria de BAMFORD, James. The shadow factory: the ultra-secrets NSA from 9/11 to the eavesdropping on America. *Democracy Now*, 14 out. 2008. Disponível em: https://www.democracynow.org/2008/10/14/james_bamford_the_shadow_factory_the. Acesso em: 29 abr. 2024.

33 Como quer Scott McNealy, CEO da Sun Microsystemns, no texto *Private Lives?* Not ours! Disponível em: https://www.pcworld.com/article/16331/private_lives_not_ours.html. Acesso em: 23 maio 2022. Há também ótima crítica a estes tempos de VATTIMO, Gianni. *La società transparente*. Roma: Garzanti, 2000. Abordamos estes temas no livro LEAL, Rogerio Gesta e LEAL, Rogerio Gesta; SILVA, Ricardo Machado da. *O direito fundamental social à segurança pública no Estado democrático de direito* – Parâmetros para políticas públicas de implementação. Cruz Alta: Ilustração, 2023.

34 Veja-se como alguns jornais divulgam estes temas, sublinhando somente aspectos positivos: "Com essas soluções é possível que sejam criados eventos de alerta e realizadas análises forenses no vídeo, reduzindo o tempo necessário para a realização de uma investigação, permitindo a notificação automática ou a realização de buscas com filtros para identificação de indivíduos e veículos, como filtros de cor de vestuário, acessórios como bolsas e mochilas, tamanho do objeto, sentido do deslocamento, placa de veículo, marca, modelo entre outras informações. Entre as principais tecnologias utilizadas no monitoramento urbano podemos citar o reconhecimento facial (FR), as tecnologias de leitura de placas de veículos (LPR)

3 Reações à sociedade da vigilância: perspectivas

A despeito de todos estes cenários, a sociedade tem reagido a movimentos panópticos como os anteriormente referidos e bem demarcados por Ryan McKinley, investigador do *MIT Media Lab*,[35] ao desenvolver um sistema denominado *Government Information Awareness* (GIA),[36] que se apresenta como resposta dos cidadãos às iniciativas de controles digitais de governos.

A iniciativa do GIA baseia-se num raciocínio simples: se o governo tem o direito de saber detalhes pessoais dos cidadãos, os cidadãos também têm o direito de saber informações críticas sobre os seus governos. O projeto GIA desenvolveu tecnologias amigáveis que permitem as pessoas criar as suas próprias agências de inteligência para obter, classificar e agir com base nas informações que obtêm sobre os seus governos, bem como documentar assuntos de interesse público, como informações relacionadas com o financiamento de campanhas eleitorais, os currículos dos funcionários públicos, documentando a existência de reclamações, as relações secretas ou confidenciais de grandes corporações, informações que têm sido mantidas classificadas, e até um sistema de construção de perfis baseado no estudo de padrões.

Nesta mesma linha, temos a criação dos chamados *weblogs*.[37] Inicialmente os *weblogs* foram concebidos como sistemas estruturados na internet que permitiam a qualquer pessoa publicar informações pessoais, de forma semelhante a um diário, com capacidade de cadastro de endereços eletrônicos, inclusão de imagens e interação assíncrona. Porém, rapidamente evoluíram para verdadeiros jornais digitais, nos quais é possível encontrar diferentes pontos de vista sobre determinado acontecimento. Estas ferramentas competem hoje – no espaço virtual – com as mídias informativas convencionais.[38]

Como a mudança tecnológica é ecológica e não aditiva, tudo é redefinido, incluindo antigas práticas criminosas, que descobrem inéditas oportunidades com

---

e as soluções de detecção e classificação de áudio" (*Jornal Diário do Comércio*, 5 out. 2022. Disponível em: https://diariodocomercio.com.br/opiniao/videomonitoramento-para-cidades-seguras/. Acesso em: 2 maio 2024).

35 Disponível em: https://www.media.mit.edu. Acesso em: 27 abr. 2024.

36 Ver o *site*: https://www.media.mit.edu/projects/open-government-information-awareness/overview/. Acesso em: 27 abr. 2024. Ver também o interessante *site*: https://www.wired.com/2003/07/slideshow-government-prying-the-good-kind/. Acesso em: 27 abr. 2024.

37 Em 1996, Dave Winer implementou um *weblog*, criando o espaço virtual *24 Horas pela Democracia*, uma reunião *on-line* realizada para apoiar a liberdade de expressão na internet. Algumas *tecnocelebridades* participaram do evento inovador, como Bill Gates, fundador e proprietário da Microsoft, e Phillipe Kahn, da Novell. Mais tarde, o próprio Winer fundou uma empresa especialmente dedicada à criação e desenvolvimento de programa que facilitasse a criação de *weblogs*. O resultado desse projeto foi o *blog* pessoal de Winer, uma das principais referências mundiais da tendência (SAUER, Moritz. *Weblogs, podcasting & online-journalism*. Cambridge: O'Reilly Verlag GmbH & Co., 2017). p. 34 e seguintes.

38 SAUER, Moritz. *Weblogs, podcasting & online-journalism*. Cambridge: O'Reilly Verlag GmbH & Co., 2017. p. 29.

a introdução de novas tecnologias de informação e comunicação a partir da IA.[39] Um exemplo disto é o cibercrime, atividade que representa ameaça real ao desenvolvimento da economia (física e digital) e da sociedade da informação, razão pela qual foi instituída a Convenção sobre o Crime Cibernético, em Budapeste, em 23.11.2001, firmada por inúmeros países do Conselho da Europa.[40]

O problema é que este documento implicou diminuição significativa de algumas garantias em termos de direitos fundamentais, entre as quais a sugestão de que fornecedores de acesso e serviços de internet mantenham registos das atividades realizadas pelos seus clientes no ciberespaço (arts. 17, 18, 24, 25), violando a privacidade e outros direitos dos usuários da internet, além de ser contrárias aos princípios estabelecidos na Declaração Universal dos Direitos Humanos.[41]

As estruturas institucionais dos Estados têm aumentado também para o enfrentamento destes problemas, como podemos ver no Chile, com a criação da *Brigada Investigadora del Cibercrimen* – BRICIB,[42] vinculada à polícia de investigações; no México, com a *Polícia Cibernética*,[43] vinculada à Polícia Federal Preventiva; na Espanha, com a *Brigada Central de Investigación Tecnológica*,[44] vinculada à Direção Geral da Polícia espanhola; em Portugal, com a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, vinculada à Polícia Judiciária; no Brasil, com a Unidade Especial de Investigação de Crimes Cibernéticos, vinculada à Policia Federal.[45] Todos estes órgãos desenvolvem políticas de vigilância da internet, com

---

39 Sobre a regulamentação da inteligência artificial na União Europeia: MIRANZO DÍAZ, Javier. El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas de estandarización. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 96, p. 43-78, abr./jun. 2024. DOI: 10.21056/ aec.v24i96.1932.

40 O Brasil editou o Decreto nº 11.941, de 12.4.2023, promulgando a Convenção sobre o Crime Cibernético no território nacional, ratificada pelo país em 1º.3.2023.

41 De lembrar que a Convenção nº 108, vinculativa para os Estados-Membros do Conselho Europeu, em seu art. 6º, proíbe o tratamento automático de dados reveladores de origem racial, opiniões políticas, crenças religiosas, saúde ou vida sexual, a menos que a legislação nacional estabeleça salvaguardas adequadas. No entanto, em seu art. 9º, permite exceções para proteger a segurança do Estado, segurança pública, interesses financeiros do Estado, repressão de infrações penais ou para proteger os direitos e liberdades de terceiros. A ver como ficarão estas questões no novo documento a Convenção 108+, adotada em 2023, com previsão de entrada em vigor em junho de 2023.

42 Maiores informações no *site*: https://www.pdichile.cl/institución/unidades/cibercrimen. Acesso em: 29 abr. 2024.

43 Maiores informações no *site*: https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica. Acesso em: 29 abr. 2024.

44 Maiores informações no *site*: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php#. Acesso em: 29 abr. 2024.

45 Esta Unidade foi criada recentemente, em 28.6.2022, conforme noticia o *site* da Polícia Federal brasileira: https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos. Acesso em: 30 abr. 2024. Também os estados brasileiros começam a criar unidades especializadas para tal fim, como mostra a notícia veiculada em 18.12.2020, do Estado de São Paulo: https://www.saopaulo.sp.gov.br/spnoticias/governo-do-estado-inaugura-divisao-de-crimes-ciberneticos-2/. Acesso em: 30 abr. 2024. No Rio Grande do Sul, em 3.7.2010, já fora criada Delegacia de Repressão aos Crimes Informáticos – DRCI, conforme anuncia o *site* oficial do governo: https://ssp.rs.gov.br/policia-civil-gaucha-cria-delegacia-pioneira-em-crimes-virtuais. Acesso em: 30 abr. 2024.

foco nas ações de *hackers*, *sites* da internet, comunidades e salas de *chat* em que a pornografia infantil é promovida (analisando as atividades de organizações pedófilas locais e internacionais, redes de prostituição infantil e redes de tráfico de crianças que as exploram em outros países), crimes contra a propriedade intelectual, fraudes eletrônicas, lavagem de dinheiro, tráfico de armas, pessoas e drogas.

No Brasil temos avançado nestes temas, nomeadamente a partir da edição de algumas legislações focadas no uso de novas tecnologias, a saber:

(i) Lei nº 12.258/2010, que modificou a Lei de Execuções Penais no sentido de promover a possibilidade de *utilização de equipamentos de vigilância pelos condenados pela justiça – monitoração eletrônica – para as hipóteses de saída temporária no regime semiaberto e cumprimento de pena em regime domiciliar*;

(ii) Lei nº 12.403/2011, que modificou o Código de Processo Penal e instituiu o monitoramento eletrônico como *medida cautelar*, nos termos do art. 319, inc. IX, desta norma;[46]

(iii) Lei nº 12.681/2012, instituindo o Sistema Nacional de Informações de Segurança Pública, Prisionais, de *Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas* (SINESP), o qual utiliza plataforma de informações integradas das bases de dados do Governo Federal e dos estados, com o escopo de criar estrutura de gestão de informações em nível nacional, produzindo, coletando, sistematizando e disponibilizando informações para a segurança pública;

(iv) Lei nº 12.737/2012, criando a tipificação criminal de delitos informáticos, com penas baixas de detenção de três meses até dois anos;

(v) Lei nº 12.965/2014, que cria o Marco Civil da Internet no Brasil;

(vi) Lei nº 13.675/2018, regulamentada pelo Decreto nº 9.489/2018, criando o Sistema Único de Segurança Pública (SUSP), instituindo políticas de governança, por meio da *padronização de dados, integração tecnológica, de inteligência e operacional* entre os agentes de segurança do país;

(vii) Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais;[47]

---

[46] Nesta ferramenta, o usuário é rastreado via satélite através de um aparelho eletrônico (bracelete, pulseira ou tornozeleira) que funciona por meio de radiofrequência e informações criptografadas dos dados sobre a posição em que ele se encontra. Os dados colhidos pelo sistema são enviados a um servidor e podem ser acessados por terminal conectado à internet. Os argumentos a favor desta opção ponderam que ela operaria redução significativa da população carcerária, bem como diminuição de gastos públicos com presos e reinserção social; enquanto que os argumentos contrários se centram: (i) na possibilidade de retorno a um Estado totalitário, em que a sociedade seria a própria prisão, (ii) na estigmatização social da pessoa em razão da utilização do equipamento de monitoramento em público, (iii) na violação ao direito a intimidade e privacidade. Neste sentido ver o texto de GRECO, Rogério. *Direitos humanos, sistema prisional e alternativas à privação de liberdade*. São Paulo: Saraiva, 2011. p. 118.

[47] FÁCIO, Rafaella Nátaly. A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil. *Revista*

(viii) em 2018, o Conselho Nacional de Justiça (CNJ) criou o Banco Nacional de Monitoramento de Prisões (BNMP), base de dados e sistema eletrônico em que constam os *dados cadastrais das pessoas presas no sistema carcerário do Brasil*, com o objetivo de centralização das informações e contribuição para o acesso às informações pelas autoridades judiciárias e policiais, auxiliando as autoridades judiciárias da justiça criminal na gestão de documentos atinentes às ordens de prisão/internação e soltura expedidas em todo o território nacional, materializando um Cadastro Nacional de Presos.

O Plano Nacional de Segurança Pública de 2018 introduziu, como estratégia nº 8, o *videomonitoramento com reconhecimento facial biométrico*, destacando-se as habilidades que *softwares* de computadores possuem de analisar rostos humanos constantes de uma base de dados específica, utilizando conexões de internet para catalogar indivíduos, via captação de sua biometria extraída por *smartphones*, computadores e câmeras de vigilância.[48] Esta política pública, no Brasil, estava voltada precipuamente para a fiscalização de fronteiras, divisas interestaduais, portos, aeroportos, rodoviárias e ferrovias.[49] Mas agora também espaços públicos urbanos estão sendo tomados por estes mecanismos, como ocorre na experiência da plataforma de videomonitoramento *Smart Sampa*, em São Paulo, que tem previsão de integrar mais de 20 mil câmeras até 2024 na capital.[50] As polêmicas acerca do projeto são muitas: questionamentos judiciais,[51] edital suspenso, muita resistência da sociedade e histórico de corrupção pela empresa responsável.[52]

Eurolatinoamericana de Derecho Administrativo, Santa Fe, v. 10, n. 2, e247, jul./dic. 2023. DOI 10.14409/redoeda.v10i2.13413.

48 Na Europa, o Conselho Europeu de Proteção de Dados, encarregado de aplicar o Regulamento Geral de Proteção de Dados, emitiu a Diretriz 05/2022, sobre o uso desta ferramenta, entendendo que ela representa interferência desproporcional nos direitos dos titulares dos dados, vez que compromete a expectativa das pessoas de permanecerem anônimas, contrariando os princípios de autodeterminação e participação livre em sociedades democráticas. Ver o documento integral no *site*: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en. Acesso em: 29 abr. 2024.

49 Inúmeros países se valeram destas tecnologias para fins de: (i) monitorar o cumprimento do *lockdown* adotado ao longo da pandemia de Covid-19 (China); (ii) monitoramento comportamental de pessoas na Olimpíada de 2020, no Japão, também decorrente da pandemia; (iii) monitoramento de grandes eventos (Reino Unido) para identificar pessoas procuradas pela polícia. Nos EUA temos notícias de proposta de lei federal (2023) que quer regulamentar a matéria (*Facial Recognition Act*), restringindo o emprego do reconhecimento facial biométrico (Disponível em: https://www.congress.gov/bill/117th-congress/house-bill/9061/text?s=1&r=7. Acesso em: 29 abr. 2024).

50 Dentre os movimentos que deram força no combate à plataforma, está a campanha *Tire meu rosto da sua mira*, feita por mais de 50 entidades da sociedade civil e que tem como objetivo solicitar o banimento do uso das câmeras para segurança pública (Disponível em: https://tiremeurostodasuamira.org.br. Acesso em: 22 abr. 2024).

51 Notícia veiculada pelo sítio jurídico do *Conjur*, em 17.5.2024, dá conta de que quatro estados brasileiros já prenderam mais de 1,7 mil pessoas utilizando o reconhecimento facial sem regulamentação adequada para tanto. Ver matéria completa no *site*: https://www.conjur.com.br/2024-mai-17/sem-regulacao-estados-prendem-centenas-utilizando-reconhecimento-facial/. Acesso em: 18 mai. 2024.

52 Informa o *site* do projeto que: "A nova plataforma ainda facilita a integração de diversos serviços municipais, como CET, SAMU, Defesa Civil e GCM, em uma única plataforma por meio da criação de uma moderna

(i) Decreto nº 10.882/2021, criando o Plano Nacional de Segurança Pública – 2021/2030, e visando, dentre outras metas, promover a *expansão tecnológica* na promoção de políticas de segurança pública, utilizando-se, para tanto, de padronização, integração e interoperabilidade dos dados sobre segurança pública entre União, estados, Distrito Federal e municípios (estratégia nº 7);[53]

(ii) também em 2021 foi instituída a política de *adoção de câmeras corporais nos uniformes dos policiais* (*body-worn*), instaladas na farda, capacete ou óculos dos policiais, com capacidade de captar e gravar, vídeo e áudio das atividades desenvolvidas pelos agentes em sua rotina policial, a exemplo de gravações de trânsito, detenções, revistas, interrogatórios.[54]

O problema é que, modo geral, estas políticas de segurança pública virtuais estão estruturadas a partir de ferramentas tecnológicas de *software* fechado, o que tem aumentado em nível global as pressões sociais e políticas à regulamentação das *big tech*, assim como se amplia o uso de sistemas de fonte aberta, já tendo algumas que fazem parte da *Software Choice Initiative*, avançado neste sentido, dentre as quais: Intel (EUA), Linux (EUA), Open Solutions (Argentina), Paradigma (Brasil), Associação Peruana de Software (Peru), Siam Commercial Bank (Tailândia), VSI (Alemanha).[55] E estes modelos abertos ao menos dariam maiores garantias

---

Central de Monitoramento Integrada. Além disso, com as novas câmeras, os órgãos de segurança terão como monitorar escolas, UBS e demais equipamentos públicos, aumentando significativamente a segurança nesses locais. As câmeras técnicas contarão ainda com monitoramento de calor, facilitando a supervisão em praças e parques, que normalmente possuem árvores e áreas verdes que podem prejudicar uma vigilância mais precisa" (Disponível em: https://participemais.prefeitura.sp.gov.br/legislation/processes/209. Acesso em: 22 abr. 2024).

53 Disponível em: https://www.gov.br/mj/pt-br/centrais-de-conteudo/publicacoes/categorias-de-publicacoes/planos/plano_nac-_de_seguranca_publica_e_def-_soc-_2021___2030.pdf. Acesso em: 29 abr. 2024.

54 O Estado de São Paulo foi pioneiro na adoção da prática, sendo replicada em outros estados como o Rio de Janeiro, Minas Gerais, Pará, Santa Catarina e Rio Grande do Sul. Ver a matéria do Núcleo de Estudos da Violência, da Universidade de São Paulo, no *site*: https://nev.prp.usp.br/projetos/pesquisa-uso-cameras-corporais-pela-policia-militar-de-sp/. Acesso em: 29 abr. 2024. O *site* dá conta de que, no Estado de São Paulo: "Estudo realizado pelo Fórum Brasileiro de Segurança Pública indicou uma queda geral de 62,7% na letalidade policial, entre 2019 e 2022, com especial ênfase nas unidades já equipadas com as COPs. Análise realizada pelo CCAS/FGV, com colaboração da PMESP, indica que as câmeras foram responsáveis diretamente por 57% de redução no número de mortes decorrentes de intervenção policial e queda 63% nas lesões corporais causadas por policiais militares. Estudo recente do Instituto Sou da Paz revela que os casos de mortes de jovens (entre 15 e 24 anos) caíram 46% após a implementação das câmeras".

55 Ver o *site*: https://web.archive.org/web/20061107202717/http://www.softwarechoice.org/. Acesso em: 29 abr. 2024. No Reino Unido, em 15.7.2002, o *Commerce Office* lançou o projeto de *software* de código aberto. Esta iniciativa afirma que um *software* de código aberto bem configurado pode ser tão seguro quanto sistemas proprietários e está atualmente sujeito a menos ataques pela internet. Por esta razão devem se estabelecer equilíbrios entre a disponibilidade de competências de administração e segurança e as vantagens que diferentes sistemas podem proporcionar. Ver as informações no *site*: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://assets.publishing.service.gov.uk/media/5a79cceced915d042206b200/All_About_Open_Source_v2_0.doc&ved=2ahUKEwiY6LC4vueFAxVqrpUCHVqmDL8QFnoECDAQAQ&usg=AOvVaw1q_eK5Ym0tvDSO4c8dUjw2. Acesso em: 29 abr. 2024.

técnicas de monitoramento e visibilidade dos processos de acesso e gestão de dados, tanto às pessoas como ao Estado.[56]

Em nível de judicialização destas discussões, vale lembrar as decisões do Supremo Tribunal Federal – STF, na Ação Declaratória de Inconstitucionalidade nº 6.649, e na Ação de Descumprimento de Preceito Fundamental nº 695, entendendo que o compartilhamento de dados pessoais entre órgãos públicos – mesmo para fins de segurança pública – pressupõe propósitos legítimos e específicos,[57] e o procedimento deve cumprir todos os requisitos da Lei Geral de Proteção de Dados (Lei nº 13.709/2018).[58] Se forem desobedecidas as diretrizes da LGPD, o Estado responderá objetivamente pelos danos causados às pessoas. E o funcionário que dolosamente violar o dever de publicidade estabelecido no art. 23, I, da LGPD responderá por ato de improbidade administrativa.[59]

De igual sorte, no Tema nº 977,[60] o STF está enfrentando o tormentoso tema de se o acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida, e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade[61] e ao sigilo das comunicações e dados dos indivíduos.

4 Notas conclusivas

Temos, pois, como conclusão destas reflexões, que algumas premissas se fazem importantes para viabilizar políticas de segurança pública democráticas com o uso de tecnologias virtuais, a saber:

---

56 Acerca do direito fundamental à proteção de dados, ver: ARAÚJO, Valter Shuenquener de; PERIM, Maria Clara Mendonça; RIBEIRO, Koryander Figueirêdo. As assimetrias da regulação estatal para a proteção de dados pessoais e a afirmação dos direitos fundamentais de primeira dimensão. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 87, p. 267-296, jan./mar. 2022. DOI: 10.21056/aec.v22i87.1453; SÁNCHEZ DÍAZ, María Fernanda. El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 10, n. 1, e235, ene./jun. 2023. DOI: 10.14409/redoeda.v10i1.12626.

57 Sobre a jurisprudência do Supremo Tribunal Federal em matéria de comunicação de dados: ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. *Revista de Investigações Constitucionais*, Curitiba, v. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280.

58 MARTINS, Ricardo Marcondes. Proteção de dados, competências dos entes federativos e a Emenda Constitucional n. 115/22. *Revista de Investigações Constitucionais*, Curitiba, v. 9, n. 3, p. 645-658, set./dez. 2022. DOI: 10.5380/rinc.v9i3.87107.

59 Conforme decisão publicada no *site* do STF: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em: 30 abr. 2024.

60 Conforme *site* do STF: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ARE%201042075%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 30 abr. 2024.

61 ROBLES OSOLLO, Ana Gloria. El derecho a la privacidad y la protección de datos personales transfronterizos. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 35-60, ene. /jun. 2021. DOI 10.14409/redoeda.v8i1.9543.

a) quadros legais e regulamentares: com a aplicação e harmonização dos quadros jurídicos e regulamentares atuais para promover um ambiente de certeza e confiança na adoção, utilização e promoção das tecnologias;
b) interoperabilidade: em torno das capacidades estruturais, técnicas, organizacionais e de governança necessárias para compartilhar informações e gerar conhecimento, com transparência e prestação de contas públicas;
c) dados abertos: disponibilização de informação governamental em formatos úteis e reutilizáveis por diferentes entidades governamentais, população, organizações da sociedade civil, cooperadores e universidades, entre outros, para promover o empreendedorismo e a governação a partir da ideia de segurança cidadã;
d) conectividade e ferramentas digitais adequadas: fortalecimento e desenvolvimento das redes (governamentais e cidadãs), expansão de melhores infraestruturas nos territórios e da capacidade das redes existentes, e o desenvolvimento de (i) competências no setor das tecnologias para estimular aplicações principalmente em redes celulares massivas, e (ii) ferramentas virtuais que viabilizem aplicações para denúncias/demandas/respostas em múltiplas plataformas;[62]
e) participação cidadã e competências digitais: desenvolvimento equitativo de competências para desenvolver e operar tecnologias e serviços digitais, contemplando a cobertura social e o desenvolvimento de competências em sistemas comunitários;
f) comunicação digital e redes sociais: como instrumento de capacitação e consciência social para apoiar estratégias digitais, comunicação digital focada nos cidadãos e nas suas necessidades como demandantes de segurança e convivência, prestando serviços baseados na gestão do conhecimento, e não apenas na informação.

Nomeadamente no Brasil estes elementos não se fazem ainda exaustivamente presentes, o que nos vai demandar ainda muito tempo.

Referências

ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. *Revista de Investigações Constitucionais*, Curitiba, v. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280.

[62] A Venezuela tem um aplicativo chamado *Patrulha Inteligente*, que detecta o quadrante de segurança correspondente à localização do usuário, fornecido pelo GPS do seu celular, ou por meio do seu provedor de rede, e fornece as informações para que possa entrar em contato com o número de telefone de emergência associado. Os cidadãos podem ligar para as autoridades policiais e militares mais próximas da sua área e fazer as suas queixas de forma anônima. Mais informações no *site*: https://consejogeneraldepolicia.org/opinion/patrullaje-inteligente/. Acesso em: 29 abr. 2024.

ARAÚJO, Valter Shuenquener de; PERIM, Maria Clara Mendonça; RIBEIRO, Koryander Figueirêdo. As assimetrias da regulação estatal para a proteção de dados pessoais e a afirmação dos direitos fundamentais de primeira dimensão. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 87, p. 267-296, jan./mar. 2022. DOI: 10.21056/aec.v22i87.1453.

BAMFORD, James. The shadow factory: the ultra-secrets NSA from 9/11 to the eavesdropping on America. *Democracy Now*, 14 out. 2008. Disponível em: https://www.democracynow.org/2008/10/14/james_bamford_the_shadow_factory_the. Acesso em: 29 abr. 2024.

BITENCOURT, Caroline Müller; MARTINS, Luisa Helena Nicknig. A inteligência artificial nos órgãos constitucionais de controle de contas da administração pública brasileira. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 3, e253, set./dez. 2023. DOI: 10.5380/rinc.v10i3.93650.

BLANCHET, Luiz Alberto; TRENTO, Melissa. A inteligência artificial como diretriz propulsora ao desenvolvimento e à eficiência administrativa. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 23, n. 93, p. 153-172, jul./set. 2023. DOI: 10.21056/aec.v23i93.1733.

BOMTEMPO, Eugênio Morais; CARMONA, Paulo Cavichioli. A solidariedade social na pandemia de Covid-19. A*&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 89, p. 251-276, jul./set. 2022. DOI: 10.21056/aec.v22i89.1662.

CASTELS, Manuel. *La sociedad en red* – La era de la información. Economía, sociedad y cultura. Madrid: Alianza Editorial, 1997. v. 1.

CASTILLO ARJONA, Mónica. El fenómeno de la Covid-19 y sus efectos sociales en el derecho administrativo del siglo XXI. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 173-187, ene./jun. 2021. DOI: 10.14409/redoeda.v8i1.9548.

CERI, Paolo. *La società vulnerabile* – Quale sicurezza, quale libertà. Roma/Bari: Laterza, 2003.

COLE, David. *Enemy Aliens* – double standards and constitutional freedoms in the war on terrorism. New York: The New Press, 2003.

D'AGOSTINI, Franca; FERRERA, Maurizio. *Le verità del potere* – Sei diritto aleatici. Roma: Einaudi, 2019.

DAVARRA RODRIGUEZ, Miguel Angel. *De las autopistas de la información a la sociedad virtual*. Madri: Aranzadi Editorial, 2008.

DOMINICI, Piero. *La società dell'irresponsabilità*. Milano: Franco Angeli, 2015.

FELICE, Emanuele. *Dubai* – L'ultima utopia. Roma: Il Mulino, 2020.

FERRAJOLI, Luigi. *La democrazia attraverso i diritti*. Roma: Laterza, 2013.

FOUCAULT, Michel. *Vigilar y castigar*. Nacimiento de la prisión. México: Siglo XXI, 1983.

GRECO, Rogério. *Direitos humanos, sistema prisional e alternativas à privação de liberdade*. São Paulo: Saraiva, 2011.

HARARI, Yuval Noah. *Homo Deus*. Uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

HERNANDES, Luiz Eduardo Camargo Outeiro; PIOVESAN, Flávia. Desafios judiciais em tempos de pandemia: fortalecendo o diálogo entre a Comissão Interamericana de Direitos Humanos e o Supremo Tribunal Brasileiro para a proteção dos direitos humanos. *Revista de Investigações Constitucionais*, Curitiba, v. 9, n. 2, p. 371-388, maio/ago. 2022. DOI: 10.5380/rinc.v9i2.86138.

KUKSO, Federico. *Una historia de control*. Buenos Aires: Capital Intelectual, 2019.

LEAL, Rogerio Gesta. *Segurança pública no Estado democrático de direito* – Avanços e recuos. São Paulo: Tirant lo Blanch, 2023.

LEAL, Rogerio Gesta; SILVA, Ricardo Machado da. *O direito fundamental social à segurança pública no Estado democrático de direito* – Parâmetros para políticas públicas de implementação. Cruz Alta: Ilustração, 2023.

MARTINS, Ricardo Marcondes. Proteção de dados, competências dos entes federativos e a Emenda Constitucional n. 115/22. *Revista de Investigações Constitucionais*, Curitiba, v. 9, n. 3, p. 645-658, set./dez. 2022. DOI: 10.5380/rinc.v9i3.87107.

MARTNEZ GARBIRAS, María Margarita; SÁNCHEZ-HUERTAS, Luis Fernando. Los atajos de la Cuarta Revolución Industrial a la democracia: una reflexión de lecciones aprendidas en clave de Lafont y Berlin. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 23, n. 94, p. 43-62, out./dez. 2023. DOI: 10.21056/aec.v23i94.1725.

MCNEALY, Scott. Private Lives? Not ours! *PC World*. Disponível em: https://www.pcworld.com/article/16331/private_lives_not_ours.html. Acesso em: 23 maio 2022.

MIRANZO DÍAZ, Javier. El Reglamento de Inteligencia Artificial de la Unión Europea: regulación de riesgos y sistemas de estandarización. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 96, p. 43-78, abr./jun. 2024. DOI: 10.21056/ aec.v24i96.1932.

MONGARDINI, Carlo. *Le dimensioni sociali della paura*. Milano: Franco Angeli, 2010.

MOROZOV, Evgeny. *The net delusion*: the dark side of internet freedom. New York: Public Affairs, 2019.

NÓBREGA, Marcos; HEINEN, Juliano. As forças que mudarão a Administração Pública pós-Covid: transparência 2.0, blockchain e smart contracts. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 21, n. 85, p. 217-230, jul./set. 2021. DOI: 10.21056/aec.v21i85.1405.

PHILIPPI, Juliana Horn Machado. Transformação digital e urgência da cultura de dados na Administração Pública brasileira. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 10, n. 1, e232, ene./jun. 2023. DOI: 10.14409/redoeda.v10i1.12401.

PUSCHEL, André Felipe Silva; RODRIGUES, Roberto Tessis; VALLE, Vivian Cristina Lima López. O dilema ético da decisão algorítmica na administração pública. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 90, p. 207-226, out./dez. 2022. DOI: 10.21056/aec.v22i90.1737.

RODRÍGUEZ-ARANA MUÑOZ, Jaime. Administrative Law and human dignity (on the post-pandemic reconstruction of Administrative Law). *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 22, n. 88, p. 11-33, abr./jun. 2022. DOI: 10.21056/ aec.v22i88.1646.

SÁNCHEZ DÍAZ, María Fernanda. El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 10, n. 1, e235, ene./jun. 2023. DOI: 10.14409/redoeda.v10i1.12626.

SÁNCHEZ DÍAZ, María Fernanda. El impacto de la inteligencia artificial generativa en los derechos humanos. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 11, n. 1, e252, ene./jun. 2024. DOI: 10.14409/redoeda.v11i1.13612.

SÁNCHEZ DIAZ, Maria Fernanda; ROMERO TELLO, Ana Guadalupe. Covid-19, Derechos Humanos y Estado frente al manejo de la Pandemia. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 8, n. 1, p. 233-254, ene. /jun. 2021. DOI 10.14409/redoeda.v8i1.9525.

SAUER, Moritz. *Weblogs, Podcasting & Online-journalism*. Cambridge: O'Reilly Verlag GmbH & Co., 2017.

SIERRA CADENA, Grenfieth de Jesus. Implementación de la Inteligencia Artificial en las Altas Cortes de Colombia: los casos de la Corte Constitucional y el Consejo de Estado. *Revista Eurolatinoamericana de Derecho Administrativo*, Santa Fe, v. 11, n. 1, e253, ene./jul. 2024. DOI 10.14409/redoeda.v11i1.13824.

TOFFLER, Alvim. *La tercera ola*. México: Edivisión, 1981.

TOLEDO, Claudia; PESSOA, Daniel. O uso de inteligência artificial na tomada de decisão judicial. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 1, e237, jan./abr. 2023. DOI: 10.5380/rinc.v10i1.86319.

VALLE, Vivian Cristina Lima López; RUIZ, Maria Guadalupe Fernandes; BÜTTNER, Marcielly. Fake news, influência na formação da opinião pública e impactos sobre a legitimidade da decisão pública. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, ano 24, n. 95, p. 73-97, jan./mar. 2024. DOI: 10.21056/aec.v24i95.1898.

VALLE, Vivian Lima López; FUENTES I GASÓ, Josep Ramón; AJUS, Attílio Martins. Decisão judicial assistida por inteligência artificial e o Sistema Victor do Supremo Tribunal Federal. *Revista de Investigações Constitucionais*, Curitiba, v. 10, n. 2, e252, maio/ago. 2023. DOI: 10.5380/rinc.v10i2.92598.

VAROUFAKIS, Yanis. *Technofeudalism*. London: Bodley Head, 2023.

VATTIMO, Gianni. *La società transparente*. Roma: Garzanti, 2000.

VERHOEVEN, Charles Leben. *Le principe de précaution* – Aspects de droit international et communautaire. Paris: Éditons Panthéon-Assas, 2022.

WALZER, Michael. *La libertà e i suoi nemici nell'età della guerra al terrorismo*. Roma/Bari: Laterza, 2010.

ZOLO, Danilo. *Sula paura* – Fragilità, aggressività, potere. Milano: Feltrinelli Editore, 2011.

ZUBOFF, Shoshana. *The age of surveillance capitalism*. New York: Perseus Books, 2019.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

LEAL, Rogério Gesta. Segurança pública e inteligência artificial – Novos paradigmas. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 81-99, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.leal.

Informações adicionais

Additional information

INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 05 · n. 02 · maio/agosto 2024 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.5.n.2

05

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

International Journal of Digital Law – IJDL
ISSN 2675-7087
DOI: 10.47975/digital.law.vol.5.n.2.niebla

Smart contracts: the new method of interaction between the law and technology*

Contratos inteligentes: El nuevo método de interacción entre el derecho y la tecnología

Jesus Manuel Niebla Zatarain**
Universidad Autónoma de Sinaloa (Culiacán Rosales, Mexico)
j.niebla@uas.edu.mx
https://orcid.org/0000-0001-8460-4538

Paola Jackeline Ontiveros Vázquez***
Universidad Nacional Autónoma de Mexico (Ciudad de Mexico, Mexico)
paolaontiveros@hotmail.com
https://orcid.org/0000-0003-1460-7914

Recebido/Received: 03.09.2024/ September 9th, 2024
Aprovado/Approved: 14.10.2024/ October 10th, 2024

Abstract: Technology has reshaped the law. The Internet and derived technologies have led to the adaptation of traditional legal figures with the objective of bringing certainty to users and developers. A field that has been subject of constant technological development is contact law. This paper will address this scenario from the perspective of smart contracts, which allows not only a digital representation of

Como citar esse artigo/*How to cite this article*: NIEBLA ZATARAIN, Jesus Manuel; ONTIVEROS VÁZQUEZ, Paola Jackeline. Smart contracts: the new method of interaction between the law and technology. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 103-123, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.niebla.

* This article is part of the project "Regulation of Digital Environments through Legal Reasoning Based on Artificial Intelligence" code CF-2023-G-772 sponsored by the National Council of Humanities Science and Technology of Mexico ("Regulación de Entornos Digitales a través derazonamiento legal basado en inteligencia artificial" claveCF-2023-G-772 del Consejo Nacionalde Humanidades, Ciencia y Tecnología (CONAHCYT) de México

** Professor and Reseacher at the Faculty of Law of Mazatlan of the Autonomous University of Sinaloa (Culiacán Rosales, Mexico). E-mail: j.niebla@uas.edu.mx.

*** Professor attached to the Postgraduate Law Program at the National Autonomous University of Mexico (Ciudad de Mexico, Mexico). E-mail: paolaontiveros@hotmail.com.

the obligations agreed by the parties, but also the capacity to solve discrepancies to ensure operation and the lawful fulfillment of its objective. Finally, this joint approach offers compatibility with transactions that take place in digital scenarios, contributing to a safer and law compliant cyberspace.

Keywords: Artificial intelligence; contracts; artificial legal reasoning; legal informatics; digital platforms.

Resumen: La tecnología ha remodelado la ley. Internet y las tecnologías derivadas han propiciado la adaptación de figuras jurídicas tradicionales con el objetivo de aportar certidumbre a usuarios y desarrolladores. Un campo que ha sido objeto de constante desarrollo tecnológico es el derecho de contactos. Este trabajo abordará este escenario desde la perspectiva de los contratos inteligentes, que permiten no solo una representación digital de las obligaciones acordadas por las partes, sino también la capacidad de resolver discrepancias para asegurar su operación y el debido complimiento de su objeto. Finalmente, este enfoque conjunto ofrece compatibilidad con transacciones que tienen lugar en escenarios digitales, contribuyendo a un ciberespacio más seguro y compatible con la ley.

Palabras clave: Inteligencia artificial; contratos; razonamiento jurídico artificial; informática jurídica; plataformas digitales.

1 Introduction

Technological development has traditionally impacted the legal field, whether through the regulation of a new scenario or by expanding already existing legal provisions. Nonetheless, this relation which has occurred in a traditional and escalated manner has been changed abruptly with the arrival of the cyberspace. This development expanded human interaction in an unforeseen volume and facilitated the migration of human activities to digital platforms through the use of the computational technologies, such as artificial intelligence. In this sense, a legal element that has been subject of technical approach are contracts, now referred as smart contracts. These agreements operate through platforms that represent the interests of the parties, guarantying the fulfilment of the contracted obligations. Within this new techno-legal paradigm, the position of the legal framework has shifted to a cooperative role, no longer being an independent subject that intervenes *ex post* but one embed to the technological element. However, these developments have recurrent errors derived of the incompatibility between natural and formal expressions of languages, which generates inconsistencies that impact the construction of the legal outcome. To solve this, a deterministic approach will be presented, which will also facilitate harmonization between different jurisdictions. This will enhance the legal representation process within the smart contract, providing legal certainty to the parties involve and facilitating its dissemination within the techno-legal market.

2 Smart contracts: making obligations "digitally" smart

Law is experimenting a transformation process as a direct result of the development of intelligent technology. This can be seen either through the expansion of regulatory frameworks to include virtual environments or by collaborating in the development of cognitive modules to allow law compliant operation of automated devices. Regarding the last point, the arrival of cyberspace and the dissemination of ubiquitous technology have incremented this approach developing new forms of legal interaction, this is the case of smart contracts. Nonetheless, there is a vast variety of definitions regarding this technology, one of the accepted ones states that "a smart contract is an agreement whose execution is both automatable and executable".[1] In this matter, Szabo (1996) defines these developments as "a set of promises, specified digitally, which include protocols in which the parties carry out a series of premises". Similarly, Alharby and van Moorsel state that smart contracts are "executable code that operates on blockchain to facilitate, execute and enforce the terms of an agreement. The main objective of smart contracts is, consequently, to automatically execute the terms of said agreement ".[2] Notably, these developments are considered not only as an extension of a traditional legal act in digital platforms, but as a new mechanism capable of delivering legal certainty to the parties under a technological scheme. In relation to its operation, it is important to note that although it is a largely automated approach, some parts may still require human intervention and control. In this sense, its operating model includes the legal application of rights and obligations as well as tamper-proof execution.[3] The implementation and automatic execution of the contract is based on legal knowledge translated into computational code.[4] Consequently, the execution of the content of the contract is not based on the human element, but on the representation of human interaction through computers, producing effects on both physical and digital environments. The operation of these developments can be seen in a variety of scenarios, for example, when a customer has acquired a particular type of bank financing, certain transactions will automatically occur if predetermined conditions are met. In this way, if the client defaults on the payments foreseen as part of their loan, the contract can trigger a particular type of consequence. As can be inferred, a smart contract seeks to replicate not only the regulatory framework applicable

1 MADIR, J. *Smart Contracts (How) Do They Fit Under Existing Legal Frameworks?*, 2018.

2 ALHARBY, M.; VAN MOORSEL. A. Blockchain-based smart contracts: A systematic mapping study, in International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), 2018, p. 2 .*Conference on Cloud Computing, Big Data and Blockchain (ICCBB),* 2018, p. 2.

3 CLACK, C. D.; BAKSHI, V. A.; BRAINE, L. Smart contract templates: foundations, design landscape and research directions, *Cornell University,* 2017, p. 8.

4 T. HVITVED, "Contract formalisation and modular implementation of domain-specific languages", in *Doctoral dissertation, PhD thesis, Department of Computer Science, University of Copenhagen*, 2011 p. 4-5.

to a particular scenario, but also the interaction process inherent to the parties. Regarding its classification, Raskin (2016) establishes the existence of two types of smart contracts: rigid and weak. The first category encompasses those that have prohibitions, including revocation and modification of terms. On the other hand, weak smart contracts do not possess these characteristics. From a legal point of view, this classification can be seen as follows: if a court is able to effectively reverse[5] or alter the operation through a legal order, it is a weak smart contract. Conversely, if altering the contract to reverse its results proves too computationally costly for the court, then it is a strong smart contract. The complexity of these digital approaches is further intended to provide a method for resolving dispute.[6] Considering its configuration, the aforementioned author presents two approaches: traditional and non-traditional application methods.[7] The first classification refers to those contracts designed to resolve disputes through the implementation of elements used by legal courts. Non-traditional media target those that are technologically more complex and have little or no opportunity to perform differently from what was originally coded (they may still have software flaws, however). This differs from traditional legal positions as the proposed solution is reasoned by the cognitive module of the smart contract. The foregoing has led to situations in which a techno-legal opinion is required depending on the nature of the scenario.

2.1 Smart contracts: Generalities

Smart contracts operate through a logical representation of contract law and respond to the particularities of the interaction of the parties in a given scenario. In general, these devices operate under two minimum elements:[8] 1. Deliver a version equivalent to a contract concluded in the physical world, guaranteeing its security through cryptographic methods, and 2. These developments are compatible with automated technology. However, beyond the apparent novelty of this approach, it is important to note that it was first presented in 1994.[9] The adoption of these devices has been limited, among other factors, by the positions coming from traditional sectors, which are reluctant to accept them as representations of their physical counterparts, which, in many cases, is the result of interpretation problems. In this sense, when one of the parties presents their case before a Court, the legal operators

5 This term refers to breaking down the structure of a smart contract.

6 STARK, J. *Making sense of blockchain smart contract*, available at: https://www.coindesk.com/making-sense-smart-contracts.

7 STARK, J. *Making sense of blockchain smart contract*, available at: https://www.coindesk.com/making-sense-smart-contracts.

8 LADLEIF, J.; WESKE, M. *A Unifying Model of Legal Smart Contracts*, in *International Conference on Conceptual Modeling Springer*, 2019 p. 3-7.

9 SZABO, N. Formalizing and securing relationships on public networks. *First Monday*, 1997, p. 10.

base their decision exclusively on the operation of these devices. However, smart contracts (especially those considered rigid) are incompatible with this position due to their technological architecture. These devices operate through a self-executing protocol which, to be analysed, requires that they conclude their execution. It is important to note that this characteristic should not be understood as a negative element in the strict sense, since it fulfils the purpose of significantly reducing the possibility of presenting operational errors during the execution stage of these contracts. This ends up being an advantage over traditional legal agreements since the fulfilment of the conditions established in the contract.

To avoid the drawbacks of this approach, the adoption of contractware is recommended.[10] Naturally, both for the legal and the technological position, its performance and application will depend on the level of compatibility of said conditional structure.[11] Additionally, it is important to note that the judge may order the operational description on which the smart contract operates, the role delivered by the parties, as well as the conditions and their representation within the contract. This scenario led to the constant development of new collaborations within the technology sector, one of the most important being the adoption of blockchain. In the next section, this approach will be addressed.

3 Let's play it safe: Blockchain and smart contracts

One of the most important technical components of smart contracts is the use of blockchain technology. This digital approach is defined by Böhme et al as "a decentralized collection of data which is analysed by members of a point-to-point network. In this sense, Satoshi Nakamoto in 2010 He said possible about the blockchain "its design allows the development of a tremendous variety of transactions. Escrow transactions, linked contracts, third party arbitration, multiple signatures, etc."[12] Regarding its technical composition, blockchain is a database distributed over a network which keeps a record of all the transactions that take place within it. This database is replicated and shared by the participants and must communicate and deliver transactions between each of them in a secure way without the participation of third parties. Each block is linked to the previous one, thus resulting in a chain of blocks, thus generating a series or chain of transactions.

10 For further reading see: M. RASKIN, *The law and legality of smart contract*, in *Georgetown Law Technology Review 304*, 2017.

11 Dicha postura fue mencionada es propuesta en: J. MCCARTHY, *Recursive functions of symbolic expressions and their computation by machine*, in *Communications of the ACM 3.4*, 1960.

12 M. SWAN, *Blockchain: Blueprint for a new economy*, in *O'Reilly Media, Inc.* 2015, p. 10.

After a block is created and appended to said chain, the transactions contained in it cannot be modified. This guarantees the integrity of these operations and increases their efficiency, preventing the problem of double investment of resources.[13]

However, the implementation of blockchain delivers a new set of legal and governance challenges. From a law enforcement perspective, merging legal concepts and smart contracts present a range of conceptual and technical problems,[14] which must be approached from an equitable perspective for both the legal and technical sectors. A promising approach to solve this relies the adoption of deontic logic to properly represent legal logic expressions through computational code. This allows not only to properly represent contract law but also to include potential situations that may affect the execution of the obligation of the parties.

3.1 Blockchain and smart contracts: the relation grows

Without a doubt, one of the most influential developments in smart technology in the last years are smart contracts. Szabo defines them as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises". Another position defines them as "executable code that runs on the blockchain to facilitate, execute and enforce the terms of an agreement. The main aim of a smart contract is to automatically execute the terms of an agreement".[15] Regarding its technical composition, these developments offer fees considerable lower than those provided by traditional systems that require a third party to enforce the terms contained on the agreement. Regardless its apparent novelty, the original conception of what it is called today smart contracts was first conceived in 1994,[16] but it was until blockchain technology emerged that the idea finally became a reality. Additionally, these developments proved compatible with electronic data interchange (EDI) formats, which have been used for several decades now to communicate digitally across supply chains.[17] A technical approach that has deeply impacted Contract Automation is the Ricardian Contract. "A Ricardian Contract can be defined as a single document that is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable by people [...], d) readable by programs [...], e) digitally signed, f) carries

13 M. ALHARBY and A. VAN MOORSEL, *op. cit.* p. 6-7.

14 G, GOVERNATORI, F, IDELBERGER, Z. MILOSEVIC, R. RIVERET, G. SARTOR, X. XU, *On legal contracts, imperative and declarative smart contracts, and blockchainsystems*, in *Artificial Intelligence and Law 26 (4)*, 2018, p. 395.

15 M. ALHARBY and A. VAN MOORSEL, *op. cit.* p. 4.

16 N. SZABO, *op. cit.* p. 11.

17 To know more about EDIs, visit: What is EDI (Electronic Data Interchange)? *EDI Basics*, 2024. Available in: https://www.edibasics.com/what-is-edi/. Last accessed August 27th 2024.

the keys and server information, and g) allied with a unique and secure identifier".[18] This approach was the first to deliver a contract suitable of being understood by humans and computers. Consequently, it is not only legally enforceable but will also lend itself to analysis by and interaction with software.[19] This concept is easily extendible to cover Contracts other than token issues. Key features of the Ricardian Contract is the concept of a single document that holds both the Natural Language Contract and its logical description in a language capable of being interpreted by a computer. In section 5, potential issues on the automation of Contracts will be discussed. A Ricardian Contract needs an underlying platform capable of providing certain features and properties to such digital construct:

1. Immutable storage, as the platform needs to hold a reliable source of contract obligations and operations that affect such contract.
2. Strict relative ordering of events, as it is key that contract clauses are executed in the order stated.
3. Deterministic execution of programs, to make sure that given a particular contract and a set of events occurring in a particular order, the state and outcome of the contract should be the same.
4. Support digital signatures, to support authorship of the operations that affect the contract (such as issuing it, signing it, and operating on it).

In this regard, Blockchain is a suitable technology to automate contracts. This was the case since the dawn of this technology in Bitcoin.

3.1.1 A brief description of the technical nature of blockchain in smart contracts

The operational architecture of smart contracts presents two attributes:[20] 1) value and 2) state. The operational structure of these devices is structured on an *if – then* architecture. In this sense, these platforms function on previously established and agreed terms, which are later submitted to the blockchain network in the form of transactions. Each and every transaction is dependant to one or more secrets linked to the identities of the parties of the contract and all parties must recognize such links. Once the transactions are broadcasted via P2P network, they are analysed and confirmed by the miners and, eventually, placed on a particular

18 I. GRIGG, *Financial cryptography in 7 layers*. In *International Conference on Financial Cryptography*, Springer, 2000, p. 332-348.

19 I. GRIGG, *Financial cryptography in 7 layers*. In *International Conference on Financial Cryptography*, Springer, 2000, p. 332-348.

20 S. WANG, OUYANG, L. YUAN, Y. NI, X. HAN, & F. Y. WANG, *Blockchain-enabled smart contracts: architecture, applications, and future trends*, in *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* 49(11), 2019, p. 2266-2277.

block. The parties involved in the contract received the returned parameters, after this, users can invoke a contract by sending a transaction. The transaction is verified by miners who operate through the system's incentive mechanism. Particularly, after the miners receive the "contract creation" transaction or invoking transaction, they register contract or execute contract code. If the conditions are properly fulfilled, the response actions are executed. After an additional validation, this transaction is located into a new block that is added to the blockchain after the whole network has reached a consensus. So, basically, the only way that the smart contract state can change is as a consequence of one or more transactions. This means that smart contracts cannot change its state as effect of externalities. Examples of externalities desirable to affect the state of a contract include the passing of time, information from external sources (such as commodity or forex prices, occurrence of events) or changes of states in other smart contracts.

For a smart contract to interact with the reality, it requires a component that allows translating events in the real world to blockchain transactions that effect the smart contract. This component is referred to it as an *oracle*. There is a taxonomy of oracles,[21] but here there will be noted that oracles can be inbound (allowing a change in the smart contract state as consequence of an externality) or outbound (allowing the smart contract to trigger a real world action as a consequence of a change in the smart contract state).

The operational structure of smart contracts aims to replicate elements contained on their physical counter parts. Nonetheless, this is not always a welcomed feature, particularly for lawyers. For example, a smart contract that operates within parties that no longer wish to be remained legally bonded may still cause legal obligations. Naturally, the response proposed by developers is to generate a "termination button", which would operate if and only if certain requirements are established by the parties prior the beginning of its operation. What remain as a complex task yet to be solved, is how to deal with unforeseen events that occur and have a direct effect on the original object for which the contract was originally conceived.

3.1.2 Blockchain platforms used for smart contracts

Bitcoin, as defined in the original protocol, is a suitable and scalable platform for the negotiation, deployment and execution of private yet publicly auditable smart contracts. These characteristics make it an attractive option to complement smart contracts, allowing them to operate dynamically, efficiently and in a law compliant manner. Its scripting language allows for the implementation of state machines that

[21] See: S. VOSHMGIR. *What Is the Token Economy?*. In *O'Reilly Media, Incorporated*. 2019.

track the states of individual clauses within a contract, and the state of the contract at large. It allows the registration not only of the code of the smart contract, but also its related natural language legal counterpart.[22] This delivers a suitable feature already mentioned on this article: the compatibility between natural language and programming.

A disadvantage of Bitcoin as a component of smart contracts, is that the toolchain (defined as the set of tools that the developers of smart contracts require to program, interact and monitor) is not as mature as in other platforms. Many smart contracts dealing with tokens are developed on Ethereum. This platform operates as a transaction-based state machine: it starts with genesis states and, as it executes transactions it morphs into some final states.[23] Additionally it operates on accounts, which can be classified as follows: 1) externally owned accounts (EOA) and contract accounts. The differences between these two is that the first classification operates on private keys without code associated with them, whereas the second one operates on contract code associated with associated code.

Transactions can only be initiated through EOAs and it can include Ether (the cyber coin of Ethereum or binary data (payload). After this the management process begin until miners finally verify the proper structure of the contract. Relevantly, all interactions with the Ethereum public blockchains are subject to fees, which are covered on gas.[24] This, with the intention of avoiding unnecessary network abuse and other potential problems. The major disadvantage of Ethereum as a platform for smart contracts are scalability issues proper of its architecture and the fact that once, the controllers of such platform performed a rollback of a transaction (the DAO incident).[25] Another platform to develop smart contracts is Hyperledger Fabric. Hosted by the Linux Foundation, it is not a blockchain developing platform but a Distributed Ledger Technology. It operates on a private approach, which restricts access to it only to membership holders. This network is developed and maintained by contributions made by peers belonging to different groups within this organization. In this sense, these peers are hosts for ledgers and chaincodes (smart contracts). The ledger is structured as a sequence, unmodifiable record of transactions and/or state of transitions. Every transaction is turned into a set of asset-key value parties that are committed to the ledger as they create, update or delete. The operative approach of the Hyperledger Fabric is composed of three phases:

22 WRIGHT, C.S. Turing Complete Bitcoin Script White Paper. *SSRN* n. 3160279.
23 WANG, S.; OUYANG, L.; YUAN, Y.; NI, X.; HAN; WANG, F. Y, *op. cit.* p. 2268.
24 WOOD, G. Ethereum: a secure decentralised generalised transaction ledger Shangai Version. 47e97f5 – 2024-08-26. *Ethereum & Parity*, 2018, available at: https://ethereum.github.io/yellowpaper/paper.pdf, last access on the 27th of August 2024.
25 COPPOLA, F. *Ethereum's DAO Hacking Shows That Coders Are Not Infallible*, 2016.

1. Proposal: In this phase, an application sends a transaction request to other peers. This is basically the request to read and/or write on a particular ledger. It is here where the running of the chain code will be executed.
2. Packaging: Here, the identity of the enforcer is confirmed through a process of signature analysis. After the previous is confirmed, it presents a proposal to modify or update the ledger. The ordering service sorts the transactions received from the network and packages batches of transactions into a block ready for distribution back to all peers connected to it.
3. Validation: The peers connected to the ordering service validate every transaction inside a specific block to confirm whether it has been properly endorsed by the validation requirements established by the organization's policy. After this process, every peer adds the block to the chain, updating the entire structure.

Some disadvantages of using Hyperledger as a platform for smart contracts is the lack of external auditability and the lack of a single source of truth across different implementations. The most evident difference between these developing platforms is their nature: Bitcoin and Ethereum are public blockchain platforms, while a Hyperledger Fabric implementation is private in nature where only a set of previously accepted users can participate. Another difference relies on the fact that in Hyperledger Fabric there is no cyber currency. As part of this, it only defines a set of assets, which are presented as key–value pairs, and provides the functions for operating on the assets and changing their states. Lastly, in relation to contract execution, unlike Ethereum, it is hosted by peer nodes. After a transaction is created, it is only executed and signed by specific peers. Overall, regardless the apparent opposition of these developing platforms, it is important to mention that collaboration between these two developing platforms is becoming more common.

4 Code is (contractual) law?

To this point, this paper has argued that there is yet no definitive method to properly translate natural language (in which the law is expressed) to programming code. This may lead to unforeseen yet legally important situations that may jeopardize the positions of the parties involved in the contract. To properly understand this scenario, one of the most important positions is presented by Larry Lessig in his "code is law approach", This allows technology and the law to be suitably combined by stating that technological artefacts can be embedded with values that constrain the volume of actions performable on them.[26] Nonetheless, there is a large

[26] LESSIG, L. Code is law. *Harvard Magazine*, 2000.

discussion of how this should be implemented.[27] Largely, software developers may implement one of two approaches: they either mirror a section of the law, which in turn may lead to an unnecessary demand of technical resources. The second, to design the operational after a particular legal provision, which in contrast may lead to over simplistic representations of the law. Inevitably, this leads us to Blockchain technology and smart contracts. Unlike other areas of law, traditional contracts are based upon of the convergence of the will of the parties to obtain the realization of a given object.

Smart contracts reduce traditional contractual relations to code-whereby clauses that are automatically enforced after pre-programmed conditions are met. To ensure security, these developments operate through a decentralized storage transaction approach, which decreases the chances of data corruption or lost. The notion of bounding the wills of the parties through technology has been subject of research and development for the digital industry long before the arrival of what we now call smart contracts. Consequently, this technology should be addressed as an evolution of the interaction between the law and technology instead of a new contribution. It is because of their dynamic nature that the proposal to provide them with the capacity of properly represent the law through computational code is a necessary feature.

4.1 How code is (contract) law

As mentioned in upper lines, computational code is suitable of representing legal provisions in technological devices, such as smart contracts. These are key elements that, if properly programmed, would allow these devices to deliver lawful compliance, based on a particular jurisdiction, according to the characteristics of the scenario. In this paper, this representation will be addressed in the following section from the perspective of the US and Mexican contract law in relation to sales contract. The Mexican Federal Civil Code states in its article 2248 that: “there will be a sales contract when one of the parties commits to transfer the property or a particular right of a thing to another, whom in turn commits to pay a price certain and in money.”

This provision can be represented in legal logical terms as:

a = seller

b = buyer

c = good

[27] WU, T. When code isn’t law. *Virginia Law Review*, 2003

```
if a offers_goodproperty_in_money c
    b (agrees=c)
    b (acquires_goodproperty=c)
    else
    b not(aquires_goodproperty=c)
End if
```

This representation contains three elements presented on the Mexican Federal Civil Code: the seller, the buyer and the thing object of the contract. It establishes that the seller offers a thing in a certain priced that must be agreed by the buyer. Once this has been met, the contract executes its effects.

From the perspective of the United States Jurisdiction, the Uniform Commercial Code states on its article 2 section 106: "Contract for sale" includes both a present sale of goods and a contract to sell goods at a future time. A "sale" consists in the passing of title from the seller to the buyer for a price. Due to its legal structure, it can be logically expressed in the same way as its Mexican counter part. Notably, this results compatible with The New Agreement between the United States of America, the United Mexican States, and Canada (USMCA).[28]

```
a = seller
b = buyer
c = good
if a offers_goodproperty_in_money c
    b (agrees=c)
    b (acquires_goodproperty=c)
    else
    b not(aquires_goodproperty=c)
End if
```

Notably, both legal logic expressions hold a notable degree of similarity, which allows them to be represented in practically identical terms This is a relevant feature in terms of software development and certainty for the parties, regardless of the jurisdiction they are from.

A technical expression compatible with these legal provisions is presented in the following lines:

```
/******* Payment state machine **********/
Var contract = <natural language contract>
Var buyer = <buyer identity>
Var seller = <seller identity>
```

[28] United States Trade Representative, Office of, "*Agreement between the United States of America, the United Mexican States, and Canada 12/13/19 Text*", available at: https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between

```
Var goods = [ <object description 1>, <object description 2> ]
Var total_price = <total price>
Var escrow = <nul>
Var delivery_time = <time of delivery>
Var contract_state = <init> //init, partially accepted, fully accepted, done
Var payment_state = <none> //none, init, buyer_to_escrow, escrow_to_seller,
escrow_to_buyer, done)
Var buyer_signature = <buyer signature>
Var seller_signature = <seller signature>
Var evidence_tracking_number = <nul>
/******* Sales contract expression **********/
If (buyer_signature XOR seller_signature) contract_state = partially_accepted
If(buyer_signature AND seller_signature) {
contract_state = fully_accepted
payment_state = init
If (payment_state == done) contract_state = done.
/******* Payment state machine, executed in case **********/
input: buyer_payment, seller_tracking_number, buyer_accepts_goods, buyer_
rejects_goods
output: send_goods_command, return_payment, deliver_payment
if (payment_state == init) SEND payment_instructions TO buyer
ON buyer_payment:
Escrow = buyer_payment;
SEND send_goods_command TO seller
ON tracking_number:
Evidence_tracking_number = tracking_number
ON buyer_accepts_goods:
SEND escrow TO seller
ON buyer_rejects_goods:
SEND escrow TO buyer
```

4.2 Traditional contract law and smart contracts: a new boundary?

To this point it has been shown that the increasing adoption of smart contracts generates concerns to the traditional legal sector. Besides an adequate representation of legal terms, transjurisdictional scenarios have been raised serious concerns. In relation to this, to Savelyev (2017), the main problem relies in the technical approach implemented to develop smart contracts, which lacks a proper degree of participation from legal experts. This leads to the development of platforms with a

limited version of the law thus, compromising legal certainty. Additionally, some of the following issues are presented in projects where and leading to the following issues:[29]

- Smart contracts do not generate legal obligations
- Vitiated consent cannot be plead in smart contracts
- Smart contracts are egalitarian platforms
- The duality of smart contracts: potential illegal uses

In the following section the adoption of smart contracts will be addressed from the perspective of international jurisdictions.

5 Smart contracts and international legal frameworks: an ongoing relation

Smart contracts have raised the attention of the legal community since its very first conception back in 1996. Many positions have presented both, positive and negative aspects related to the potential consequences of this technology. However, it was during the 2016 attack when this technology reached its peak when a hacker stole 3.6 million Ether (the currency used on the Ethereum platform) from the Ethereum's Decentralised Autonomous Organisation (DAO). Shortly after this was reported, a statement was released claiming that the amount would be recovered thus, minimizing the risk for investors. Nonetheless, this led to questions about the composition of smart contract since, as it was stated by the cracker and later confirmed by DAO forensic experts, this was the result of self-executing transactions and it was not committed through traditional illegal actions.[30]

Regardless of this, the implementation of Blockchain has expanded in many markets. For example, in the US it is expected that by 2025 such growth will be worth around US$41-US$60bn. Parallel to this, it is also expected the arrival of new legislations at local and federal levels, which will have an impact on this market bringing certainty and increasing its adoption rates. In relation to the legal aspect, one of the most relevant provisions was presented in the state of Wyoming in 2019. This contained 13 Blockchain-enabling laws that provided property rights to users and creators and offered regulatory relief (Spindler 2019).[31] Arizona joined the regulatory effort by taking some the initiatives presented by Wyoming and keeping close collaboration with the technologic sector. Nevertheless, there are very few

29 DUGGAL, P. Blockchain Contracts & Cyberlaw. *New York,* 2015.

30 STEEMIT, *An Open Letter to the DAO and the Ethereum Community,* available at: https://steemit.com/ethereum/@chris4210/an-open-letter-to-the-dao- and-the-ethereum-community.

31 C. LONG, *What Do Wyoming's 13 New Blockchain Laws Mean?*, available at: www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean.

provisions directly related to smart contracts. This, since legislation perceives them merely as an extension of Blockchain development.

In relation to the European Union, there are two legal measurements currently being discussed, first, the Directive 2000/31/EC on e-commerce and second, the Consumer Rights Directive 2011/83/EU. If these two are passed, they will deliver provisions related to the formation of contracts on the Internet. For example, they would require pre-contractual obligations for a trader in e-commerce consumer contracts in the form of informing the consumer about relevant facts, which could be interpreted as also containing certain information about security vulnerabilities of smart contracts. In addition to this, the General Data Protection Regulation (GDPR) should also have a relevant role in the design and implementation of smart contracts. Latin American jurisdictions are also in the process of adapting their legal framework to the arrival of this technology. In the particular case of Mexico, the development of the Law to Regulate Institutions of Finance Technology provides relevant starting point towards the lawful and certain use of this type of technology. Regardless the fact smart contracts are not expressly contained on this law, they fall within the figure of "Novelty Models". These are required to establish all the necessary arrangements to facilitate the interaction between users and technological developments. In other words, authorities are allowed to keep a close contact with the organizations developing this technology to avoid the creation of unlawful implementations. In relation to Blockchain, the term is not properly mentioned on the law. However, the section related to "digital assets" is configured in such a manner that can be addressed as a manifestation of this technology. Digital technology presents a constant challenge for international jurisdictions. In the particular case of smart contracts, legal frameworks around the world are currently on the process of designing a legal figure suitable to regulate the activities derived from the adoption of these developments. Nonetheless, the development of legal figures to regulate smart contracts should be performed taking in consideration the principle of legal harmonisation. This will increase the level of success of law enforcement strategies, delivering legal protection to law abiding users regardless of their geographical location.

5.1 Smart contracts, blockchain and international legal framework

One of the areas that is expected to receive the impact of smart contract technology is, without a doubt, international trade. This, as result of some of the following reasons:[32] international companies are increasingly accepting virtual

[32] BALLY, G. *Cryptocurrencies accepted by Switzerland's biggest online retailer*, available in https://www.swissinfo.ch/eng/bitcoin-or-cash_cryptocurrencies-accepted-by-switzerland-s-biggest-online-retailer/44835480

currencies as a form of payment, blockchain offers not only a significantly smaller fees but also safer transactions. This has led us to a new scenario where decentralized relations and application present themselves as new challenges for the legal framework. In fact, this has already taking place: Ethereum provides an approach where third parties are no longer required and (smart) contracts can produce their effects in a more efficient manner. Speaking from a purely legal perspective, there is no global consensus of how smart contracts should be regulated on an international level, however, it seems to be a general consensus on three main elements[33] 1. Payment/exchange/currency tokens (virtual currencies or cryptocurrencies), 2. Investment tokens, and 3. Utility tokens. Within this scenario, this paper aims to fulfil this gap by allowing a representation that results compatible with the jurisdictions presented on the previous section. To achieve this, through the use of a logical description, legally relevant terms will be translated into a computational from that suits legal requirements from the positions of the parties.

6 Code is not perfect

The technical nature of the Blockchain and its relation with Smart Contracts presents challenges on different steps, which include development, deployment, updates, arbitration and interaction with reality of such Smart Contracts. This section will overview such challenges.

6.1 Potential issues in the lifecycle of a smart contract

The following are the issues that have been identified per type within the lifecycle of a smart contract.

A. Defects of origin. This type of issues appears when the law or the source legal contract has a defect, which can be: contradiction, de-harmonization of the contract with the body of law and lack of consideration to different scenarios, amongst others. The consequences of defects are the same for any traditional Legal Contract in this situation (mainly high contractual risks, litigation costs, etc).
B. Defects in the Logical Abstraction process: Wrongly identifying actionable clauses, sub-optimally selecting actionable clauses for automation, errors in the logic abstraction of clauses, lack of consideration of the properties and limitations of the underlying technology (i.e. oracles).
C. Defects in the Smart Contract. Those are the defects not found in the validation phases.

[33] EUROPEAN COMISSION, *Legal and regulatory framework of blockchains and smart contracts thematic report*, available at: EUBlockchain, 2019.

D. Defects in the Smart Contract's dependencies. Examples of these are defects in external libraries, compilers, debuggers or applications of the toolchain.
E. Defects in the Smart Contract's Platform (SCP). Examples of these are problems in the deployment of the contracts or problems in the upgrading of the contracts.
F. Defects in the inbound or outbound oracles. Examples of these are downtime, erroneously serving information, wrongly executing actions.
G. Defects in the Oracles' dependencies. These are mainly due to downtime of the underlying mechanisms, such as payment service suppliers.

Consequences of critical severity are a potential outcome of the defects B, C, D, E, F and G, because they can cause the Smart Contract system to behave differently than the agreed legal contract, thus, increasing contractual risks and potentially, litigation costs. There could also be minor severity consequences in defects D, E, F and G, which could cause a delay in the actions as consequences of the Smart Contract's logic.

6.2 Proposal for the development of a technical process for smart contracts

The roles involved in the proposed development process of a Smart Contract are: Legal Contract Writer (LCW), Smart Contract Developer (SCD), Logical Abstraction Technical Lawyer (LA), Smart Contract Tester (SCT), Smart Contract Platform (SCP) and Oracles (O).

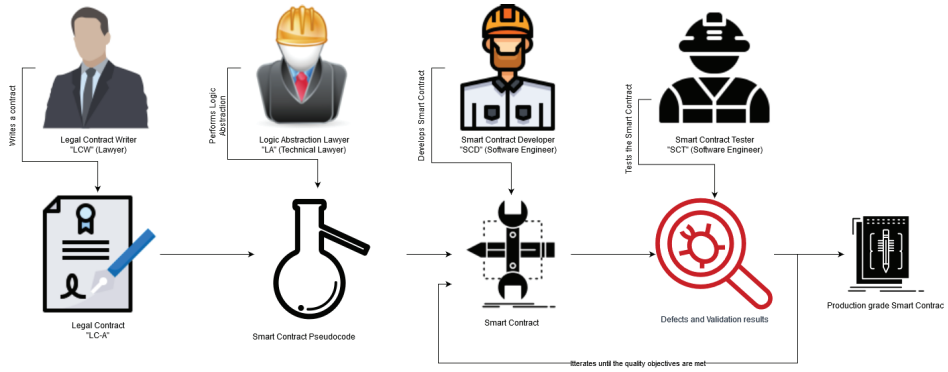

Figure 1: describes the Smart Contract development process.

The development process of a Smart Contract starts with a Legal Contract. Assuming that there is already a natural language, jurisdictionally bound Legal Contract "LC-A", it will be the trigger for the process of development of a Smart Contract. It is important that this process starts with the definition of the Legal

Contract, because it can use the standard mechanisms in place for validation and harmonization processes (which could include peer reviews), to reduce the risks associated with contracting. Once the legal contract "LC-A" is developed, a process of logic abstraction is started. The purpose of this process is to determine which clauses are declarative and which are actionable, then select which actionable clauses will be automated. Once the particular subset of actionable clauses subject to automation are identified, the LA role abstracts the logic on each of them. This is a critical part of the Smart Contract development. Since all the automatable actions are identified, selected and implemented here, careful consideration must be taken to ensure that harmonization with existing laws and jurisprudence, in order to reduce the contractual risks. In this process, it is also imperative that the LA role takes into consideration the limitations of the underlying technology *as a whole*, not just the blockchain part, but also its interactions with external libraries, oracles, action mechanisms, and inputs of information. Even though careful consideration is required, it is possible that errors are injected in the logic abstraction of the Legal Contract. The outcome of the Logic Abstraction process is a pseudocode of the Smart Contract, which holds the business rules to be implemented as a Smart Contract. The next step of this to actually write the Smart Contract. This process is executed by the SCD role and takes the Smart Contract pseudocode generated by the LA and implements it. To take a pseudocode and implement it as an executable code, there are different cognitive and technical decisions to be defined such as:

- Which data types should be used?
- How to properly organize the data structure of the Smart Contract?
- Which programming language (in case that options are available) should be used?
- Does the Smart Contract require external libraries?

It is important to mention that in Software Development, error injection is unavoidable and there is no way to guarantee a bug-free software (when not using formal methods). The outcome of this process is an executable code of the Smart Contract, which is tied to a particular platform and corresponds to the pseudocode generated by LA. The next step in the process is the validation of the Smart Contract. This step is performed by the SCT role. Although it is possible that both the SCD and SCT roles lay within the same person, it is highly recommended that the SCT's activities in this step is performed by a different person. The activities of this step is to formally validate the Smart Contract, taking as its specification the pseudocode. This activity involves the creation of a testing plan, test cases and validation reports. It is imperative to achieve 100% code coverage during the validation phase, to ensure that even the more conspicuous situations are validated. The outcome of this phase is a validation report detailing the functional and non-functional characteristics of the performance of the Smart Contract, plus the set of defects found. It is important to

note that a lack of defects does not mean that the Smart Contract code is error free, and more often than not, it means that the validation phase was not as stringent as required. This may also contribute to properly detect the lack of compatibility between the legal logic expression of the law and its computational counterpart.

The Smart Contract development and validation phases should iterate, so the SCD role can fix the defects found by the SCT. Once a quality objective has been reached, the Smart Contract code "SC" is ready for production. However, as previously stated, the Smart Contract is self-contained. For it to be truly an automation of its Legal Counterpart, it must interact with reality.

These interactions might include:

1. Interaction with the parties of contract, to assert their will on different parts of the process.
2. Interactions with external sources of information, for instance, to receive information on event referenced in the smart contract.
3. Interactions with external actuators, for instance, to trigger a payment, a delivery of a good or service, to grant access to an intelligent lock, etcetera.
4. Interaction with an external arbiter.
5. Interactions with external authorities (e.g. Tax Institutions, AML Institutions).

In order to connect the "SC" and make it fully functional, such "SC" must be connected to an existing platform "SCP" that allows such connections and a new validation phase to begin: Integration Testing. Such smart contract platform "SCP" can be in house or an external service provided by a third party. The Integration Testing and System Validation must occur with SCD, SCT and SCP, across several iterations, to fix any defect found on the Smart Contract and/or the oracles. Once the system validation is completed, the Smart Contract is fully functional and can be deployed.

7 Conclusions

Smart contracts offer not only the capacity to operate on digital platforms but are also developments capable of adapting their behaviour based on cognitive features. This, by integrating the developing and legal process through an approach that substantially reduces the chances of presenting technical errors. The impact of this is both, legal and technological sound. In the first case, it brings legal certainty to the parties involved, reducing potential litigations due to the mistranslation of the legal clauses. In the second case, it increases the impact on the market by making smart contracts a reliable product, suitable of delivering legal compatibility. Overall, the presented process delivers a novel process of reasoning without reducing technical efficiency, allowing compatibility with digital dynamic scenarios. Finally,

this contribution aims to encourage further research into the development legal technological solutions for digital scenarios and to provide compatibility among different jurisdictions.

References

ALHARBY, M.; VAN MOORSEL, A. *Blockchain-based smart contracts: A systematic mapping study*, in *International Conference on Cloud Computing, Big Data and Blockchain (ICCBB),* 2018, p. 2.*Conference on Cloud Computing, Big Data and Blockchain (ICCBB),* 2018.

BALLY, *Cryptocurrencies accepted by Switzerland's biggest online retailer*, available in https://www.swissinfo.ch/eng/bitcoin-or-cash_cryptocurrencies-accepted-by-switzerland-s-biggest-online-retailer/44835480

CLACK, C. D.; BAKSHI, V. A.; BRAINE, L. *Smart contract templates: foundations, design landscape and research directions*, in *Cornell University,* 2017.

COPPOLA, F. *Ethereum's DAO Hacking Shows That Coders Are Not Infallible*, 2016.

DUGGAL, P. *Blockchain Contracts & Cyberlaw*, in *New York,* 2015.

EUROPEAN COMISSION, *Legal and regulatory framework of blockchains and smart contracts thematic report*, in EUBlockchain, 2019.

GOVERNATORI, G.; IDELBERGER, F.; MILOSEVIC, Z.; RIVERET, R.; SARTOR, G.; XU, X. On legal contracts, imperative and declarative smart contracts, and blockchainsystems, in *Artificial Intelligence and Law 26 (4),* 2018.

HVITVED, T. "Contract formalisation and modular implementation of domain-specific languages", in *Doctoral dissertation, PhD thesis, Department of Computer Science, University of Copenhagen*, 2011.

LADLEIF, J.; WESKE, M. *A Unifying Model of Legal Smart Contracts*, in *International Conference on Conceptual Modeling Springer,* 2019.

LESSIG, L. *Code is law*, in *Harvard Magazine*, 2000.

LONG, C. *What Do Wyoming's 13 New Blockchain Laws Mean?,* available in: www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean.

MADIR, J. *Smart Contracts (How) Do They Fit Under Existing Legal Frameworks?,* 2018.

STARK, J. *Making sense of blockchain smart contract*, in *coindesk,* https://www.coindesk.com/making-sense-smart-contracts.

STEEMIT, *An Open Letter to the DAO and the Ethereum Community*, in https://steemit.com/ethereum/@chris4210/an-open-letter-to-the-dao-and-the-ethereum-community.

SWAN, M. *Blockchain: Blueprint for a new economy*, in *O'Reilly Media, Inc.* 2015.

SZABO, N. *Formalizing and securing relationships on public networks*, in *First Monday,* 1997.

United States Trade Representative, Office of, "*Agreement between the United States of America, the United Mexican States, and Canada 12/13/19 Text"*, in https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between

VOSHMGIR, S. What Is the Token Economy? In *O'Reilly Media, Incorporated.* 2019.

WANG, S.; OUYANG, L.; YUAN, Y; NI, X; HAN; WANG, F. Y. Blockchain-enabled smart contracts: architecture, applications, and future trends, in *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* 49(11), 2019.

WOOD, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger Shanghai Version 47e97f5 – 2024-08-26. *Ethereum & Parity,* 2018, available at: https://ethereum.github.io/yellowpaper/paper.pdf, last access on the 27th of August 2024.

WRIGHT, C.S. *Turing Complete Bitcoin Script White Paper*, in SSRN 3160279.

WU, T. When code isn't law. *Virginia Law Review*, 2003.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

NIEBLA ZATARAIN, Jesus Manuel; ONTIVEROS VÁZQUEZ, Paola Jackeline. Smart contracts: the new method of interaction between the law and technology. *International Journal of Digital Law*, Belo Horizonte, ano 5, n. 2, p. 103-123, maio/ago. 2024. DOI: 10.47975/digital.law.vol.5.n.2.niebla.

Informações adicionais

Additional information

Sobre a Revista

IJDL – INTERNATIONAL JOURNAL OF DIGITAL LAW

Objetivo

O International Journal of Digital Law é um periódico científico eletrônico de acesso aberto e periodicidade quadrimestral promovido pelo **Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano (NUPED), do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná**.

O Conselho Editorial é composto por renomados professores vinculados a instituições de ensino superior do Brasil, Argentina, Austrália, Colômbia, Espanha, Egito, França, Holanda e Índia. A linha editorial segue o eixo das atividades de pesquisa do NUPED, um grupo inscrito no diretório do CNPq e filiado à **Rede de Pesquisa em Direito Administrativo Social (REDAS)**. Seu enfoque é o estudo crítico das instituições jurídico-políticas típicas do Estado de Direito, notadamente as voltadas à inovação e ao desenvolvimento humano por intermédio da revolução digital.

Linha Editorial

A linha editorial segue o eixo de concentração do **NUPED – PPGD/PUCPR** intitulada "**Direito Econômico e Desenvolvimento**". Por sua vez, a área congrega duas importantes linhas de pesquisa: 1. **Estado, Economia e Desenvolvimento** e 2. **Direitos Sociais, Globalização e Desenvolvimento**. A revista dará destaque a este marco teórico. Entretanto, transversalmente ao tema da economia, do desenvolvimento, da globalização e dos direitos sociais, as palavras-chave que melhor definem o escopo da revista implicam a tratativa de temas como: acesso à informação, *big data*, *blockchain*, cidades inteligentes, contratos inteligentes, *crowdsourcing*, cibercrimes, democracia digital, direito à privacidade, direitos fundamentais, *e-business*, economia digital, educação digital, eficiência administrativa, e-*government*, *fake news*, *gig economy*, globalização, inclusão digital, infraestrutura, inovação, inteligência artificial, interesse público, internet, internet das coisas, jurimetria, *lawfare*, novas tecnologias, perfilamento digital, pesquisa em multimeios, processo administrativo eletrônico, proteção de dados, regulação administrativa, regulação econômica, risco, serviços públicos, sistemas de informação, sociedade da informação, transparência governamental e telecomunicações.

Double blind peer review

A publicação dos artigos submete-se ao procedimento *double blind peer review*. Os trabalhos são remetidos sem identificação de autoria a dois pareceristas *ad hoc* portadores de título de doutor, todos eles exógenos à instituição promotora da revista (PUCPR). Os pareceristas são, portanto, sempre pesquisadores vinculados a renomadas instituições de ensino superior nacionais e estrangeiras.

Cobertura temática (classificação do CNPq)

GRANDE: Ciências Sociais Aplicadas (6.00.00.00-7)/Área: Direito (6.01.00.00-1)/ Subárea: Direitos Especiais (6.01.04.00-7)

GRANDE: Ciências Sociais Aplicadas (6.00.00.00-7)/Área: Ciência da Informação (6.07.00.00-9)/Subárea: Teoria da Informação (6.07.01.00-5)

GRANDE: Ciências Exatas e da Terra (1.00.00.00-3)/Área: Ciência da Computação 1.03.00.00-7/Subárea: Sistemas de Computação (1.03.04.00-2)

Diretrizes para Autores

1. Submissão de artigos
As propostas de artigos para publicação na *International Journal of Digital Law* deverão ser enviadas através do sistema eletrônico de submissões (gratuitamente), por meio de cadastro no Sistema Eletrônico e acesso mediante login e senha a ser realizado no site. Não serão aceitas propostas enviadas por e-mail. A revista reserva-se o direito de aceitar ou rejeitar qualquer original recebido, de acordo com as recomendações do seu corpo editorial, inclusive por inadequação da temática do artigo ao perfil editorial da revista, como também o direito de propor eventuais alterações.

2. Qualificação dos autores
Ao menos um dos autores do artigo deverá possuir o título de Doutor (Dr.), Doctor of Juridical Science (J.S.D. ou S.J.D.), Doctor juris (Dr. iur. ou Dr. jur.), Doctor of Philosophy (Ph.D.) ou Legum Doctor (LL.D.). A exigência poderá ser relativizada, nunca extrapolando o percentual de 30% por edição, em casos excepcionais de: (i) artigos de autores afiliados a instituições estrangeiras; (ii) artigos escritos em inglês.

3. Ineditismo e exclusividade
Os textos para publicação na *International Journal of Digital Law* deverão ser inéditos e para publicação exclusiva, salvo no caso de artigos em língua estrangeira que tenham sido publicados fora do país. Uma vez publicados nesta revista, também poderão sê-lo em livros e coletâneas, desde que citada a publicação original. Roga-se aos autores o compromisso de não publicação em outras revistas e periódicos, bem como de que as propostas de artigo não se encontrem postulados de forma simultânea em outras revistas ou órgãos editoriais.

4. Idiomas
Podem ser submetidos artigos redigidos em Português, Espanhol ou Inglês.

5. Cadastro dos metadados no sistema eletrônico de submissões
5.1. No momento da submissão do artigo no sistema eletrônico, os campos dos metadados deverão ser preenchidos obrigatoriamente de acordo com estas diretrizes, sob pena de rejeição liminar da submissão.
5.2. Autores
5.2.1. *Nome/Nome do Meio/Sobrenome:* indicação do nome completo do(s) autor(es) apenas com as iniciais de cada nome em caixa alta. Em caso de artigos em coautoria, os nomes de todos os coautores devem ser inseridos no sistema na ordem que deverá constar no momento da publicação.
5.2.2. *E-mail:* indicação do e-mail do(s) autor(es) para contato, que será obrigatoriamente divulgado na versão publicada do artigo.
5.2.3. *ORCID iD:* indicação do número de identificação ORCID (para maiores informações clique aqui). O identificador ORCID pode ser obtido no registro ORCID. Você deve aceitar os padrões para apresentação de iD ORCID e incluir a URL completa; por exemplo: https://orcid.org/0000-0003-1781-1726.

5.2.4. *URL:* link para o currículo completo do autor. No caso de autores brasileiros, deve ser indicado o link para o Currículo Lattes.
5.2.5. *Instituição/Afiliação:* indicação da sua principal afiliação institucional ou das duas principais, caso o vínculo com ambas possua a mesma importância (instituição à qual encontra-se vinculado como docente ou discente, ou, caso não seja docente ou discente, a instituição onde foi obtido o seu maior título acadêmico, como doutorado, mestrado, especialização etc.). O nome da instituição deverá constar por extenso e na língua original da instituição (ou em inglês quando a escrita não for latina), seguida da indicação do país de origem da instituição entre parênteses. Caso o autor seja docente e esteja cursando mestrado ou doutorado em outra instituição, a afiliação principal será a da instituição na qual o autor figura como mestrando ou doutorando.
5.2.6. *País:* indicação do país da principal afiliação institucional do autor.
5.2.7. *Resumo da biografia:* indicação do mini currículo, iniciando com a indicação da instituição onde figura como docente, seguida de cidade, sigla do Estado e país entre parênteses, indicação das titulações acadêmicas (começando pela mais elevada), outros vínculos com associações científicas, profissão etc.
5.3. Título e Resumo
5.3.1. *Título:* título no idioma do artigo, com apenas a primeira letra da sentença em maiúscula.
5.3.2. *Resumo:* resumo no idioma do artigo, sem parágrafo ou citações e referências, com até 200 palavras.
5.4. Indexação
5.4.1. *Palavras-chave*: indicação de 5 palavras-chave no idioma do artigo (em letras minúsculas e separadas por ponto vírgula).
5.4.2. *Idioma*: indicar a sigla correspondente ao idioma do artigo (Português=pt; English=en; Español=es).
5.5. Contribuidores e Agências de fomento: os artigos resultantes de projetos de pesquisa financiados deverão indicar neste campo a fonte de financiamento.
5.6. Referências: inserir a lista completa de referências citadas no artigo, dando um espaço entre cada uma delas.

6. Apresentação do texto e elementos pré-textuais
6.1. Recomenda-se que o trabalho tenha entre 15 e 30 páginas (tamanho A4 – 21 cm x 29,7 cm), compreendendo a introdução, desenvolvimento, conclusão (não necessariamente com esses títulos) e uma lista de referências bibliográficas.
6.2. As margens utilizadas deverão ser: esquerda e superior de 3 cm e direita e inferior de 2 cm.
6.3. No corpo do texto deverá ser utilizada Fonte Times New Roman, tamanho 12, espaçamento entre linhas de 1,5 cm e espaçamento de 0 pt (pontos) antes e depois dos parágrafos.
6.4. Nas notas de rodapé deverá ser utilizada Fonte Times New Roman, tamanho 10, espaçamento simples entre linhas.
6.5. No desenvolvimento do texto, os parágrafos deverão conter recuo de 1,5 cm em relação à margem esquerda. Títulos e subtítulos deverão estar alinhados à margem esquerda, sem recuo.
6.6. A estruturação deverá observar a exposta neste item 6.6.

6.6.1. Título no idioma do artigo, com apenas a primeira letra da sentença em maiúscula e em itálico, centralizado.
6.6.2. Nos casos de necessidade de indicar informações a respeito do artigo (financiamento por agências de fomento, agradecimentos, tradutores do texto etc.), deverá ser inserida uma nota de rodapé com um asterisco (e não com número) situada à direita do título no idioma do artigo.
6.6.3. Título em inglês, com apenas a primeira letra da sentença em maiúscula, em itálico e centralizado. No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelo título em português.
6.6.4. O artigo não deve incluir os nomes do(s) autor(es). As informações, para fins de publicação, serão retiradas dos metadados inseridos pelo(s) autor(es) no sistema eletrônico da revista no momento da submissão.
6.6.5. Resumo no idioma do artigo (fonte Times New Roman 12, espaçamento entre linhas simples, sem parágrafo ou citações e referências, com até 200 palavras), antecedido da palavra "Resumo" escrita no idioma do artigo.
6.6.6. Indicação de 6 palavras-chave no idioma do artigo (em letras minúsculas e separadas por ponto vírgula), antecedidas da expressão "Palavras-chave" redigida no idioma do artigo.
6.6.7. Resumo em inglês (Fonte Times New Roman 12, espaçamento entre linhas simples, sem parágrafo ou citações e referências, com até 200 palavras), antecedido da palavra "Abstract". No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelo resumo em português.
6.6.8. Indicação de seis palavras-chave em inglês (em letras minúsculas e separadas por ponto e vírgula), antecedidas da expressão "Keywords". No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelas palavras-chave em português.
6.6.9. Sumário com a identificação dos títulos das seções e das subseções, com numeração progressiva, separados por ponto vírgula, sequencialmente e em parágrafo único.
6.6.10. Desenvolvimento do trabalho científico: a numeração progressiva, em números arábicos, deve ser utilizada para evidenciar a sistematização do conteúdo do trabalho.
6.6.11. Lista das referências bibliográficas efetivamente utilizadas no artigo, ao final do trabalho, separadas por um espaço simples, alinhadas à margem esquerda (sem recuo).
6.6.12. Aplicam-se, para os demais aspectos de formatação, as normas técnicas brasileiras (ABNT NBR 10520:2002 e 14724:2011).
6.6.13. No caso de artigos com 4 ou mais autores, é necessário incluir uma nota de rodapé indicando qual foi a contribuição de cada um.
6.7. Todo destaque que se queira dar ao texto deve ser feito com o uso de itálico, ficando vedada a utilização de negrito, sublinhado ou caixa alta para fins de dar destaque ao texto.
6.8. Figuras e tabelas devem estar inseridas no texto, e não no final do documento na forma de anexos.

7. Metodologia científica
7.1. As referências dos livros, capítulos de obras coletivas, artigos, teses, dissertações e monografias de conclusão de curso de autores citados ou utilizados como base

para a redação do texto devem constar em nota de rodapé, com todas as informações do texto, em observância às normas técnicas brasileiras (ABNT NBR 6023:2018), e, especialmente, com a indicação da página da qual se tirou a informação apresentada no texto logo após a referência.

7.1.1. O destaque dado ao título dos livros (ou revistas) citados deverá constar em itálico, ficando vedada a utilização de negrito.

7.1.2. Os artigos redigidos com citação no formato AUTOR-DATA não serão aceitos para publicação, somente o sistema de chamadas numérico exposto nas notas de rodapé.

7.1.3. As referências deverão constar da seguinte forma:

7.1.3.1. Livros:

SOBRENOME, Nome. *Título da obra em itálico*: subtítulo sem itálico. número da edição. Cidade: Editora, ano.

Exemplo:

KEEN, Andrew. *Vertigem digital*: por que as redes sociais estão nos dividindo, diminuindo e desorientando. Trad. Alexandre Martins, Rio de Janeiro: Zahar, 2012. 254p.

7.1.3.2. Capítulos de livros coletivos:

SOBRENOME, Nome. Título do capítulo sem itálico. In: SOBRENOME DO 1º ORGANIZADOR, Nome do organizador; SOBRENOME DO 2º ORGANIZADOR, Nome do 2º organizador e assim sucessivamente, separados por ponto vírgula (Org. ou Coord.). *Título da obra ou coletânea em itálico*: subtítulo sem itálico. número da edição. Cidade: Editora, ano. página inicial-página final [antecedidas de "p."].

Exemplo**:**

DOTTA, Alexandre Godoy. Derechos de la Población LGBT+ en Brasil: Vulnerabilidad Social entre Avances y Retrocesos. In: BRAVO, Álvaro Sánches; CASIMIRO, Ligia Melo de; GABARDO, Emerson. (Org.). *Estado Social Y Derechos Fundamentales en Tiempos de Retroceso*. Sevilha: Ponto Rojo, 2019. p. 203-228.

7.1.3.3. Artigos em revistas:

SOBRENOME, Nome. Título do artigo sem itálico. *Título da Revista em itálico*, cidade, volume, número, página inicial-página final [antecedidas de "p."], meses da publicação [abreviados com as três primeiras letras do mês seguidas de ponto e separados por barra]. ano.

Exemplo:

GABARDO, Emerson; SAIKALI, Lucas Bossoni. A prescritibilidade da ação de ressarcimento ao erário em razão de atos de improbidade administrativa. *Revista Jurídica – Unicuritiba*, Curitiba, v. 1, p. 514-543, 2018.

7.1.3.4. Teses de Titularidade, Livre-Docência, Doutorado, Dissertações de Mestrado, Monografias de Conclusão de Curso de Graduação e Pós-Graduação:

SOBRENOME, Nome. *Título do trabalho em itálico*: subtítulo sem itálico. Cidade, ano. número de folhas seguido de "f". Modalidade do trabalho (Grau obtido com a defesa) – Órgão perante o qual o trabalho foi defendido, Nome da instituição.

Exemplo:

SANTOS, Fábio de Sousa. *Análise Comparada da Competição na Contratação Pública Brasileira e Estadunidense*. Curitiba, 2018. 134f. Dissertação (Mestrado em Mestrado em Direito) – Pontifícia Universidade Católica do Paraná. Curitiba: 2018.

7.1.3.5 DOI – Digital object identifier: Caso o documento consultado na pesquisa tenha o número de DOI recomenda-se a inclusão, de modo complementar, do número após o término de cada referência.
Exemplo:
DOTTA, Alexandre Godoy. Public policies for the assessment of quality of the Brazilian higher education system. *Revista de Investigações Constitucionais*, Curitiba, v. 3, p. 53-69, 2016. DOI. 10.5380/rinc.v3i3.49033.
7.1.3.6. Documentos em meio eletrônico: Documentos extraídos do meio eletrônico deverão apresentar após o término de cada referência o local da rede onde foi encontrado e apresentado da seguinte maneira.
Exemplo:
IJDL. International Journal of Digital Law. *Regras para a submissão de artigos*. Disponível em: https://journal.nuped.com.br/index.php/revista/about/submissions. Acesso em: 12 fev. 2020.
7.1.4. Os elementos das referências devem observar o seguinte padrão:
7.1.4.1. Autor: SOBRENOME em maiúsculas, vírgula, Nome com as iniciais em maiúsculas, seguido de ponto final.
7.1.4.2. Edição: deve ser incluída a informação somente a partir da segunda edição, sem ordinal, seguido de ponto e "ed.". Exemplo: 2. ed.
7.1.4.3. Ano: grafado com algarismos arábicos, sem ponto no milhar, antecedido de vírgula e seguido de ponto.
7.1.5. Nos casos em que for absolutamente impossível obter alguma das informações acima, a ausência deverá ser suprida da seguinte forma:
7.1.5.1. Ausência de cidade: substituir por [S.l.].
7.1.5.2. Ausência de editora: substituir por [s.n.].
7.1.5.3. Ausência de ano: indicar entre colchetes o ano aproximado, seguido de ponto de interrogação. Exemplo: [1998?].
7.2. As citações (palavras, expressões, períodos) deverão ser cuidadosamente conferidas aos textos originais.
7.2.1. Citações diretas devem seguir o seguinte padrão de registro: transcrição com até quatro linhas devem constar do corpo do texto, com letra e espaçamento normais, e estar entre aspas.
7.2.2. Recomenda-se fortemente que citações textuais longas (mais de quatro linhas) não sejam utilizadas. Entretanto, se imprescindíveis, deverão constituir um parágrafo independente, com recuo de 1,5 cm em relação à margem esquerda (alinhamento justificado), utilizando-se espaçamento entre linhas simples e tamanho da fonte 10. Neste caso, aspas não devem ser utilizadas.
7.2.3. Fica vedado o uso do op. cit., loc. cit., ibidem e idem nas notas bibliográficas, que deverão ser substituídas pela referência completa, por extenso.
7.2.4. Para menção de autores no corpo do texto, fica vedada sua utilização em caixa alta (ex.: para Nome SOBRENOME...). Nestes casos todas as menções devem ser feitas apenas com a primeira letra maiúscula (ex.: para Nome Sobrenome...).

8. Redação
8.1. Os textos devem ser revisados, além de terem sua linguagem adequada a uma publicação editorial científica.

8.2. No caso de artigos redigidos na língua portuguesa, a escrita deve obedecer às regras ortográficas em vigor desde a promulgação do ACORDO ORTOGRÁFICO DA LÍNGUA PORTUGUESA, a partir de 1º de janeiro de 2009.
8.3. As citações de textos anteriores ao ACORDO devem respeitar a ortografia original.

9. Artigos resultantes de pesquisas financiadas
Os artigos resultantes de projetos de pesquisa financiados deverão indicar em nota de rodapé, situada ao final do título do artigo no idioma do texto, a informação relativa ao financiamento da pesquisa.

10. Declaração de direitos autorais
Autores que publicam nesta revista concordam com os seguintes termos:
10.1. Não serão devidos direitos autorais ou qualquer outra remuneração pela publicação dos trabalhos.
10.2. Autores mantêm os direitos autorais e concedem à *IJDL* o direito de primeira publicação, com o trabalho simultaneamente licenciado sob a Licença Creative Commons Attribution que permite o compartilhamento do trabalho com reconhecimento da autoria e publicação inicial nesta revista. Ainda, em virtude de aparecerem nesta revista de acesso público, os artigos são de uso gratuito, com atribuições próprias, com aplicações educacionais e não comerciais.
10.3. Autores têm permissão e são estimulados a publicar e distribuir seu trabalho online (ex.: em repositórios institucionais ou na sua página pessoal) a qualquer ponto antes ou durante o processo editorial, já que isso pode gerar alterações produtivas, bem como aumentar o impacto e a citação do trabalho publicado (ver O Efeito do Acesso Livre).

11. Responsabilidade dos autores
11.1. Autores são responsáveis pelo conteúdo publicado, comprometendo-se, assim, a participar ativamente da discussão dos resultados de sua pesquisa científica, bem como do processo de revisão e aprovação da versão final do trabalho.
11.2. Autores são responsáveis pela condução, resultados e validade de toda investigação científica.
11.3. Autores devem noticiar a revista sobre qualquer conflito de interesse.
11.4. As opiniões emitidas pelos autores dos artigos são de sua exclusiva responsabilidade.
11.5. Ao submeter o artigo, o autor atesta que todas as afirmações contidas no manuscrito são verdadeiras ou baseadas em pesquisa com razoável exatidão.

12. Conflito de interesses
A confiabilidade pública no processo de revisão por pares e a credibilidade de artigos publicados dependem em parte de como os conflitos de interesses são administrados durante a redação, revisão por pares e tomada de decisões pelos editores.
12.1. É obrigatório que o autor do manuscrito declare a existência ou não de conflitos de interesse. Mesmo julgando não haver conflitos de interesse, o autor deve declarar essa informação no ato de submissão do artigo, marcando esse campo específico.
12.2. Conflitos de interesses podem surgir quando autores, pareceristas ou editores possuem interesses que, aparentes ou não, podem influenciar a elaboração ou avaliação de manuscritos. O conflito de interesses pode ser de natureza pessoal, comercial, política, acadêmica ou financeira.

12.3. Quando os autores submetem um manuscrito, eles são responsáveis por reconhecer e revelar conflitos financeiros ou de outra natureza que possam ter influenciado seu trabalho.
12.4. Os autores devem reconhecer no manuscrito todo o apoio financeiro para o trabalho e outras conexões financeiras ou pessoais com relação à pesquisa. As contribuições de pessoas que são mencionadas nos agradecimentos por sua assistência na pesquisa devem ser descritas, e seu consentimento para publicação deve ser documentado.
12.5. Manuscritos não serão rejeitados simplesmente por haver um conflito de interesses, mas deverá ser feita uma declaração de que há ou não conflito de interesses.
12.6. Os pareceristas devem, igualmente, revelar aos editores quaisquer conflitos de interesse que poderiam influir em suas opiniões sobre o manuscrito, e devem declarar-se não qualificados para revisar originais específicos se acreditarem que esse procedimento é apropriado. Assim como no caso dos autores, se houver silêncio por parte dos pareceristas sobre conflitos potenciais, isso significará que os conflitos não existem.
12.7. No caso da identificação de conflito de interesse da parte dos pareceristas, o Conselho Editorial encaminhará o manuscrito a outro parecerista *ad hoc*.
12.8. Se os autores não tiverem certeza do que pode constituir um potencial conflito de interesses, devem contatar o Coordenador Editorial da Revista.
12.9. Para os casos em que editores ou algum outro membro publiquem com frequência na Revista, não serão atribuídos tratamentos especiais ou diferenciados. Todos os artigos submetidos serão avaliados através do procedimento *double blind peer review*.

13. Outras informações
13.1. Os trabalhos serão selecionados pelo Coordenador Editorial e pelo Conselho Editorial da Revista, que entrarão em contato com os respectivos autores para confirmar o recebimento dos textos, e em seguida os remeterão para análise de dois pareceristas do Conselho de Pareceristas.
13.2. Os originais recebidos e não publicados não serão devolvidos.
13.3. Asseguram-se aos autores o direito de recurso das decisões editorais.
13.3.1. Serão concedidos 5 (cinco) dias, contados da data da decisão final do Conselho Editorial.
13.3.2. O arrazoado escrito deverá ser enviado para o e-mail: journal@nuped.com.br.
13.3.3. O recurso será analisado pelo Conselho Editorial no prazo de 30 (trinta) dias.

CONDIÇÕES PARA SUBMISSÕES

Como parte do processo de submissão, os autores são obrigados a verificar a conformidade da submissão em relação a todos os itens listados a seguir. As submissões que não estiverem de acordo com as normas serão devolvidas aos autores.

1. A contribuição é original e inédita (salvo em caso de artigos em língua estrangeira publicados no exterior), e não está sendo avaliada para publicação por outra revista; caso contrário, deve-se justificar em “Comentários ao editor”.
2. O arquivo da submissão está em formato Microsoft Word.
3. URLs para as referências foram informadas quando possível.
4. O texto possui entre 15 e 30 páginas (tamanho A4 – 21 cm x 29,7 cm), compreendendo a introdução, desenvolvimento, conclusão (não necessariamente

com esses títulos) e uma lista de referências bibliográficas; as margens utilizadas são: esquerda e superior de 3 cm e direita e inferior de 2 cm; no corpo do texto utilizou-se Fonte Times New Roman, tamanho 12, espaçamento entre linhas de 1,5, e espaçamento de 0 pt antes e depois dos parágrafos; nas notas de rodapé utilizou-se Fonte Times New Roman, tamanho 10, espaçamento simples entre linhas; no desenvolvimento do texto, os parágrafos contêm recuo de 1,5 cm em relação à margem esquerda; títulos e subtítulos estão alinhados à margem esquerda, sem recuo; as figuras e tabelas estão inseridas no texto, não no final do documento na forma de anexos.

5. O texto segue os padrões de estilo e requisitos bibliográficos descritos em Diretrizes para Autores, na página para submissão.
6. Em caso de submissão a uma seção com avaliação pelos pares (ex.: artigos), as instruções disponíveis em Assegurando a avaliação pelos pares cega foram seguidas.
7. O autor declara que, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, este artigo é de sua autoria e, portanto, não contém plágio. Declara, ainda, que está ciente das implicações legais que a utilização de material de terceiros acarreta.
8. O autor declara que participou suficientemente do trabalho para tornar pública sua responsabilidade pelo conteúdo e que todas as afirmações contidas no manuscrito são verdadeiras ou baseadas em pesquisa com razoável exatidão.
9. O autor concorda com a política de responsabilidade estabelecida no item 10. Responsabilidade dos autores das Diretrizes para Autores.

POLÍTICA DE PRIVACIDADE

Os nomes e endereços informados nesta revista serão usados exclusivamente para os serviços prestados por esta publicação, não sendo disponibilizados para outras finalidades ou a terceiros.

Este periódico tem um compromisso com a ética e a qualidade das publicações, seguindo padrões internacionais de publicação científica. Defendemos um comportamento ético de todas as partes envolvidas na publicação em nosso periódico: autores, editor, pareceristas, Equipe Editorial e a Editora. Não aceitamos plágio ou qualquer outro comportamento antiético. Para isso, são seguidas as diretrizes do 2nd World Conference on Research Integrity, Singapore, July 22-24, 2010.

Deveres do Editor

- **Decisão de publicação:** o editor é responsável por decidir quais artigos submetidos à revista devem ser publicados. O editor é guiado pelas políticas decididas pelo Conselho Editorial. Essas políticas devem obedecer às exigências legais em vigor sobre difamação, violação de direitos autorais e plágio. Para tomada de decisões o editor pode consultar o Conselho Editorial e os pareceristas.
- **Transparência e respeito:** o editor deve avaliar os manuscritos submetidos sem levar em conta a raça, sexo, a orientação sexual, a crença religiosa, a origem étnica, a nacionalidade ou a filosofia política dos autores.
- **Confidencialidade:** o editor e demais membros da equipe editorial não devem divulgar qualquer informação sobre um manuscrito submetido, a não ser aos pareceristas e os conselheiros editoriais.

- **Divulgação e conflitos de interesse:** O editor não deve utilizar materiais inéditos divulgados em um manuscrito submetido em pesquisas próprias sem o consentimento expresso e por escrito do autor. O editor deve recusar avaliar os manuscritos em que tenha conflitos de interesse por questões competitivas, colaborativas ou outros relacionamentos ou ligações com qualquer um dos autores, empresas ou (possivelmente) instituições ligadas aos manuscritos.
- **Envolvimento e cooperação em investigações:** o editor deve tomar medidas necessárias cabíveis quando foram apresentadas reclamações éticas a respeito de um manuscrito submetido ou artigo publicado.

Deveres dos Pareceristas

- **Contribuição para as decisões editoriais:** a revisão dos pareceristas auxilia o editor na tomada de decisões editoriais e por meio das comunicações com o autor também pode auxiliar o mesmo na melhora do artigo.
- **Pontualidade:** qualquer avaliador de artigo que não se sinta qualificado para analisar o artigo ou sabe que a sua imediata leitura será impossível deve notificar imediatamente o editor.
- **Confidencialidade:** os trabalhos recebidos para análise devem ser tratados como documentos confidenciais. Eles não devem ser mostrados ou discutidos com os outros.
- **Padrões de objetividade:** os pareceres devem ser conduzidos de forma objetiva. Os pareceristas devem expressar seus pontos de vista de maneira clara e apoiados em argumentos.
- **Sobre as fontes:** os pareceristas devem identificar trabalhos publicados relevantes que não foram citados pelos autores. O parecerista deve chamar a atenção do editor sobre qualquer semelhança substancial ou sobreposição entre o manuscrito em questão e qualquer outro *artigo* publicado de que tenha conhecimento pessoal.
- **Divulgação e conflito de interesses:** informações privilegiadas ou ideias obtidas pelo parecerista por meio da leitura dos manuscritos devem ser mantidas em sigilo e não devem utilizadas para proveito pessoal. O parecerista não deve avaliar manuscritos em que tenha conflitos de interesse por questões competitivas, colaborativas ou outros relacionamentos ou ligações com qualquer um dos autores, empresas ou instituições ligadas aos manuscritos.

Deveres dos Autores

- **Normas gerais:** os autores de trabalhos que se referem a pesquisas originais devem apresentar um relato preciso do trabalho realizado, bem como uma discussão objetiva sobre o seu significado. Dados complementares devem ser representados com precisão no artigo. O documento deve conter detalhes suficientes e referências que permitam que outros possam replicar o trabalho. Declarações fraudulentas ou intencionalmente imprecisas constituem um comportamento antiético e são inaceitáveis.
- **Originalidade e plágio:** os autores devem garantir que as obras são inteiramente originais e se eles utilizam o trabalho e/ou textos dos outros que isso seja devidamente citado. Plágio em todas as suas formas constitui um comportamento editorial antiético e é inaceitável.

- **Publicação múltipla ou redundante:** um autor não deve publicar manuscritos que descrevam essencialmente a mesma pesquisa em mais de um periódico. Publicar o mesmo artigo em mais de um periódico sem informar os editores e obter seu consentimento constitui um comportamento editorial antiético e é inaceitável.
- **Sobre as fontes:** o trabalho de outros autores deve sempre ser reconhecido. Os autores devem citar as publicações que foram importantes na determinação da natureza do trabalho relatado. As informações obtidas em particular, como em uma conversa, correspondência, ou discussão com terceiros, não devem ser utilizadas ou relatadas sem a permissão explícita por escrito da fonte. As informações obtidas por meio de serviços confidenciais, tais como arbitragem manuscritos ou pedidos de bolsas, não devem ser utilizadas sem a permissão explícita por escrito do autor do trabalho envolvido nestes serviços.
- **Autoria:** a autoria do trabalho deve ser restrita àqueles que fizeram uma contribuição significativa para a concepção, projeto, execução ou interpretação do estudo relatado. Todos aqueles que fizeram contribuições significativas devem ser listados como coautores. Pessoas que participaram em certos aspectos do projeto de pesquisa devem ser listadas como colaboradores. O autor principal deve garantir que todos os coautores apropriados estejam incluídos no artigo. O autor principal também deve certificar-se que todos os coautores viram e aprovaram a versão final do manuscrito e que concordaram com sua submissão para publicação.
- **Divulgação e conflitos de interesses:** todos os autores devem divulgar no manuscrito qualquer conflito financeiro ou de outra natureza que possa influenciar os resultados ou a interpretação de seu manuscrito. Todas as fontes de apoio financeiro para o projeto devem ser divulgadas.
- **Erros fundamentais em trabalhos publicados:** quando um autor descobre um erro significativo ou imprecisão em seu trabalho publicado é obrigação do autor informar imediatamente o editor da revista ou a Editoria de Periódicos e cooperar com o editor para corrigir o artigo.

Deveres da Editora

Estamos empenhados em garantir que publicidade, reimpressão ou qualquer outra fonte de receita comercial não tenha qualquer impacto ou influência sobre as decisões editoriais.

Nossos artigos são avaliados por pares para garantir a qualidade da publicação científica. Este periódico utiliza o CrossCheck (software antiplágio da CrossRef).

* Esta declaração se baseia nas recomendações da Elsevier e no *Best Practice Guidelines for Journal Editors* do Committee on *Publication Ethics – COPE*.

Author Guidelines

1. Article Submission

Article propositions for publishing on the International Journal of Digital Law must be sent through the electronic submission system (free of cost) and access through login and password. Propositions sent by e-mail will not be accepted. The Journal has the right to accept or reject any originals received, according to its Editorial Board's recommendations, including the inadequacy of the article's theme to the journal's editorial profile, as well as the right to propose modifications.

2. Author Qualification

At least one of the authors must own either a PhD degree or a Doctor of Juridical Science (J.S.D. or S.J.D), Doctor juris (Dr. iur. or Dr. jur.), Doctor of Philosophy (Ph.D.) ou Legum Doctor (LL.D.) degree. This requirement can be relativized, never exceeding 30% of the articles per edition, in exceptional cases of: (i) authors affiliated to foreign institutions; (ii) articles written in English.

3. Originality and exclusivity

Articles for publication in the International Journal of Digital Law must be original and exclusive, except in case of articles written in a foreign language and published outside Brazil. After the publication of the article in this journal, it can also be published in books and compilations, as long as the original publication is mentioned. We ask the authors to commit to not publish the article in other journals or reviews, as well as not to submit it to other journals at the same time.

4. Languages

Articles can be submitted in English, Portuguese, and Spanish.

5. Registration of the metadata in the electronic submission system

5.1. At the time of submission of the article to the electronic system, the metadata fields must be filled in according to these guidelines, under penalty of preliminary rejection of the submission.

5.2. Authors

5.2.1. *First name/Middle name/Last name:* indication of the full name of the author(s) with only the initials of each name in capital letter. In case of articles in co-authorship, the names of all coauthors must be inserted in the system in the order that should appear at the time of publication.

5.2.2. *E-mail:* indication of the e-mail address of the author(s) for contact, which will mandatorily appear in the published version of the article.

5.2.3. *ORCID iD:* indication of the number of the author's ORCID identifier (for further information click here). The ORCID identifier can be obtained in ORCID register. Authors must have to accept the patterns for presentation of ORCID iD and include the full URL (e.g.: https://orcid.org/0000-0003-1781-1726).

5.2.4. *URL:* link to the author's full curriculum. In the case of Brazilian authors, the link to the Lattes Curriculum should be indicated.

5.2.5. *Affiliation:* indication of the author's main institutional affiliation (or two main affiliations if both of the links with them have the same importance). The main institution is where the author is professor or student, or, in case of not being professor or student anymore, the institution where the authors obtained their major academic title (PhD, J.S.D., LL.M, B.A., etc.). The institution's name must be written in full (not abbreviated) and in the original language of the institution (or in English for non-Latin languages), followed by an indication of the country of origin of the institution between parentheses. If the author is a professor and also a PhD, J.S.D or LL.M candidate in another institution, the main affiliation will be the institution where the author is candidate.
5.2.6. *Country:* indication of the country of the author's main institutional affiliation.
5.2.7. *Bio Statement:* indication of the author's abbreviated CV, with the information organized in the following sequence: first, the indication of the institution to which the author is affiliated as a professor; second, between parentheses, the city, state/province (if applicable) and country of the institution; third, indication of academic titles (starting with the highest); fourth, other bonds with scientific associations; fifth, profession; etc.

5.3. Title and Abstract

5.3.1. *Title:* title in the language of the article, with only the first letter of the sentence in capital letter.
5.3.2. *Abstract:* abstract in the language of the article, without paragraph or citations and references, with up to 200 words.

5.4. Indexing

5.4.1. *Keywords:* indication of 5 keywords in the language of the article (in lower case and separated by semicolons).
5.4.2. *Language:* indicate the acronym corresponding to the language of the article (Português=pt; English=en; Español=es).
5.5. *Supporting Agencies:* articles resulting from funded research projects should indicate in this field the source of funding.
5.6. *References:* insert the complete list of references cited in the article, with a space of one line between them.

6. Text Presentation and pre-textual elements

6.1. The article must have between 15 and 30 pages (size A4 – 21 cm × 29,7 cm), including introduction, development and conclusion (not necessarily with these titles) and a bibliographic reference list. The maximum number of pages can be relativized in exceptional cases, decided by the Editorial team.
6.2. Edges (margins) must be: top and left with 3 cm, bottom and right with 2 cm.
6.3. The text must use Font Times New Roman, size 12, line spacing 1.5, and spacing 0 pt before and after paragraphs.
6.4. References must use Font Times New Roman, size 10, simple space between lines.
6.5. In the development of the text, the paragraphs must contain decrease of 1.5 cm from the left margin. Titles and subtitles must be aligned with the left margin without decrease.
6.6. The structure should observe the following order:

6.6.1. Title in the article's language, in bold, centralized, with the first letter of the sentence in capital letter.
6.6.2. In case of indicating information related to the article (financing from sponsoring agencies, acknowledgments, translators, etc.), it is necessary to insert a footnote with an asterisk (not number) on the right side of the title in the article's language.
6.6.3. Title in English, with only the first letter in capital letter, in bold and in italic, centralized. In the case of articles written in English, this element must be substituted by the title in Portuguese.
6.6.4. The article must not include the names of the author(s). The information for publication purposes will be taken from the metadata entered by the author(s) in the journal's electronic system at the time of submission.
6.6.5. Abstract in the article's language (font Times New Roman, 12, simples lines, without paragraph or quotations and references, until 200 words), preceded by the word "Abstract" written in the article's language.
6.6.6. Indication of five keywords in the article's language (in lower case and separated by semicolon), preceded by the expression "Keywords" written in the article's language.
6.6.7. Abstract in English (font Times New Roman, 12, simples lines, without paragraph or quotations and references, up to 200 words), preceded by the word "Abstract". In case of articles written in English, this element must be replaced by the abstract ("*resumo*") in Portuguese.
6.6.8. Indication of five keywords in English (in lower case and separated by semicolon), preceded by the expression "Keywords". In case of articles written in English, this element must be replaced by keywords ("*palavras-chave*") in Portuguese.
6.6.9. Table of contents, indicating the titles of the sections and subsections, with progressive numbering in Arabic numbers.
6.6.10. Development of the scientific article: progressive numbering, in Arabic numbers, must be used to make clear the content's systematization.
6.6.11. Bibliographic references list must bring only sources that were really used, located in the end of the article, separated by a simple space, lined to the left margin (no indent).
6.6.12. For other aspects, apply Brazilian technical norms (ABNT NBR 10520:2002 e 14724:2011).
6.6.13. In the case of articles with 4 or more authors, it is necessary to include a footnote indicating the contribution of each one to the article.
6.7. Highlights must be made only in italics, meaning that bold, underlined or caps lock, cannot be used to highlight.
6.8. Images and boards must be inserted in the text, not in the end in form of attachments.

7. Scientific Methodology
7.1. The references of books, chapters in collective books, articles, theses, dissertations/essays, monographs of quoted authors used as base to write the text must be mentioned as a reference on the footnotes, with all the information about the text, according to the Brazilian technical norms (ABNT NBR 6023:2018 – summarized in the item 7.1.3 below), and especially, indicating the page of which the information written on the text was taken, right after the reference.

7.1.1. Book's title (or journal's title) must be highlighted in italics (bold shall not be used for that purpose).
7.1.2. Articles written in the format AUTHOR-YEAR will not be accepted for publishing.
7.1.3. References shall appear as follows:
7.1.3.1. Books:
LAST NAME, Name Middle Name. *Title of the book in italics:* subtitle not in italics. Number of the edition. City: Publisher, Year.
Example:
KEEN, Andrew. *Vertigem digital*: por que as redes sociais estão nos dividindo, diminuindo e desorientando. Trad. Alexandre Martins, Rio de Janeiro: Zahar, 2012. 254p.
7.1.3.2. Chapter in a collective book:
LAST NAME, Name Middle Name. Title of the Chapter not in bold. In: ORGANIZER'S LAST NAME, Name Middle Name; 2ND ORGANIZER'S LAST NAME, Name Middle Name, and so on, separated by semicolon (Org. or Coord.). *Title of the book in italics***:** subtitle not in Italics. Number of the edition. City: Publisher, Year. first page-last page [preceded by "p."].
Example:
DOTTA, Alexandre Godoy. Derechos de la Población LGBT+ en Brasil: Vulnerabilidad Social entre Avances y Retrocesos. In: BRAVO, Álvaro Sánches; CASIMIRO, Ligia Melo de; GABARDO, Emerson. (Org.). *Estado Social Y Derechos Fundamentales en Tiempos de Retroceso*. Sevilha: Ponto Rojo, 2019. p. 203-228.
7.1.3.3. Articles in journals:
LAST NAME, Name Middle Name. Title of the article not in bold. *Title of the journal in italics*, city, volume, number, first page-last page [preceded by "p."], months of publishing [abbreviated with the first three letters of the month followed by dot and separated by a slash]. Year.
Example:
GABARDO, Emerson; SAIKALI, Lucas Bossoni. A prescritibilidade da ação de ressarcimento ao erário em razão de atos de improbidade administrativa. *Revista Jurídica – Unicuritiba*, Curitiba, v. 1, p. 514-543, 2018.
7.1.3.4. Theses of Full Professor contests, Doctoral theses, Master's dissertations/ essays, Undergraduate and Graduate courses monographs:
LAST NAME, Name Middle Name. *Title in italics:* subtitle. City, year. number of pages followed by "f". Kind of the work (Degree obtained with the defense) – Department or Sector, Name of the institution.
Example:
SANTOS, Fábio de Sousa. *Análise Comparada da Competição na Contratação Pública Brasileira e Estadunidense*. Curitiba, 2018. 134f. Dissertação (Mestrado em Mestrado em Direito) – Pontifícia Universidade Católica do Paraná. Curitiba: 2018.
7.1.3.5. DOI – Digital object identifier: If the document consulted in the research has the DOI number, it is recommended to include, in a complementary way, the number after the end of each reference. Example:
DOTTA, Alexandre Godoy. Public policies for the assessment of quality of the Brazilian higher education system. *Revista de Investigações Constitucionais*, Curitiba, v. 3, p. 53-69, 2016. DOI. 10.5380/rinc.v3i3.49033.

7.1.3.6. Documents in electronic media: Documents extracted from electronic media must present after the end of each reference the location of the network where it was found and presented as follows. Example:
DIJDL. International Journal of Digital Law. *Regras para a submissão de artigos*. Disponível em: https://journal.nuped.com.br/index.php/revista/about/submissions. Acesso em: 12 fev. 2020.
7.1.4. The elements of references must observe the following model:
7.1.4.1. **Author:** LAST NAME in capital letters, comma, Name with the initials in capital letters, Middle Name with the initials in capital letters, followed by a dot.
7.1.4.2. Edition: the information must only be included after the second edition of the book, without ordinal, followed by a dot and "ed.". Example: 2. ed.
7.1.4.3. Year: it must be written with Arabic numerals, without dot in thousand, preceded by comma, and followed by a dot**.** Example: 1997.
7.1.5. In case of being impossible to find one of those elements, the absence must be resolved in the following manner:
7.1.5.1. Absence of city: replace for [S.l.].
7.1.5.2. Absence of publisher: replace for [s.n.].
7.1.5.3. Absence of year: the approximated year must be indicated between brackets, followed by a question mark. Example: [1998?].
7.2. The quotations (words, expressions, sentences) must be carefully reviewed by the authors and/or translators.
7.2.1. The direct quotations must follow this pattern: transcription until four lines should fit in the text body, with normal letter, normal spacing and quotation marks.
7.2.2. It is strongly recommended that long textual quotations (more than four lines) are not used. However, if indispensable, they shall constitute an independent paragraph, with 1,5 cm of decrease related to the left margin (justified alignment), with simple lines and font 10. In that situation, quotation marks must not be used.
7.2.3. It is forbidden the use of "op. cit.", "loc. cit.", "ibidem" and "idem" in the footnotes. The references in footnote must be complete and written out.
7.2.4. For the mention of authors in the text body, it is forbidden the use of capital letters (e.g. for Name LAST NAME...). In this case all mentions shall be written only with the first letter in capital letter (ex.: for Name Last Name...).

8. Composition
8.1. Apart from having an adequate scientific language for an editorial publication, the text must be reviewed.
8.2. In the case of articles written in Portuguese, the writing must obey the new orthographic rules in force since the promulgation of the Portuguese Language Orthographic Agreement, from January 1st, 2009.
8.3. Citations of texts that precede the Agreement must respect the original spelling.

9. Articles resulted from funded researches
Articles resulted from funded research projects shall indicate in a footnote, located at the end of the article title in the original language, the information related to the research financing.

10. Copyright statement

Authors who publish in this Journal have to agree to the following terms:

10.1. No copyright or any other remuneration for the publication of papers will be due.

10.2. Authors retain copyright and grant the International Journal of Digital Law the right of first publication with the article simultaneously licensed under the Creative Commons Attribution License, which allows sharing the work with recognition of its initial publication in this Journal. Moreover, because of their appearance in this open access Journal, articles are free to use, with proper attribution, in educational and non-commercial applications.

10.3. Authors are allowed and encouraged to post their work online (e.g. in institutional repositories or on their personal webpage) at any point before or during the submission process, as it can lead to productive exchanges, as well as increase the impact and citation of published work (see The Effect of Open Access).

11. Authors responsibilities

11.1. Authors are responsible for the published content, committing therefore to participate actively in the discussion of the results of their scientific research, as well as the review process and approval of the final version of the work.

11.2. Authors are responsible for the conducting all the scientific research, as well as its results and validity.

11.3. Authors should report the Journal about any conflict of interest.

11.4. Authors are fully and exclusively responsible for the opinions expressed in their articles.

11.5. When submitting the articles, authors recognize that all statements contained in the manuscript are true or based on research with reasonable accuracy.

12. Conflict of interest

The public confidence in the double-blind peer review process and the credibility of published articles depend in part on how conflicts of interest are managed during manuscript writing, peer review and decision making by the editors.

12.1. It is mandatory that the author of the manuscript declares the existence or not of conflicts of interest. Even thinking that there are no conflicts of interest, the author must declare this information in the article submission act, marking that field.

12.2. Conflicts of interest may appear when authors, reviewers or editors have interests that, apparently or not, may influence the development or evaluation of manuscripts.

12.3. When authors submit a manuscript, they are responsible for recognizing and revealing financial or other nature conflicts that may have influenced their work.

12.4. Authors must recognize all the financial support for the work and other financial or personal connections related to the research. The contributions of people who are mentioned in the acknowledgments for their assistance in the research must be described, and its consent to publication should be documented.

12.5. Manuscripts will not be simply dismissed because of a conflict of interest. A statement that there is or not a conflict of interest must be made.

12.6. The ad hoc reviewers must also reveal to editors any conflicts of interest that could influence their opinions about the manuscript and must declare themselves unqualified to review specific documents if they believe that this procedure is appropriate. In the

case of the authors, if there is silence from the peer reviewers about potential conflicts, it will mean that conflicts do not exist.

12.7. If a conflict of interest on the part of the peer reviewers is identified, the Editorial Board will send the manuscript to another ad hoc reviewer.

12.8. If the authors are not sure about what might constitute a potential conflict of interest, they should contact the Journal's Editor-in-Chief.

12.9. In cases in which members of the Editorial Team or some other member publish frequently in the Journal, it will not be given any special or different treatment. All submitted papers will be evaluated by double blind peer review procedure.

13. Other information

13.1. The articles will be selected by the Editor-in-Chief and the Editorial Board of the Journal, which will contact the respective authors to confirm the text reception, and then forward them to the two ad hoc reviewers' analysis.

13.2. The received and not published originals will not be given back.

13.3. Authors have the right to appeal of the editorial decisions.

13.3.1. They will be granted five (5) days from the date of the final decision of the Editorial Board to appeal.

13.3.2. The written appeal must be sent to the e-mail: <journal@nuped.com.br>.

13.3.3. The appeal will be examined by the Editorial Board within thirty (30) days

CONDITIONS FOR SUBMISSIONS

As part of the submission process, authors are required to check off their submission's compliance with all the following items, and submissions may be returned to authors that do not adhere to these guidelines.

1. The contribution is original and unpublished (except in the case of articles in a foreign language published abroad) and it is not being evaluated for publication by another Journal; otherwise, it must be justified in "Comments to the Editor."
2. The submission file is in Microsoft Word, OpenOffice or RTF.
3. URLs for the references have been informed when possible.
4. The text has between 15 and 30 pages (A4 size – 21 cm by 29.7 cm), including the introduction, development, conclusion (not necessarily with these titles) and a list of references; margins used are: left and top of 3 cm and right and bottom of 2 cm; the text is written in Times New Roman format, size 12, line spacing 1.5, and spacing 0 pt. before and after paragraphs; in the footnotes it was used Times New Roman, size 10, 1 pt. spacing; in the text development, paragraphs have an indent of 1.5 cm from the left margin; headings and subheadings are aligned on the left margin; figures and tables are inserted in the text, not in the end of the document as attachments.
5. The text respects the stylistic and bibliographic requirements outlined in the Author Guidelines, on the page About.
6. In case of submission to a section with peer review (e.g.: articles), the instructions available in Ensuring blind evaluation by peer reviewers have been followed.
7. The author states that, except for the direct and indirect quotations clearly indicated and referenced, the article is of his/her authorship and therefore does not contain plagiarism. And states that he/she is aware of the legal implications of the use of other authors material.

8. The author states that participated in the work enough to make public their responsibility for the content and that all statements contained in the manuscript are true or based on research with reasonable accuracy.
9. The author agrees with the liability policy defined in item 10. Authors responsibilities of the Author Guidelines.

PRIVACY STATEMENT

This journal is committed to ethics and quality in publication, following international patterns of scientific publication. We support standards of expected ethical behavior for all parties involved in publishing in our journal: the author, the journal editor, the peer reviewer and the publisher. We do not accept plagiarism or other unethical behavior. Thus, it follows the guidelines of the 2nd World Conference on Research Integrity, Singapore, July 22-24, 2010.

Duties of Editors

- **Publication decision:** The journal's editor is responsible for deciding which of the articles submitted to the journal should be published. The editor is guided by the policies of the journal's editorial board and constrained by such legal requirements as shall then be in force regarding libel, copyright infringement and plagiarism. The editor may consult with editorial board or reviewers in decision making.
- **Fair play:** The editor should evaluate manuscripts for their intellectual content without regard to race, gender, sexual orientation, religious belief, ethnic origin, citizenship, or political philosophy of the authors.
- **Confidentiality:** The editor and any editorial staff must not disclose any information about a submitted manuscript to anyone other than the corresponding author, reviewers, potential reviewers, other editorial advisers, and the publisher, as appropriate.
- **Disclosure and Conflicts of interest:** The editor must not use unpublished information in his/her own research without the express written consent of the author. The editor should recuse him/herself from considering manuscripts in which he/she has conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or (possibly) institutions connected to the papers.
- **Involvement and cooperation in investigations:** The editor should take reasonable responsive measures when ethical complaints have been presented concerning a submitted manuscript or published paper.

Duties of Reviewers

- **Contribution to Editorial Decision:** Peer review assists the editor in making editorial decisions and through the editorial communications with the author may also assist the author in improving the paper.
- **Promptness:** Any selected referee who feels unqualified to review the research reported in a manuscript or knows that its prompt review will be impossible should notify the editor and excuse himself from the review process.
- **Confidentiality:** Any manuscripts received for review must be treated as confidential documents. They must not be shown to or discussed with others.

- **Standards of Objectivity:** Reviews should be conducted objectively and referees should express their views clearly with supporting arguments.
- **Acknowledgement of Source:** Peer reviewers should identify relevant published work that has not been cited by the authors. The peer reviewer should also call to the editor's attention any substantial similarity or overlap between the manuscript under consideration and any other published paper of which they have personal knowledge.
- **Disclosure and Conflicts of Interest:** Privileged information or ideas obtained through peer review must be kept confidential and not used for personal advantage. Reviewers should not consider manuscripts in which they have conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or institutions connected to the papers.

Duties of Authors

- **Reporting standards:** Authors of reports of original research should present an accurate account of the work performed as well as an objective discussion of its significance. Underlying data should be represented accurately in the paper. A paper should contain sufficient detail and references to permit others to replicate the work. Fraudulent or knowingly inaccurate statements constitute unethical behavior and are unacceptable.
- **Originality and Plagiarism:** The authors should ensure that they have written entirely original works, and if the authors have used the work and/or words of others that this has been appropriately cited or quoted. Plagiarism in all its forms constitutes unethical publishing behavior and is unacceptable.
- **Multiple or Redundant Publication:** An author should not in general publish manuscripts describing essentially the same research in more than one journal or primary publication. To publish the same article in different journals without informing the editors and having their agreement constitute unethical publishing behavior and is unacceptable.
- **Acknowledgement of Sources:** Proper acknowledgment of the work of others must always be given. Authors should cite publications that have been influential in determining the nature of the reported work. Information obtained privately, as in conversation, correspondence, or discussion with third parties, must not be used or reported without explicit, written permission from the source. Information obtained in the course of confidential services, such as refereeing manuscripts or grant applications, must not be used without the explicit written permission of the author of the work involved in these services.
- **Authorship of the Paper:** Authorship should be limited to those who have made a significant contribution to the conception, design, execution, or interpretation of the reported study. All those who have made significant contributions should be listed as co-authors. Where there are others who have participated in certain substantive aspects of the research project, they should be acknowledged or listed as contributors. The corresponding author should ensure that all appropriate co-authors and no inappropriate co-authors are included on the paper, and that all co-authors have seen and approved the final version of the paper and have agreed to its submission for publication.

- **Disclosure and Conflicts of Interest:** All authors should disclose in their manuscript any financial or other substantive conflict of interest that might be construed to influence the results or interpretation of their manuscript. All sources of financial support for the project should be disclosed.
- **Fundamental errors in published works:** When an author discovers a significant error or inaccuracy in his/her own published work, it is the author's obligation to promptly notify the journal editor or publisher and cooperate with the editor to retract or correct the paper.

Duties of the Publisher

We are committed to ensuring that advertising, reprint or other commercial revenue has no impact or influence on editorial decisions.

Our articles are peer reviewed to ensure the quality of scientific publishing and we are also users of CrossCheck (CrossRef's plagiarism software).

* This statement is based on Elsevier recommendations and COPE's Best Practice Guidelines for Journal Editors.