

Marília Rulli Stefanini
Ernane Rosa Martins
(Orgs.)



DIREITO DIGITAL

PRIVACIDADE, TECNOLOGIA E REGULAÇÃO



científica digital



CIENTÍFICA DIGITAL EDITORIAL LTDA

Barueri - São Paulo - Brasil
www.cientificadigital.org - contato@cientificadigital.org

Diagramação e Arte	Edição © 2025 Científica Digital
Diego Santos	Texto © 2025 Os Autores
Diogo Lima	1ª Edição - 2025
Imagens da Capa	Acesso Livre - Open Access
Adobe Stock - 2025	

© COPYRIGHT - TODOS OS DIREITOS RESERVADOS. A editora detém os direitos autorais sobre a edição e o projeto gráfico, enquanto os autores mantêm os direitos autorais de seus respectivos textos. Esta obra está licenciada sob a Licença Creative Commons Atribuição 4.0 Internacional, permitindo o download e compartilhamento integral ou parcial, desde que a fonte seja devidamente citada e os créditos atribuídos aos autores. É obrigatório que a obra permaneça em formato de Acesso Livre (Open Access), sem qualquer alteração. A catalogação em plataformas de acesso restrito ou com fins comerciais é estritamente proibida.



Dados Internacionais de Catalogação na Publicação (CIP)

D598 Direito digital: privacidade, tecnologia e regulação / Organização de Marília Rulli Stefanini, Ernane Rosa Martins. – Barueri-SP: Científica Digital, 2025.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui Bibliografia
ISBN 978-65-83998-45-3
DOI 10.37885/978-65-83998-45-3

1. Direito. I. Stefanini, Marília Rulli (Organizadora). II. Martins, Ernane Rosa (Organizador). III. Título.

CDD 340

Elaborado por Janaína Ramos – CRB-8/9166

Índice para catálogo sistemático:

I. Direito

E-BOOK

ACESSO LIVRE ON LINE - IMPRESSÃO PROIBIDA

2025

Marília Rulli Stefanini
Ernane Rosa Martins
(Orgs.)

Direito Digital:
Privacidade, Tecnologia e Regulação

1ª EDIÇÃO



científica digital

2025 - BARUERI - SP

CONSELHO EDITORIAL

Prof. Dr. André Cutrim Carvalho
Prof. Dr. Antônio Marcos Mota Miranda
Prof^a. Ma. Auristela Correa Castro
Prof. Dr. Carlos Alberto Martins Cordeiro
Prof. Dr. Carlos Alexandre Oelke
Prof^a. Dra. Caroline Nóbrega de Almeida
Prof^a. Dra. Clara Mockdece Neves
Prof^a. Dra. Claudia Maria Rinhel-Silva
Prof^a. Dra. Clecia Simone Gonçalves Rosa Pacheco
Prof. Dr. Cristiano Marins
Prof^a. Dra. Cristina Berger Fadel
Prof. Dr. Daniel Luciano Gevehr
Prof. Dr. Diogo da Silva Cardoso
Prof. Dr. Ernane Rosa Martins
Prof. Dr. Everaldo dos Santos Mendes
Prof. Dr. Fabricio Gomes Gonçalves
Prof^a. Dra. Fernanda Rezende
Prof. Dr. Flávio Aparecido de Almeida
Prof^a. Dra. Francine Náthalie Ferraresi Queluz
Prof^a. Dra. Geuciane Felipe Guerim Fernandes
Prof. Dr. Humberto Costa

Prof. Dr. Joachin Melo Azevedo Neto
Prof. Dr. Jónata Ferreira de Moura
Prof. Dr. José Aderval Aragão
Prof. Me. Julianno Pizzano Ayoub
Prof. Dr. Leonardo Augusto Couto Finelli
Prof. Dr. Luiz Gonzaga Lapa Junior
Prof. Me. Marcelo da Fonseca Ferreira da Silva
Prof^a. Dra. Maria Cristina Zago
Prof^a. Dra. Maria Otília Zangão
Prof. Dr. Mário Henrique Gomes
Prof. Dr. Marcus Fernando da Silva Praxedes
Prof. Dr. Nelson J. Almeida
Prof. Dr. Pedro Afonso Cortez
Prof. Dr. Reinaldo Pacheco dos Santos
Prof. Dr. Rogério de Melo Grillo
Prof^a. Dra. Rosenery Pimentel Nascimento
Prof. Dr. Rossano Sartori Dal Molin
Prof. Me. Silvio Almeida Junior
Prof^a. Dra. Thays Zigante Furlan Ribeiro
Prof. Dr. Wescley Viana Evangelista
Prof. Dr. Willian Carboni Viana
Prof. Dr. Willian Douglas Guilherme

Acesse a lista completa dos Membros do Conselho Editorial em www.editoracientifica.com.br/conselho

Parecer e revisão por pares

Os textos que compõem esta obra passaram por avaliação do Conselho Editorial e revisão por pares externos (*Peer Review*), recebendo a devida recomendação para publicação.

Nota: Esta obra é fruto de um processo colaborativo, configurando-se como uma coletânea na qual os direitos autorais permanecem resguardados para os respectivos autores. Alguns capítulos podem ter origem em trabalhos anteriormente apresentados em eventos acadêmicos; no entanto, os autores foram orientados a adotar o devido rigor na prevenção do autoplágio. A responsabilidade pelo conteúdo de cada capítulo, assim como pela originalidade e integridade das informações publicadas, é inteiramente dos respectivos autores e autoras. O conteúdo da obra não reflete, necessariamente, a opinião da editora, dos organizadores ou dos membros do conselho editorial.

APRESENTAÇÃO

Esta obra é fruto de um esforço colaborativo que reuniu professores, estudantes e pesquisadores cujo envolvimento enriqueceu significativamente as discussões neste espaço formativo. Além disso, resulta de iniciativas interinstitucionais e ações voltadas ao incentivo à pesquisa, congregando especialistas de diversas áreas do conhecimento, vinculados a Instituições de Educação Superior, públicas e privadas, em âmbito nacional e internacional.

Seu principal objetivo é fortalecer a integração entre instituições, tanto no Brasil quanto no exterior, por meio de redes de pesquisa comprometidas com a formação continuada de profissionais da educação. Para isso, busca-se a produção e a ampla disseminação do conhecimento em distintas áreas do saber.

Expressamos nossa profunda gratidão aos autores pelo empenho, comprometimento e dedicação na concepção e finalização desta obra. Esperamos que ela se consolide como um recurso didático-pedagógico valioso, atendendo às necessidades de estudantes, docentes de todos os níveis de ensino e demais interessados na temática.

Marília Rulli Stefanini
Ernane Rosa Martins

SUMÁRIO

Capítulo 01

ÉTICA DOS ALGORITMOS NA SOCIEDADE EM REDE: SOBRE DESIGUALDADES E SEGURANÇA

Pablo Michel Candido Alves de Magalhães; Igor Ferreira Fontes

doi 10.37885/250419284 8

Capítulo 02

TRATAMENTO DE DADOS PESSOAIS EM OPERAÇÕES DE M&A: UM ESTUDO SOBRE AS BASES LEGAIS APLICÁVEIS E AS MEDIDAS TÉCNICAS E ADMINISTRATIVAS ADOTADAS PARA CONFORMIDADE COM A LEGISLAÇÃO

Allan Nascimento Turano; João Gabriel de Oliveira Freitas

doi 10.37885/250619598 28

Capítulo 03

DIREITO À COMUNICAÇÃO E LACUNA DIGITAL NO NORTE DA ARGENTINA: O ACESSO À INTERNET COMO GARANTIA DE USUFRUTO DO ESPAÇO PÚBLICO

Franco-David Hessling-Ferreiro; Andrea Paola Yanguas Xavier

doi 10.37885/250920058 45

Capítulo 04

JUSTIÇA EM RISCO: O PASSIVO OCULTO DA LGPD E A AMEAÇA DE INSOLVÊNCIA ESTATAL

Lydia de Jesus Azêdo Neta; Pablo Oliva Souza; Taís Viga de Albuquerque Oliva Souza

doi 10.37885/251020442 64

Capítulo 05

A ESCALADA DAS DEEPFAKES E CRIPTOFRAUDES NO BRASIL: ANÁLISE DA RESPOSTA JURÍDICA E DESAFIOS ESTRATÉGICOS FRENTE À INTELIGÊNCIA ARTIFICIAL

Jaison Sfogia Ricardo

doi 10.37885/251220868 75

SOBRE OS ORGANIZADORES 96

ÍNDICE REMISSIVO 97

ÉTICA DOS ALGORITMOS NA SOCIEDADE EM REDE: SOBRE DESIGUALDADES E SEGURANÇA

Pablo Michel Candido Alves de Magalhães
SEDUC/AL - IFAL campus Murici

Igor Ferreira Fontes
SEDUC/AL - IFS campus Socorro

RESUMO

O presente trabalho reflete sobre a ética nas práticas humanas em uma sociedade interconectada, especialmente no uso de algoritmos. Através de uma análise de pesquisas e leitura de estudiosos, o artigo explora dois eixos principais: desigualdades digitais e segurança nas redes. As desigualdades digitais são evidentes na falta de acesso a dispositivos e internet, comprometendo oportunidades educacionais e participação democrática, conforme dados da União Internacional de Telecomunicações e Cetic.br. Além disso, a segurança nas redes enfrenta dilemas entre proteção contra crimes graves, como a pornografia infantil, e a privacidade dos usuários, destacando-se discussões em torno da Lei de Segurança Online do Reino Unido e regulamentações da União Europeia. Pesquisas de Nathalia Sautchuk Patrício (2021) apontam vulnerabilidades nas tecnologias de varredura de conteúdo, enquanto estudos brasileiros propõem sistemas de monitoramento de mensagens contra pedofilia. Pesquisas de Pierre Lévy (1999) e Cathy O'Neil (2021) destacam os desafios éticos e sociais impostos pelas tecnologias, ressaltando a importância de regulamentações, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais no Brasil, para garantir a integridade e proteção dos dados dos usuários.

Palavras-chave: ética; algoritmo; tecnologia; sociedade.

INTRODUÇÃO

Este artigo busca formular uma análise sobre a ética das práticas humanas na sociedade em rede, especialmente em relação aos usos dos algoritmos, a partir de teóricos que versam sobre filosofia ética, história e cultura digital. Desde sua produção até sua execução, é imperativo discutir como essas tecnologias podem ser regulamentadas e utilizadas e como os usos e apropriações humanas precisam de mediação legal. Dois eixos principais guiarão nossas análises: o primeiro, sobre as desigualdades digitais; e o segundo, sobre segurança e liberdade nas redes.

O advento da era digital trouxe inúmeras transformações, revolucionando a maneira como a sociedade interage, trabalha e se informa. Enquanto alguns indivíduos e comunidades se beneficiam amplamente dessas inovações tecnológicas, outros ainda enfrentam significativas barreiras para acessar esses avanços. As desigualdades digitais são uma realidade palpável, manifestando-se na falta de acesso a dispositivos tecnológicos e à internet, especialmente em regiões menos desenvolvidas.

Paralelamente, a segurança e a privacidade nas redes são questões que vêm ganhando destaque, especialmente em casos que envolvem a proteção contra crimes graves, como a pornografia infantil. Propostas de leis, como a Lei de Segurança Online do Reino Unido, trazem à tona debates sobre o equilíbrio entre a privacidade dos usuários e a necessidade de segurança.

Nesse contexto, os algoritmos desempenham um papel central, moldando experiências digitais e influenciando comportamentos.

Isto posto, podemos iniciar as reflexões, ponto a ponto.

Desigualdades digitais

Enquanto parte da população mundial avança a passos largos na era digital, acessando informações, serviços e oportunidades por meio da internet e da tecnologia, outra parte, bastante significativa, fica à margem deste processo, devido a barreiras econômicas, geográficas, educacionais e culturais.

Ao mesmo tempo em que algumas áreas urbanas desfrutam de conexões de alta velocidade e infraestrutura tecnológica de ponta, zonas rurais e regiões menos desenvolvidas muitas vezes carecem deste serviço. Além de limitar o

acesso a informações e oportunidades educacionais, este acesso desigual compromete a participação no dito *mercado de trabalho*¹ global, onde a conectividade digital é essencial. Essa desigualdade também se manifesta na falta de acesso a dispositivos tecnológicos, como computadores e smartphones. Para muitas famílias de baixa renda, adquirir um dispositivo e pagar por serviços de internet pode ser um desafio financeiro significativo. Isso cria uma divisão digital entre aqueles que têm acesso à tecnologia e aqueles que não têm, tornando ainda mais difícil para os últimos competir no mundo digital.

A desigualdade no acesso a dispositivos tecnológicos pode se tornar mais manifesta no momento de inserção no mercado de trabalho. Tomemos como exemplo a chamada geração Z (os nascidos entre 1995 e 2010), por vezes conhecida também como geração “digital” ou “da tecnologia”: ultimamente tem se tornada notória a dificuldade geral de se usar um computador, seja no manuseio do *mouse*, na incompreensão do pacote *Office*, não conhecer comandos como *Ctrl+C* e *Ctrl+V*, enviar um e-mail, configurar uma impressora ou fazer pesquisa não em mecanismos de buscas, mas em ferramentas que não foram criadas para esse propósito, como o *TikTok* e o *ChatGPT*. Embora se trate de um problema generalizado entre os jovens, das classes mais baixas às mais elevadas, as consequências tendem a ser maiores para a população mais pobre, pois enquanto os mais ricos seriam capazes de pagar por cursos de informática ou encontrar com maior facilidade um computador para suprir tais deficiências, os mais vulneráveis enfrentariam maiores dificuldades para acessar tais dispositivos e ferramentas. Em um país como o Brasil, no qual a ascensão social era estimada pela OCDE (2018) em nove gerações para acontecer, a desigualdade tecnológica pode resultar na exclusão do e no mercado de trabalho, relegando às pessoas com menor desenvoltura tecnológica cargos e salários inferiores, perpetuando as desigualdades socioeconômicas.

As implicações da desigualdade tecnológica são extremamente significativas também na participação política das pessoas. Com a disseminação de

¹ O termo refere-se a uma perspectiva capitalista relacionada ao trabalho, que estabelece a visão de um mercado onde os trabalhadores se sujeitam como produtos ao contratante/comprador dos seus serviços. A este, sugerimos em substituição o conceito de mundo do trabalho, pela sua capacidade de melhor sintetizar as dinâmicas das relações contemporâneas em torno das atividades laborativas (FIGARO, 2008)

notícias e informações ocorrendo principalmente online, aqueles que não têm acesso à internet ou não têm a capacidade de avaliar criticamente as informações que encontram estão em desvantagem na formação de opiniões informadas e na participação em processos democráticos. Segundo dados da União Internacional de Telecomunicações (UIT), uma agência da ONU, coletados até o ano de 2021, os 46 países menos desenvolvidos abrigavam quase um terço da população mundial sem conexão.² No levantamento da TIC Domicílios de 2023³, pesquisa realizada pelo Cetic.br (Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação), um total de 29 milhões de brasileiros não tiveram acesso à internet no ano passado. Ao todo, 156 milhões de brasileiros utilizam a rede online, sendo que 142 milhões fizeram uso diário ou quase diário; 58% das pessoas que têm acesso à internet navegam no ambiente só por meio do celular, o que corresponde a 90 milhões de pessoas.

Para enfrentar as desigualdades digitais, é necessário um esforço conjunto da sociedade. Isso inclui a expansão de infraestrutura de internet em áreas sub atendidas, a promoção de programas de alfabetização digital acessíveis e a disponibilização de dispositivos tecnológicos para comunidades carentes. Contudo, na periferia do capitalismo, onde vivemos, repleta de periferias outras marcadas por desigualdades urbanas, regionais, de classe, de gênero, estas soluções que acabei de elencar se tornam quase utópicas.

Muito por isso, as populações periféricas devem buscar seus próprios meios de organização e resistência, se apropriando das ferramentas tecnológicas disponíveis. De acordo com Nemer (2021), que analisa as nuances do acesso à conectividade digital nas favelas brasileiras, essas apropriações de tecnologias cotidianas têm o nome de *Tecnologias Mundanas*, que é o modo pelo qual a tecnologia é reinterpretada, adaptada e reinventada pelos usuários periféricos, distantes dos locais de poder e que contestam a opressão tecnodigital a eles imposta. Daí o papel fundamental dos centros tecnológicos comunitários, como

² UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. Relatório. Disponível em: <<https://www.itu.int/en/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx>>, acesso em: 15/06/2024.

³ CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO - CETIC. TIC Domicílios 2023. Disponível em: <<https://cetic.br/pt/pesquisa/domicilios/indicadores/>>, acesso em: 15/06/2024.

LAN houses, bibliotecas ou Telecentros, que são “apropriados por comunidades marginalizadas para reivindicarem um espaço social vital” (NEMER, 2021, p. 351).

O dilema da segurança nas redes

Um recente projeto do governo britânico levantou discussões sobre até que ponto a proteção de dados deve ser encarada como algo inviolável ou não. O caso tem a ver, especificamente, com o aplicativo de mensageria WhatsApp e a pornografia e abuso sexual infantil. O projeto em questão é parte da Lei de Segurança Online⁴ do Reino Unido e visa a identificação de conteúdo veiculado no aplicativo identificado como pedofilia, como imagens e vídeos. Para tal, o dispositivo legal prevê a utilização de uma tecnologia credenciada, sob controle do governo, que fará uma varredura das mensagens privadas dos usuários, gerando notificações de conteúdo inapropriado e identificando o emissor.

Em 2021, polêmica semelhante havia atingido a Apple. A fim de combater o abuso infantil, naquele ano a empresa havia anunciado uma atualização de seu sistema operacional na qual implementaria um algoritmo de inteligência artificial que analisaria as imagens armazenadas no iCloud para detectar possível conteúdo pornográfico envolvendo menores de idade. Segundo a empresa, o processo seria criptografado e sigiloso, sem lhe fornecer acesso exato ao conteúdo das fotos – o processo se daria pela comparação do *hash* das imagens com o banco de dados de pornografia infantil e, em caso positivo, os servidores da empresa teriam acesso a uma chave criptográfica que permitiria desbloquear apenas os resultados positivos da análise, que seriam enviados para uma revisão manual feita por uma pessoa. A Apple alegava que a chance de erro seria de 1 em 1 trilhão, mas pesquisadores do *Imperial College* de Londres apresentaram um método simples para burlar o algoritmo, com resultados que colocariam xeque as alegações da Apple. Por causa de toda a repercussão negativa em torno da medida, a Apple acabou voltando atrás e adiando o lançamento do algoritmo, mas esse caso mostra que a discussão não se limita a quem teria acesso aos conteúdos dos usuários, se o Estado ou a iniciativa privada, mas tem como

⁴ PARLAMENTO DO REINO UNIDO. Lei governamental. Disponível em: <<https://bills.parliament.uk/bills/3137>>, acesso em 16/06/2024.

ponto nevrálgico a própria ideia de se violar a privacidade. Há, em paralelo às discussões políticas em torno da lei, o desenvolvimento de ferramentas que possam proporcionar esse monitoramento, em especial baseadas no *client-side scanning* (PATRÍCIO, 2021), tecnologia que realiza o escaneamento e a comparação com uma base de dados de conteúdo “questionável”. Nathalia Sautchuk Patrício (2021), pesquisadora do Centre for Global Cooperation Research da Universidade de Duisburg-Essen na Alemanha, destacou a vulnerabilidade que o *client-side scanning* proporciona a criminosos, aumentando a chamada “superfície de ataque” às contas dos usuários.

A proposta de lei tem um objetivo urgente e necessário, que é o combate ao abuso infantil e o compartilhamento de pornografia de menores na rede. Contudo, as entrelinhas trazem alguns problemas que giram em torno da própria segurança e liberdade na rede. Em 14 de abril de 2022, diversas organizações e especialistas assinaram uma carta aberta⁵, onde expressaram suas preocupações com a proposta de Lei de Segurança Online. Em destaque estava a crítica unânime às tecnologias de varredura, caracterizadas como não confiáveis e altamente suscetíveis a sinalizar conteúdos que não tenham a ver com material pornográfico infantil.

A outra questão mencionada à exaustão é a liberdade do usuário. Aplicativos como o WhatsApp utilizam a tecnologia E2EE, uma criptografia de ponta a ponta que protege com robustez as mensagens dos usuários. Uma vez aprovado, o projeto governamental introduziria um algoritmo de varredura que iria acessar toda e qualquer mensagem presente no aplicativo instalado nos dispositivos móveis, quebrando seu sigilo. Ou seja, as mensagens deixariam de ser privadas (PATRÍCIO, 2021).

A resposta oficial do WhatsApp veio em entrevista⁶ à BBC. Will Cathcart, diretor da empresa, avisou que o aplicativo não iria baixar sua segurança mediante exigência de nenhum governo. “O que está sendo proposto é que nós

⁵ 45 organizações e especialistas em cibersegurança assinam carta aberta expressando preocupações com a Lei de Segurança Online do Reino Unido. Internet Society Capítulo Brasil, 2022. Disponível em: <[https://isoc.org.br/files/Lei%20de%20Seguran%C3%A7a%20Online%20do%20Reino%20Unido%20\(1\).pdf](https://isoc.org.br/files/Lei%20de%20Seguran%C3%A7a%20Online%20do%20Reino%20Unido%20(1).pdf)>, acesso em 16/06/2024

⁶ Entrevista disponível em: <<https://www.bbc.com/portuguese/geral-62361452>>.

– seja diretamente ou indiretamente, via softwares – leiamos as mensagens de todos. [...] Não acho que as pessoas queiram isso”, disse o executivo à ocasião.

Não só o governo britânico, mas também a União Europeia apresentou um projeto de regulamentação no uso dos aplicativos de mensagens, tendo em vista o combate à pedofilia e o abuso infantil na internet, muito similar ao apresentado no Reino Unido. A Comissão Europeia apresentou a proposta em maio de 2022, logo sendo criticada por órgãos especializados no assunto, como o Conselho Europeu de Proteção de Dados (EDPC) e a Autoridade Europeia para a Proteção de Dados (EDPS), que expressaram preocupação em relação ao impacto que o projeto de lei poderia causar na privacidade dos usuários.

A despeito das discussões e polêmicas, a pornografia infantil é uma terrível realidade no mundo inteiro. De acordo com dados⁷ do Centro para Crianças Desaparecidas e Exploradas (NCMEC), dos Estados Unidos, 82 milhões de conteúdos veiculados por aplicativos na internet, entre fotos e vídeos, foram reportados como abuso infantil. De todo esse material, 60% estava hospedado em servidores europeus. Isso acendeu o alerta dos governos do continente, que utilizaram mecanismos legais para combater o problema.

Eis que somos jogados diante de um dilema que ronda a vida nas redes: é possível ter privacidade e segurança, sem destruir uma ou outra?

No Brasil, Daniela Milón Flores e Robson Cordeiro, pesquisadores da USP, desenvolveram em fevereiro de 2022 um sistema de monitoramento de mensagens que alerta sobre conteúdo relacionado à pedofilia⁸. O estudo utilizou um conjunto de dados de mensagens de texto em que adultos se fizeram passar por crianças para interagir com pedófilos. A análise dos dados focou em identificar características das conversas que possam ser ensinadas a uma máquina para reconhecer interações potencialmente perigosas. O algoritmo escaneia e identifica as mensagens que podem ser entendidas como assédio a menores de idade. A análise detalhada dos termos sexuais presentes nas conversas com

⁷ NATIONAL CENTER OF MISSING AND EXPLOITED CHILDREN. Child Sexual Abuse Material. Disponível em: <<https://www.missingkids.org/theissues/csam>>, acesso em 16/06/2024.

⁸ A pesquisa do Grupo de Bases de Dados e de Imagens (GBDI) do ICMC da USP contou com apoio da Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) e do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

abusadores resultou na criação de um dicionário, que inclui variações usadas na tentativa de enganar o algoritmo. Por exemplo, “sex” pode ser reconhecido mesmo se escrito como “\$ex” ou “s3x”, formas alternativas chamadas de typos, o que torna a ferramenta mais sofisticada (FLORES; CORDEIRO, 2022).

O objetivo é que pais possam utilizar essa ferramenta com seus filhos, reforçando a proteção contra a atuação de pedófilos na rede. Além disso, o sistema possui um banco de dados com palavras de cunho sexual e ainda tem defesas contra estratégias que os abusadores utilizam para driblar programas de monitoramento (FLORES; CORDEIRO, 2022).

Obviamente, há um custo, que é a perda da privacidade. E possivelmente seja um ponto de inflexão difícil de esgotar neste texto. O combate à pedofilia exige o acesso à privacidade de usuários envolvidos neste crime hediondo, sendo este um ponto passivo na construção de uma ética da conectividade em rede. Porém, mesmo a privacidade de conversas íntimas de cunho sexual entre dois adultos também estaria dentro do radar do algoritmo.

Além das polêmicas envolvendo a privacidade dos usuários e as chances de erro do algoritmo, a ideia de se poder vasculhar as imagens (ou mensagens) levantou questionamentos sobre os possíveis usos de tais ferramentas. Uma vez que mecanismos de quebra da criptografia e de vasculhamento das imagens e mensagens em cada dispositivo eletrônico são criados, mesmo que para finalidades honestas e necessárias, como o combate ao abuso infantil, inevitavelmente essas mesmas ferramentas poderiam ser utilizadas e reprogramadas para outros objetivos, como perseguição política, por exemplo. Mesmo que a Apple, por exemplo, atualmente se recuse a implementar mudanças que promovam tal uso persecutório, nada garante que no futuro essa postura seja mantida ou que outros não o façam – uma vez que o recurso é criado, seu uso se torna incontrolável. Para usarmos uma analogia e uma discussão que se popularizaram recentemente, é como se estivéssemos julgando Oppenheimer e seus estudos sobre a física nuclear: um cientista poderia ser responsabilizado pelo uso que se faz de suas descobertas? Ou, ainda, se o fizesse com boas intenções e alguém posteriormente deturpasse seu uso, poderia o cientista ser responsabilizado? Não há, infelizmente, respostas simples a dilemas.

Por uma ética dos algoritmos

Pierre Lévy (1999) é um dos mais destacados pesquisadores no campo da conectividade e suas implicações na sociedade contemporânea. Sua obra *Cibercultura* constitui um ponto de partida essencial para entender as dinâmicas sociais da cultura digital. Um dos aspectos mais intrigantes do livro aborda precisamente o impacto das tecnologias na sociedade. Lévy, com perspicácia, propõe a questão de forma interrogativa: existe, de fato, um impacto?

Ao acessar suas redes sociais favoritas, entre as postagens de seus contatos, surgem sugestões de vídeos e imagens potencialmente de interesse do usuário. Em grande parte dos casos, essas sugestões são realmente atraí-tivas, e aquelas que não despertam seu interesse são rapidamente ignoradas, reduzindo a probabilidade de visualizações futuras. Quando decide descansar do celular e ligar a televisão, utilizando seu serviço de streaming preferido, o objetivo do usuário é relaxar e assistir a algo interessante. Na tela, diversas opções são apresentadas; mesmo que não correspondam exatamente às suas preferências, parecem selecionadas especificamente para o usuário. Ao assistir uma recomendação e não gostar, é possível marcar com um “dislike”, diminuindo a ocorrência de sugestões similares no futuro.

Embora numerosos exemplos desse fenômeno possam ser citados, limitamo-nos a estes dois, provavelmente os mais familiares ao público em geral. O mecanismo subjacente a esse processo é constituído por algoritmos. De maneira simplificada, algoritmos são fórmulas, cálculos e diretrizes incorporados em toda a internet, com o propósito de otimizar e personalizar a experiência do usuário durante a navegação.

Como isso é viabilizado? Através do recurso mais valioso em uma sociedade conectada: os dados. Paradoxalmente, esse recurso é entregue voluntariamente por nós a empresas como Google, Amazon, Facebook e Twitter. Essas empresas coletam informações dos usuários e as comercializam para outras corporações, que utilizam esses dados para veicular anúncios direcionados. Dessa forma, uma pesquisa por um tênis da marca X no Google pode resultar em anúncios dessa marca sendo exibidos em vídeos do YouTube que você assiste.

Assim como qualquer espaço físico e público, o mundo digital é igualmente produzido, criado e mantido por seres humanos. E é importante salientar

o termo “mundo digital” em oposição a “mundo virtual”, uma vez que a palavra “virtual”, conforme definido pelo dicionário Aurélio, significa “1. que existe como potência, mas não realmente. 2. Com possibilidade de realizar-se” (FERREIRA, 2004, p. 819). Nós, que estamos conectados, compreendemos claramente que as ocorrências na rede têm consequências reais. No mundo digital, as desigualdades também estão presentes e são tão prejudiciais quanto no ambiente físico.

Um exemplo elucidativo é um levantamento realizado pela Infobase/Interativa⁹ em 2021, que destaca uma característica da inteligência artificial pouco conhecida: o racismo. Os dados coletados revelam que, em 2015, o algoritmo do Google identificou pessoas negras como resultados da busca pelo termo “gorila”. Em 2021, o algoritmo do YouTube desmonetizou vídeos que abordavam a temática Black Lives Matter. No Twitter, o algoritmo tende a privilegiar usuários com fotos de perfil de pessoas brancas em comparação com pessoas negras. No Brasil, os sistemas de reconhecimento facial exacerbam o racismo algorítmico: mais de 90% dos indivíduos encarcerados identificados por esses sistemas de segurança são negros. Os algoritmos tendem a reproduzir os preconceitos comuns da sociedade (O’NEIL, 2020), replicando e reforçando “crenças racistas e sexistas de sociedades em que os mecanismos de busca operam” (NEMER, 2021, p. 23).

No contexto dos sites de compartilhamento, O’Neil (2020) argumenta que os algoritmos das redes sociais são projetados exclusivamente para gerar audiência. Ela observa, por exemplo, que comentários e ‘emojis’ de raiva geram mais engajamento do que os de felicidade. A razão é evidente: os desenvolvedores querem que o usuário passe mais tempo utilizando o serviço, ampliando as oportunidades de vendas (seja de produtos ou de ideias). É crucial enfatizar que os algoritmos não são exclusivos das mídias sociais ou de navegadores como o Google Chrome. Eles são amplamente utilizados por bancos, empresas e governos. Um exemplo fornecido por O’Neil é o caso da Amazon, que desenvolveu um algoritmo para a seleção de novos engenheiros que excluía mulheres das etapas mais avançadas do processo seletivo. O padrão inserido

⁹ O infográfico está disponível em <https://infobase.com.br/inteligencia-artificial-e-a-perpetuacao-do-racismo/>

no algoritmo privilegiava homens brancos, oriundos de faculdades renomadas e com histórico de promoções em curto prazo.

Enfim, retomemos a questão de Lévy: a tecnologia produz impactos?

O primeiro aspecto a ser considerado é que nenhuma tecnologia é alheia ao contexto histórico, cultural e social. As tecnologias não surgem de forma isolada ou desvinculada do seu tempo; são, fundamentalmente, frutos de anseios e necessidades inerentes ao cotidiano das pessoas. Analogamente ao mito de Prometeu, que trouxe o fogo aos mortais, a roda não foi um presente de seres extraterrestres compadecidos com os humanos que se esforçavam arduamente para transportar cargas. Pelo contrário, foi a necessidade de uma locomoção mais eficiente que impulsionou a humanidade a criar um mecanismo capaz de suprir tal deficiência. Uma vez inventada, a roda desencadeou uma verdadeira revolução. A maior velocidade, aliada ao menor esforço físico, proporcionou uma nova dinâmica social, transformando e revolucionando a sociedade da época. Essa transformação, por sua vez, gerou novas necessidades, que impulsionaram novamente a humanidade a desenvolver novas tecnologias, cada uma trazendo consigo novas revoluções e transformações sociais.

Não podemos separar o mundo material - e menos ainda sua parte artificial - das ideias por meio das quais os objetos técnicos são concebidos e utilizados, nem dos humanos que os inventam, produzem e utilizam. Mesmo supondo que realmente existam três entidades - técnica, cultura e sociedade -, em vez de enfatizar o impacto das tecnologias, poderíamos igualmente pensar que as tecnologias são produtos de uma sociedade e de uma cultura (LÉVY, 1999, p. 22)

Essa explicação não sugere que a história é cíclica, mas sim ilustra como há uma relação entre sociedade e tecnologia. A sociedade cria a tecnologia, que por sua vez transforma a sociedade e lhe impõe novos desafios. A análise de Lévy aplica-se perfeitamente aos algoritmos. Por mais que sejam por vezes utilizados como ferramentas de controle e direcionamento por grupos sobre os usuários, os algoritmos foram concebidos pela própria sociedade como instrumentos destinados a melhorar e proporcionar conforto diante das necessidades cotidianas.

A questão crucial reside nos usos que essa ferramenta recebe por parte dos seres humanos. Nenhuma tecnologia é intrinsecamente boa ou má, nem mesmo aquela que possibilitou a criação da bomba nuclear. A tecnologia não

possui moral ou ética; essa reside no ser humano que a manipula (LÉVY, 1999). Chegamos, então, a um ponto fundamental: a necessidade de formular uma ética do uso de dados que garanta a integridade das informações dos usuários contra o uso criminoso. Ao contrário da percepção dos usuários das décadas de 1990 e 2000, a internet não é um território sem lei.

Quem asseguraria tal garantia? Diversos Estados já empreenderam iniciativas neste sentido. No Brasil, destaca-se o Marco Civil da Internet (Lei nº 12.965/2014), que regulamenta e define os direitos e deveres dos usuários na rede mundial de computadores. Mais recentemente, em 14 de agosto de 2018, o então presidente Michel Temer sancionou a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que entrou em vigor em 18 de setembro de 2020, com a aplicação de multas e sanções iniciando-se em agosto de 2021. O principal objetivo da LGPD é proporcionar um maior controle das pessoas sobre suas próprias informações. A legislação estabelece normas rigorosas para empresas e organizações no que tange à coleta, uso, armazenamento e compartilhamento de dados pessoais, impondo severas penalidades em casos de descumprimento.

Mas o que se entende por dados pessoais? Não se trata apenas de informações como nome, endereço ou dados bancários, mas, sobretudo, de *cookies*¹⁰ e outras informações de navegação que são comercializadas com empresas de publicidade. A LGPD elenca onze princípios que as organizações devem observar no tratamento de dados. Esses princípios constituem um conjunto de “melhores práticas”, funcionando como uma espécie de ética aplicada aos algoritmos. A estrutura da LGPD foi inspirada no GDPR (General Data Protection Regulation), que entrou em vigor em 2020 e regulamenta a proteção de dados nos países europeus.

Dados possuem um valor inestimável, pois geram enormes possibilidades de lucro para empresas que operam na web. Não se trata de uma invasão internacional aos dados pessoais dos usuários, em conformidade com teorias conspiratórias em voga. Cada indivíduo já fornece essas informações, de forma

¹⁰ Cookies de HTTP, ou cookies da Internet, são desenvolvidos especificamente para que navegadores da Web rastreiem, personalizem e salvem informações sobre a sessão de cada usuário.

voluntária, para gigantes norte-americanas da internet, como Facebook e Google. Os desafios enfrentados pela sociedade civil, neste estágio da civilização humana pós-revolução digital, são dois: Primeiro, educar para a conectividade, incluindo nisso a parcela da população mundial excluída dos processos conectivos em rede, permitindo-lhe compreender as nuances de estar digitalmente integrado. Segundo, tal como Aristóteles o fez, perambulando com seus discípulos em práticas peripatéticas, devemos hoje refletir sobre a ética, talvez uma nova ética, que contemple e regule nossas relações no mundo digital.

Incluir aqueles que estão excluídos do mundo digital seria apenas o início do enfrentamento ao primeiro desafio, mas estaria longe de ser o suficiente. A pandemia de COVID-19 acelerou o processo de digitalização a um nível que talvez não se pudesse esperar ocorrer em tão pouco tempo. Durante o período pandêmico, diversos setores, processos e serviços se digitalizaram ao máximo que puderam, seja pela comodidade de se fazer tudo de forma remota, seja pela redução de custos. Desta forma, ter um dispositivo eletrônico com acesso à internet acabou se tornando imprescindível à vida em comunidade: um exemplo que pode facilmente vir à mente do leitor é o uso do Pix para a realização de pagamentos. Contudo, há outro exemplo mais pertinente: na rede de ensino municipal de Aracaju, com exceção daqueles que desejam continuar na mesma unidade de ensino, todos os outros devem fazer a matrícula de forma *online* (para os casos de transferência interna, alunos novos e vagas remanescentes). Para quem não tem acesso à internet, a Prefeitura informa que todas as escolas da rede municipal contam com Wi-Fi gratuito que pode ser utilizado para a realização da matrícula e, em caso de dúvidas, possui ainda um canal de atendimento via telefone ou WhatsApp. Embora forneça acesso à internet, nada é dito quanto ao caso de alguém não ter um dispositivo eletrônico para poder ir às escolas realizar a matrícula, do que se imagina que tal pessoa ficaria excluída do acesso à educação. Isto é, ter um dispositivo eletrônico com acesso à internet torna-se, cada vez mais, um requisito para o exercício da cidadania.

O processo de inclusão, contudo, não deve ser pensado meramente em termos quantitativos, isto é, em simplesmente fornecer acesso à internet àqueles que não o têm. A inclusão precisa ser pensada em termos sobretudo qualitativos, entendendo-se por isto fornecer o acesso às ferramentas tecnológicas e ensiná-las a usar essas ferramentas para que possam propriamente participar

da vida digital – o que joga luz para o papel da educação neste processo de inclusão. Se as instituições de ensino têm a tarefa de formar cidadãos e preparar para o mercado de trabalho, faz-se imprescindível repensar os currículos em razão desta nova realidade imposta pelo avanço tecnológico. Não se trata de entrar naqueles discursos vazios de que os currículos escolares são engessados ou que a escola não prepara para a vida, menos ainda de “flexibilizar” com itinerários formativos, mas reconhecer que a sociedade mudou, a tecnologia promoveu mudanças revolucionárias em nossa forma de viver e, diante deste novo cenário, uma educação tecnológica se faz necessária.

Essa educação digital, contudo, não deve se limitar a ensinar a usar um computador, o pacote *Office* ou aquilo que normalmente se ensina num curso de informática básica. Esses conhecimentos são necessários e devem fazer parte dessa educação, mas este não deve ser o seu objetivo; a educação tecnológica deve ter como fim o uso crítico das ferramentas digitais, como entender qual o uso adequado de cada ferramenta (por exemplo, Google para fazer buscas e ChatGPT para simular conversas) e saber realizar checagem de fatos. Estes dois pontos se tornam cruciais tanto para o mercado de trabalho quanto para a vida em comunidade: uma pessoa pode usar a inteligência artificial a seu favor, por exemplo, facilitando seu trabalho de forma inteligente, somente se souber usá-la da forma adequada e com o propósito para o qual foi criada. A checagem de fatos, por sua vez, atenderia ao propósito de combater falsas narrativas políticas, é certo, mas em determinados casos poderia, literalmente, salvar vidas, blindando as pessoas de conteúdo desinformativo sobre saúde. O uso crítico das ferramentas digitais e a checagem de fatos não seriam exclusivos de uma única disciplina nova pensada especificamente à educação digital, podendo ser desenvolvidos pelas disciplinas já tradicionais dos currículos. Nesse aspecto, as disciplinas da área de Ciências Humanas em específico teriam uma contribuição indispensável a este processo: tomemos como exemplo a disciplina de Filosofia, que, ao abordar temas como Lógica, Epistemologia e Filosofia da Ciência, poderia fornecer as bases de raciocínio de um uso propriamente crítico das ferramentas digitais e da checagem de fatos. Evidentemente, uma disciplina pensada exatamente com o objetivo de se voltar à educação digital contribuiria ao processo formativo e poderia ser um ótimo complemento; mas as disciplinas tradicionais já seriam capazes de contribuir com esse processo educativo.

Parte dessa educação digital passaria, inevitavelmente, por uma reflexão ética sobre como deveríamos nos portar nesse novo mundo. Das teorias benthamiana e foucaultiana sobre o panóptico, passando pela sociedade do espetáculo debordiana a modernidade líquida de Bauman e pelas análises de Byung-Chul Han (apenas para citarmos alguns exemplos), as Ciências Humanas teriam um papel fundamental neste processo pela sua capacidade de proporem questionamentos e reflexões capazes de ecoar no modo como as pessoas lidam com a tecnologia.

O pensar numa nova ética para o mundo digital não exige, necessariamente, a desconsideração de outras concepções éticas já existentes. Seria possível adaptá-las, atualizá-las, tomá-las como base para se pensar nas novas dinâmicas da realidade; tomemos como exemplo a ética kantiana do imperativo categórico: embora formulada há alguns séculos, em que nem se imaginava a existência de algo como a internet, seus princípios não são incompatíveis com o mundo digital, pois as máximas basilares da ética kantiana poderiam se estender às redes sociais. Como exemplo, o princípio kantiano de agir como se toda ação pudesse valer como lei universal ainda teria validade para guiar a conduta humana nas redes, bem como o de tratar outro humano como um fim em si mesmo, não como um meio.

Contudo, um elemento deveria ser tido como imprescindível para qualquer reflexão ética no mundo digital consistiria na abrangência das ações humanas. Com o advento e popularização das redes digitais, o que uma pessoa faz não fica mais contido em um insignificante recorte do espaço-tempo, podendo atingir um número muito maior de pessoas e se prolongar por mais tempo que o desejado. Não que qualquer coisa que qualquer pessoa faça necessariamente repercuta entre dezenas de milhões de pessoas, mas deve-se ter em mente que existe a possibilidade de se alcançar um número maior de pessoas; um exemplo é o caso de uma passageira de avião que se recusou a dar seu lugar a uma criança, foi filmada e sua ação não ficou contida no espaço da aeronave e no instante em que aquilo aconteceu, repercutindo em todo o país, tanto na internet quanto em importantíssimos jornais na televisão.

Essa maior abrangência das ações implica na necessidade de um maior cuidado e responsabilidade por parte de seus agentes, uma vez que essas condutas podem repercutir e tomar proporções muito maiores que o desejado. Uma

fala descompromissada de alguém, sem embasamento algum, pode atingir um número de pessoas inimaginável a seu autor; uma reação impensada de alguém pode trazer consequências mais sérias do que ocorreria antigamente, quando as chances de mais pessoas tomarem conhecimento eram mínimas. Assim, autocontrole, responsabilidade e maturidade vão se tornando valores nevrálgicos dessa nova ética, devendo ser enfatizados em um processo educativo digital.

Para Piercarlo Maggiolini, há um “princípio unificante” nessa nova ética digital que descreve o uso e a difusão da tecnologia da informação [...] baseado em dois fatores relacionados à necessidade da informação e das suas tecnologias: um que podemos chamar de complexidade técnica e outro de complexidade política. O primeiro é diretamente proporcional ao nível de complexidade dos processos (e dos fenômenos) que se quer conhecer e controlar, seja numa organização, na economia ou na sociedade. O segundo é inversamente proporcional ao nível de confiança entre os agentes envolvidos nesses processos. (MAGGIOLINI, 2014, p. 586)

Ainda seguindo Maggiolini (2014), podemos dizer que a obra de Platão, “Fedro”, oferece um insight valioso sobre a questão que ora analisamos, por meio do diálogo entre o rei do Egito e Theuth, o deus que inventou a escrita, a primeira tecnologia da informação da humanidade.

Quando Theuth apresentou sua invenção, ele afirmou: “Este é um ramo do conhecimento, rei, que tornará os Egípcios mais sábios e com melhor memória. Na verdade, foi descoberto o remédio da memória e da sabedoria”. O rei, no entanto, respondeu: “Ó engenhosíssimo Theuth, um homem é capaz de criar os fundamentos de uma arte, mas um outro deve julgar que parte de dano e de utilidade possui para quantos dela vão fazer uso. Ora tu, neste momento, como pai da escrita que és, apontas-lhe, por lhe queres bem, os efeitos contrários àqueles de que ela é capaz” (MAGGIOLINI, 2014, p. 590).

Cada nova tecnologia da informação certamente avança a história da civilização humana. Seus “inventores” e aqueles com interesses, especialmente econômicos, em sua adoção e difusão, destacam seus benefícios para a economia, a sociedade e a humanidade. No entanto, é necessário que alguém, como o “rei do Egito”, que encarne a consciência crítica e a ética da humanidade, avalie os potenciais danos e utilidades antes que se manifestem de forma irreversível ou

demasiado custosa para reparar. Este papel de julgamento e divulgação dessa consciência é essencial na era da informação.

REFERÊNCIAS

BBC. Como os dados de milhões de usuários do Facebook foram usados na campanha de Trump. BBC News Brasil, abril de 2018. Disponível em: <https://www.bbc.com/portuguese/geral-43705839>. Acesso em: 04/03/2021

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD) (Redação dada pela lei n. 13.853, de 2019). Brasília, DF: Diário Oficial da União, 2019.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO - CETIC. TIC Domicílios 2023. Disponível em: <https://cetic.br/pt/pesquisa/domicilios/indicadores/>, acesso em: 15/06/2024.

FERREIRA, Aurélio Buarque de Holanda. **Miniaurélio: o minidicionário da Língua Portuguesa**, coord. de edição Margarida dos Anjos. 6a edição atualizada. Curitiba: Positivo, 2004.

FÍGARO, Roseli. O mundo do trabalho e as organizações: abordagens discursiva de diferentes significados. **ORGANICOM**, ano 5, n. 9, 2º semestre de 2008.

FLORES, Daniela F. Milon; CORDEIRO, Robson L. F. How to take advantage of behavioral features for the early detection of grooming in online conversations. **ScienceDirect**, volume 240, 15 mar. 2022. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0950705121011187>. Acesso em 16/06/2024.

MAGGIOLINI, Piercarlo. Um aprofundamento para o conceito de ética digital. **RAE**, São Paulo, V. 54, n. 5, set-out 2014, 585-591.

NAPOLITANO, Marcos. **1964: História do Regime Militar Brasileiro**. São Paulo: Contexto, 2014.

NEMER, David. **Tecnologia do Oprimido: desigualdade e o mundano digital nas favelas do Brasil**. Vitória: Editora Milfontes, 2021.

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

PARLAMENTO DO REINO UNIDO. Lei governamental. Disponível em: <https://bills.parliament.uk/bills/3137>, acesso em 16/06/2024.

PATRÍCIO, Nathalia Sautchuk. Por que o client-side scanning é uma preocupação para a criptografia?. **Medium**, 2021. Disponível em: <https://medium.com/cryptomap-fgv-cepi/por-que-o-client-side-scanning-%C3%A9-uma-preocupacao%C3%A7%C3%A3o-para-a-criptografia-68336cc5da7b>, acesso em 16/06/2024.

PAUL, Christopher; MATTHEWS, Miriam. The Russian "Firehose of Falsehood" Propaganda Model. **Rand**, 2016. Disponível em: <https://www.rand.org/pubs/perspectives/PE198.html>, acesso em 16/06/2024.

RIBEIRO, Ricardo de Queirós Batista; RIBEIRO, Silvar Ferreira. Guerra de Informação: entendendo o conceito a partir de uma revisão sistemática do período de 2010 a 2020. **Revista Agulhas Negras**, Resende, Vol. 5, Nº. 6, p. 135-148, Ano 2021

RÜDIGER, F. Eugen Hadamovsky e a teoria da propaganda totalitária na Alemanha nazista. **Galaxia**, São Paulo, n. 27, p. 48-60, jun. 2014. Disponível em: <<https://www.scielo.br/j/gal/a/TBVFkVWVHMMdrHB3BBn3TS8h/#>>, acesso em 16/06/2024.

SIMÃO, Renan Borges. Firehosing: por que fatos não vão chegar aos bolsonaristas. **Le Monde Diplomatique**, ed. 137, 14 de janeiro de 2019. Disponível em: <<https://diplomatie.org.br/firehosing-por-que-fatos-nao-vaao-chegar-aos-bolsonaristas/>>, acesso em: 16/06/2024.

VIEIRA, Ana Paula Leite. **O Departamento de Imprensa e Propaganda e a política editorial do Estado Novo (1937-1945)**. Tese (Doutorado) - Universidade Federal do Estado do Rio de Janeiro, Programa de Pós-Graduação em História, 2019.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. Relatório. Disponível em: <<https://www.itu.int/en/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx>>, acesso em: 15/06/2024.

OECD. A broken social elevator? How to promote social mobility. Relatório. Disponível em: <https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/06/a-broken-social-elevator-how-to-promote-social-mobility_g1g8e196/9789264301085-en.pdf>. Acesso em: 10/03/2025.

LABATE, Alice. 'Geração digital' tem dificuldade ao usar computadores e enfrenta desafios no mercado de trabalho. **Estadão**, março de 2024. Disponível em: <https://www.estadao.com.br/link/cultura-digital/geracao-digital-tem-dificuldade-ao-usar-computadores-e-enfrenta-desafios-no-mercado-de-trabalho/?rslltid=AfmBOoppCoSHBjr92dgE_9QpKie6h_jB4bhQmxYoVTN-OU7X37G4l8j1>. Acesso em: 10/03/2024.

PILAGALLO, Sofia. 'Ela não conhecia Ctrl C + Ctrl V': geração Z pena com PC e assusta chefes. **Tilt UOL**, junho de 2024. Disponível em: <<https://www.uol.com.br/tilt/noticias/redacao/2024/06/10/ela-nao-sabia-ctrl-c--ctrl-v-geracao-z-pena-com-computador-no-trabalho.htm>>. Acesso em: 10/03/2025.

ROSA, Vika. "Eles nem sabem copiar e colar": especialista afirma que jovens não têm domínio básico sobre computadores. **IGN Brasil**, dezembro de 2023. Disponível em: <<https://br.ign.com/tech/118013/news/eles-nem-sabem-copiar-e-colar-especialista-afirma-que-jovens-nao-tem-dominio-basico-sobre-computador>>. Acesso em: 10/03/2025.

INTRIERI, Laura. Geração Z não é tão digital quando se trata de trabalho, dizem especialistas. **Terra**, março de 2024. Disponível em: <<https://www.terra.com.br/byte/geracao-z-nao-e-tao-digital-quando-se-trata-de-trabalho-dizem-especialistas,24334c5af8a0620f58f35c7429cf73c8zds7btbp.html>>. Acesso em: 10/03/2025.

MATHIAS, Viny. Geração Z cresceu com a Internet e se sente confortável com a tecnologia, só não peça a eles que usem o Excel. **IGN Brasil**, janeiro de 2025. Disponível em: <<https://br.ign.com/tech/134738/news/geracao-z-cresceu-com-a-internet-e-se-sente-confortavel-com-a-tecnologia-so-nao-peca-a-eles-que-usem>>. Acesso em: 10/03/2025.

DEMOPOULOS, Alaina. "Scanners are complicated": why Gen Z faces workplace 'tech shame'. **The Guardian**, fevereiro de 2023. Disponível em: <<https://www.theguardian.com/technology/2023/feb/27/gen-z-tech-shame-office-technology-printers>>. Acesso em: 10/03/2025.

DUARTE, Marcella. Apple vai vigiar minhas fotos? Entenda o filtro contra pornografia infantil. **Tilt UOL**, agosto de 2021. Disponível em: <<https://www.uol.com.br/tilt/noticias/redacao/2021/08/11/apple-vai-vigiar-minhas-fotos-entenda-o-filtro-contr-pornografia-infantil.htm>>. Acesso em: 10/03/2025.

BROGAN, Caroline. Proposed illegal image detectors on devices are 'easily fooled.' **Imperial News**, novembro de 2021. Disponível em: < <https://www.imperial.ac.uk/news/231778/proposed-illegal-image-detectors-devices-easily/>>. Acesso em: 10/03/2025.

BROGAN, Caroline. Privacy gaps in Apple's data collection scheme revealed. **Imperial News**, setembro de 2025. Disponível em: < <https://www.imperial.ac.uk/news/239752/privacy-gaps-apples-data-collection-scheme/>>. Acesso: 10/03/2025.

TRATAMENTO DE DADOS PESSOAIS EM OPERAÇÕES DE M&A: UM ESTUDO SOBRE AS BASES LEGAIS APLICÁVEIS E AS MEDIDAS TÉCNICAS E ADMINISTRATIVAS ADOTADAS PARA CONFORMIDADE COM A LEGISLAÇÃO

Allan Nascimento Turano

Doutorando em Propriedade Intelectual e Inovação
pela Academia do INPI, Mestre em Direito pela
UNIRIO, Bacharel em Direito pela UFRJ

João Gabriel de Oliveira Freitas

Bacharel em Direito pela UFRJ, Conselheiro da LADS/
UFRJ

RESUMO

As operações de Fusões e Aquisições (M&A) envolvem intensa troca de informações entre as partes, especialmente nas fases de negociações preliminares e auditoria (*due diligence*), em que há formação de diretórios físicos ou digitais (*data rooms*). Nesse contexto, além de informações protegidas por segredo industrial e comercial, é comum o compartilhamento de dados pessoais, o que impõe às partes o dever de conformidade com as normas aplicáveis no Brasil, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD). Este artigo analisa as medidas jurídicas, operacionais e técnicas que devem ser adotadas para assegurar a licitude do tratamento de dados pessoais ao longo da operação. Discute-se a suficiência dos acordos de confidencialidade e a necessidade de enquadramento do tratamento em uma das bases legais previstas na LGPD, considerando os entraves práticos do consentimento. Examina-se a viabilidade de se adotar a execução de contrato, a proteção do crédito e o legítimo interesse como fundamentos legais para o tratamento. Investiga-se, ainda, os procedimentos necessários para transferências internacionais de dados. Por fim, o estudo propõe um conjunto de medidas técnicas e administrativas que complementam a governança jurídica da operação, a fim de mitigar riscos e garantir a segurança das informações. A pesquisa adota o método dedutivo, possui caráter exploratório e analítico, e se desenvolve por meio de revisão bibliográfica, análise da legislação e exame empírico a partir de declarações de boas práticas de governança de dados.

palavras-chave: tratamento de dados pessoais; fusões e aquisições; auditoria jurídica; bases legais.

ESTRUTURAÇÃO DE UMA OPERAÇÃO DE M&A

Motivadores para realização de uma operação

A decisão de realizar uma operação de M&A¹ não é tomada de forma aleatória ou exclusivamente oportunista pelas partes envolvidas. Trata-se de um movimento estratégico, frequentemente ancorado em um conjunto de fatores econômicos, concorrenciais, operacionais e financeiros que justificam a reestruturação societária. Tais operações são instrumentos de reorganização empresarial capazes de gerar sinergias, ganhos de eficiência e reposicionamento competitivo².

Dentre os principais vetores motivacionais, destacam-se as economias de escala e de escopo. A reorganização ou combinação de negócios permite o compartilhamento de estruturas, tecnologias e redes de distribuição, diluindo custos fixos sobre uma base ampliada de receitas. Além disso, a integração de portfólios complementares viabiliza ganhos de escopo, ampliando a gama de produtos ou serviços ofertados ao mercado, sem a necessidade de duplicação de estruturas administrativas e operacionais³.

Outro motivador relevante consiste na ampliação do poder de mercado. Por meio da consolidação empresarial é possível aumentar a capacidade de barganha frente a fornecedores e distribuidores, além de fortalecer a presença territorial ou setorial da sociedade companhia. A aquisição de concorrentes ou de empresas que operam em segmentos adjacentes pode permitir acesso mais rápido a novos mercados ou a carteiras de clientes, reduzindo significativamente os custos de entrada e os riscos de expansão orgânica⁴.

¹ M&A é a abreviação de Mergers & Acquisitions, conjunto de operações que usualmente são traduzidas para o português como Fusões e Aquisições. Compreende uma vasta gama de negócios jurídicos, do que são exemplos operações de compra e venda de participações societárias, de estabelecimento empresarial ou operações de reorganização societária, como transformação, incorporação, cisão, fusão e dropdown.

² BOTREL, Sérgio. Fusões & Aquisições. São Paulo: Saraiva, 2012, pp. 26-39.

³ Ibidem. p. 27.

⁴ "Operações de concentração que implicam a aquisição por uma empresa de outra que, embora produzindo o mesmo tipo de produto, atua em diverso mercado relevante geográfico, são denominadas 'expansões de mercado'. Já as concentrações que envolvem 'expansão de produto' referem-se à união de empresas produtoras de bens complementares por natureza." Cf. FORGIONI, Paula Andrea. Os Fundamentos do Antitruste. 7ª ed. São Paulo: Editora Revista dos Tribunais, 2014, p. 404.

As operações de M&A também podem ser impulsionadas por razões financeiras e especulativas. A valorização de ativos, a busca por economia tributária e a gestão eficiente de passivos são frequentemente citados como fatores adicionais de incentivo. Em períodos de crise ou reestruturação econômica, sociedades em dificuldades podem ser adquiridas⁵ por valores abaixo de seu valor patrimonial ou de mercado, representando oportunidades estratégicas para investidores com apetite por risco e capacidade de recuperação empresarial⁶.

Não menos relevante é a motivação relacionada à inovação e à substituição de processos internos de pesquisa e desenvolvimento (P&D). Empresas que enfrentam desafios em seus ciclos de inovação ou que desejam internalizar *know-how* específico podem recorrer à aquisição como mecanismo de rejuvenescimento ou ampliação tecnológica. Nesses casos, o M&A funciona como forma de incorporação de novos ativos intangíveis, como marcas, desenhos industriais, modelos de utilidade, patentes ou capital intelectual em geral, muitas vezes mais eficiente que a criação e o desenvolvimento interno desses ativos.

Por fim, há motivações defensivas, voltadas à preservação da posição estratégica da sociedade ou companhia⁷. Isso inclui a prevenção de movimentos hostis de concorrentes, a proteção contra aquisições predatórias e a limitação do ingresso de novos *players* no mercado.

⁵ "Dentre as operações de reorganizações societárias como meios de recuperação judicial de empresas, a transformação da recuperanda ou constituição de novas sociedades, alteração do controle societário e substituição ou modificação da administração da recuperanda são as operações implementadas com maior frequência." Cf. FERREIRA, Arnaldo Vieira. Reorganizações Societárias como Meios de Recuperação Judicial. São Paulo: Quartier Latin, 2024, p. 16.

⁶ SADDI, Jairo (Org.). Fusões e aquisições: aspectos jurídicos e econômicos. São Paulo: IOB, 2002. p. XIV.

⁷ Alguns exemplos de M&A como medidas de defesa são as operações com cavaleiro branco (*white knight* e escudeiro branco (*white squire*)), como explica João Pedro Nascimento: "O cavaleiro branco, usualmente referido por sua tradução em inglês *white knight*, é a medida defensiva adotada pela companhia-alvo, por meio da qual são convidados terceiros, amigáveis à administração e/ou a determinados grupos de acionistas relevantes da companhia-alvo, para realizarem oferta para a aquisição do controle da companhia-alvo impedindo que o adquirente hostil o faça." [...] "O escudeiro branco, usualmente referido por sua tradução em inglês *white squire*, é a medida defensiva adotada pela companhia-alvo por meio da qual são convidados terceiros, amigáveis à administração e/ou a determinados grupos de acionistas relevantes da companhia-alvo, para adquirirem participação acionária, a fim de apoiar a administração e/ou determinados grupos de acionistas relevantes da companhia-alvo, fazendo com que esta se sinta mais protegida contra ofertas hostis. Sua existência desestimularia a oferta hostil pela dificuldade e pelo alto preço que eventual ofertante teria que pagar para a obtenção do controle." Cf. NASCIMENTO, João Pedro Barroso do. Medidas Defensivas à Tomada de Controle de Companhias. São Paulo: Quartier Latin, 2011, pp. 167-170.

Tais motivações revelam o caráter multifacetado das operações de M&A, cuja racionalidade vai além da simples soma de ativos, exigindo análise jurídica, econômica e estratégica integrada⁸.

Fases

As operações de M&A geralmente seguem um percurso dividido em múltiplas fases interdependentes, sendo possível identificar etapas pré-contratuais, contratuais e pós-contratuais. O ciclo tem início com as tratativas preliminares, envolvendo reuniões com assessores jurídicos, financeiros e contábeis, bem como a celebração de um acordo de confidencialidade (*Non Disclosure Agreement - NDA*) para resguardar o sigilo do levantamento de informações estratégicas sobre a potencial sociedade-alvo. Tais tratativas precedem a assinatura de qualquer documento vinculante, embora possam ensejar compromissos negociais limitados por meio de instrumentos como cartas de intenção (*Letter of Intent - Lol*) e memorandos de entendimento (*Memorandum of Understanding - MoU*), que formalizam os termos essenciais da negociação em caráter preliminar.

Esses documentos que antecedem os contratos e atos societários definitivos de uma operação de M&A cumprem relevante papel funcional: delimitam o escopo das negociações, estabelecem eventuais compromissos de exclusividade ou outras boas práticas, e servem de base para a condução de auditorias jurídicas e financeiras. A Lol, geralmente unilateral, manifesta o interesse de uma das partes em adquirir participação societária. Já o MoU tende a assumir caráter bilateral, consolidando pontos de convergência entre as partes e estabelecendo, de forma sintética, os termos econômicos e jurídicos principais que nortearão a negociação do contrato definitivo.

A mera celebração de um NDA, Lol ou MoU não pressupõe adequação à LGPD, tendo em vista que suas respectivas formatações tradicionais não contemplam cláusulas de proteção de dados. Dessa forma, é de suma importância a inclusão dessas cláusulas ou a celebração de um documento apartado, como um contrato de compartilhamento de dados (*data sharing agreement*),

⁸ BULGARELLI, Waldírio. Fusões, incorporações e cisões de sociedades. 4. ed. São Paulo: Atlas, 1999. p. 27.

especificando os dados pessoais envolvidos, o compartilhamento, o tratamento de dados e as responsabilidades das partes da negociação.⁹

Superada essa fase, dá-se início à *due diligence*, processo que consiste na auditoria jurídica, regulatória, contábil, financeira e operacional da sociedade-alvo. Essa etapa é essencial para avaliar riscos ocultos, passivos contingentes, litígios, conformidade regulatória e eventuais inadimplementos contratuais ou fiscais¹⁰, a partir de determinados critérios de relevância e materialidade¹¹.

A *due diligence* tem como objetivo: (i) reduzir a assimetria informacional entre comprador e vendedor, melhorando a compreensão do possível negócio que será adquirido pelo comprador; (ii) possibilitar ajustes no preço; (iii) avaliar os riscos da operação e do negócio; e (iv) reduzir a exposição do vendedor a eventuais reclamações do comprador¹². O procedimento de auditoria não é meramente técnico, mas também estratégico, pois pode impactar diretamente a estruturação do preço, a negociação e redação de cláusulas de garantias e indenizações, e até mesmo a decisão de seguir adiante com a operação ou dela desistir (*deal breaker*).

A realização da *due diligence* pressupõe a organização de um diretório (*data room*), que pode ser físico ou virtual. O *data room* físico é um espaço controlado, com acesso restrito, no qual documentos são disponibilizados à equipe de compradores/investidores. Contudo, o modelo mais adotado atualmente é o *data room* virtual, hospedado em plataformas seguras, que muitas vezes adotam medidas de segurança como autenticação de múltiplos fatores e restrição segmentada de acesso. Tal estrutura permite maior agilidade, flexibilidade e controle de acesso à informação, além de viabilizar o acompanhamento em tempo real da análise dos documentos pelas equipes envolvidas. É justamente

⁹ MARCO, Daniele Verza. Cláusulas de Confidencialidade e Proteção de Dados nas Negociações de Aquisição de Participação Societária. Revista Semestral de Direito Empresarial, n. 29, pp. 165-190, jul./dez. 2021, pp.184-185.

¹⁰ EIZIRIK, Nelson. M&A: regime societário e contratual. São Paulo: Quartier Latin, 2024. p. 299.

¹¹ A *due diligence* é uma representação da sociedade ou dos ativos alvo e como tal, possui limites. Normalmente, são adotados parâmetros como ações judiciais e contratos acima de determinado valor, bem como pesquisas por amostragem, tendo em vista que a auditoria possui circunscrição financeira, temporal, geográfica, dentre outras. Cf. MUNIZ, Joaquim de Paiva. Introdução às Operações de Compra e Venda de Participação Societária: Manual de M&A. São Paulo: Quartier Latin, 2024, p. 41.

¹² MUNIZ, Joaquim de Paiva. Introdução às Operações de Compra e Venda de Participação Societária: Manual de M&A. São Paulo: Quartier Latin, 2024, p. 39.

a fase que motiva o desenvolvimento do presente trabalho, pois enseja reflexões quanto à conformidade do compartilhamento dessas informações com a legislação brasileira.

Durante a análise das informações, é comum que novos elementos sejam incorporados aos instrumentos negociais. A depender dos achados da *due diligence*, os compradores/investidores podem pleitear ajustes nas condições econômicas, na distribuição de riscos ou na inclusão de cláusulas específicas de responsabilidade. A etapa também é marcada por intenso intercâmbio de minutas contratuais, onde as partes ajustam os limites da responsabilização, definem mecanismos de resolução de disputas, inserem cláusulas de ajustes de preço e condições suspensivas ou resolutivas.

Concluída a fase de diligência e negociação preliminar, as partes seguem para a formalização do contrato definitivo de aquisição, etapa que costuma demandar aprovações societárias da administração, deliberação em órgãos sociais e até mesmo eventual submissão à autoridades governamentais, bem como outros trâmites concorrenciais e regulatórios.¹³ Todo esse processo, que vai desde o interesse inicial à conclusão da operação, demonstra o alto grau de sofisticação e técnica exigido nas operações de M&A. É justamente esse amplo intercâmbio de informações, com compartilhamento não só entre as administrações internas dos agentes econômicos envolvidos, como também de diversos assessores externos, que demanda uma análise cautelosa sobre a conformidade legal sobre o tratamento de dados.

CONFORMIDADE DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS COM A LEGISLAÇÃO

Definições e escopo material e territorial

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, estabelece um regime jurídico de observância obrigatória nas operações que envolvem dados pessoais, inclusive no contexto de operações

¹³ ELIZIRIK, Nelson. M&A: regime societário e contratual. São Paulo: Quartier Latin, 2024, pp. 167-172.

de M&A. O art. 1º da LGPD fixa sua finalidade: proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Nesse sentido, uma vasta gama de atividades que envolve dados relacionados a pessoas naturais identificadas ou identificáveis deve ser submetida aos parâmetros da lei¹⁴.

Do ponto de vista material, a LGPD se aplica a toda operação de tratamento de dados pessoais, independentemente do meio ou da tecnologia utilizada. O conceito de tratamento, previsto no art. 5º, inciso X, é propositalmente amplo e exemplificativo, abrangendo desde a coleta, recepção e classificação, até o compartilhamento, transferência, acesso, reprodução e outras formas de uso de dados pessoais. Tal abrangência revela que mesmo operações preliminares em M&A, como a organização de *data rooms*, envio e disponibilização de documentos para *due diligence*, são caracterizados como tratamento de dados e, por isso, devem observar as normas legais, sobretudo a estipulação de bases legais, como explica Rony Vainzof:

Referida constatação de abrangência do conceito é de fundamental importância, pois o agente de tratamento, em absolutamente todas essas hipóteses, deverá manter registros das suas operações, bem como, no caso do controlador, avaliar o cumprimento de uma das bases legais previstas na Lei, o que implica dizer que um simples dado pessoal arquivado, mesmo que não seja processado, precisará ter um fundamento previsto na Lei para estar sob a responsabilidade do agente. Se o controlador não encontrar um embasamento jurídico para manter o dado pessoal consigo (ou com o operador), deverá eliminá-lo.¹⁵

No que se refere ao âmbito territorial, o art. 3º da LGPD determina que sua aplicação independe do local de sede do agente de tratamento, incidindo sempre que (i) a operação de tratamento for realizada no território nacional; (ii) a atividade tiver por objetivo a oferta de bens ou serviços a indivíduos localizados

¹⁴ A proteção de dados pessoais foi alçada a garantia fundamental pela Emenda Constitucional nº 115/2022, que incluiu o inciso LXXIX no art. 5º da Constituição Federal: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."

¹⁵ VAINZOF, Rony. Art. 5º. In: MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados Comentada. 2ª ed. São Paulo: Thomson Reuters, 2020, p. 108.

no Brasil; ou (iii) os dados tratados tenham sido coletados no país. A norma, portanto, adota critérios expansivos, de modo que operações transnacionais de M&A envolvendo empresas com qualquer ponto de contato com o território brasileiro também se sujeitam à sua disciplina.

A abrangência normativa exige das partes envolvidas em M&A uma análise cautelosa da cadeia de tratamento de dados que será desencadeada ao longo da operação. A disponibilização de cadastros, contratos de trabalho, lista de clientes e fornecedores, quando contiverem informações relacionadas a pessoas naturais, submete os agentes aos deveres legais previstos na LGPD. A análise de conformidade, portanto, deve ocorrer desde a fase preparatória da operação, especialmente se os dados forem acessados, compartilhados, processados ou de quaisquer outras formas tratados por terceiros, como assessores e consultores.

A definição de “tratamento” e os critérios de aplicação territorial impõem às operações de M&A uma necessária compatibilização com os princípios da LGPD, notadamente os da finalidade, necessidade, segurança, transparência e responsabilização. Assim, mesmo antes da formalização de um contrato definitivo de aquisição/investimento ou da consumação de um ato de reorganização societária, os agentes devem avaliar se o compartilhamento de dados observou os deveres de adequação e proporcionalidade, cabendo adotar medidas técnicas, jurídicas e administrativas para prevenir violações, demonstrar *accountability* e mitigar riscos regulatórios decorrentes da operação.

Bases legais para o tratamento de dados pessoais em operações de M&A

No contexto de operações de M&A, o tratamento de dados pessoais realizado durante qualquer das suas diversas fases, em especial nas tratativas preliminares e na *due diligence*, exige que se observe uma base legal prevista na LGPD. O art. 7º da referida norma elenca hipóteses legais que autorizam o tratamento de dados, sendo necessário, em cada situação, identificar aquela que melhor se adequa à finalidade e aos riscos envolvidos na operação.

A primeira base legal indicada pela LGPD é o consentimento do titular (art. 7º, I), que consiste em manifestação livre, informada e inequívoca, mediante a qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Apesar de parecer, à primeira vista, uma opção segura,

o consentimento enfrenta limitações práticas importantes no contexto de M&A. A obtenção do consentimento de colaboradores, clientes ou fornecedores pode ser logisticamente inviável e, em muitos casos, não é desejada pelas partes, pois pode comprometer a confidencialidade e o sucesso da operação. Isso porque sua divulgação prévia pode gerar insegurança no ambiente de negócios, como receio de desligamento, remanejamento de equipe, mudança de direção, ou até mesmo outros “burburinhos” que retirem dos colaboradores o foco nas suas atividades rotineiras. Da mesma forma, é possível que se comprometa o compartilhamento integral e fidedigno das informações necessárias para fins de avaliação na *due diligence* e o curso ordinário dos negócios durante o período entre a assinatura e o fechamento da operação.

Além disso, o consentimento é revogável a qualquer tempo pelo titular, nos termos do art. 8º, §5º da LGPD, o que fragiliza sua estabilidade como base jurídica para operações que podem levar meses de negociação. Em outras palavras, mesmo após a obtenção do consentimento, o titular pode retirar sua autorização, criando um risco jurídico para a continuidade do tratamento iniciado com base nesse fundamento. Por essas razões, o consentimento não é considerado a base legal mais adequada ou robusta para sustentar o tratamento de dados em operações de M&A.

Outra hipótese legal é o tratamento necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, conforme dispõe o art. 7º, V da LGPD. Essa base legal pode ser utilizada quando, por exemplo, há necessidade de tratar dados pessoais de sócios ou administradores da sociedade-alvo, cujos contratos envolvem cláusulas que preveem a alienação de participação societária. Contudo, ela exige vínculo contratual direto com o titular, sendo difícil sustentar sua aplicação ao tratamento de dados de terceiros não diretamente vinculados à transação, como colaboradores ou clientes da sociedade-alvo analisada.

Adicionalmente, a LGPD autoriza o tratamento de dados para fins de proteção do crédito (art. 7º, X). Tal base pode ser relevante em M&A quando há necessidade de consultar dados financeiros, históricos de inadimplência ou relacionamento com instituições de crédito, especialmente em operações que envolvam avaliação da solvência dos sócios da sociedade-alvo ou de seus fiadores. Contudo, seu uso deve observar a legislação específica aplicável ao sistema

de proteção ao crédito, como a Lei do Cadastro Positivo (Lei nº 12.414/2011), e deve ser restrito à finalidade estrita da análise de risco financeiro¹⁶.

Ressalte-se que nos casos de transferências internacionais de dados, como será abordado na seção seguinte, é necessário tanto indicar uma base legal para a transferência (art. 7 e 11 da LGPD) quanto para a própria transferência internacional, de modo específico (art. 33 da LGPD)¹⁷.

Uma das bases mais discutidas na prática de M&A é o legítimo interesse do controlador ou de terceiro (art. 7º, IX da LGPD), que autoriza o tratamento de dados pessoais sempre que necessário para atender interesses legítimos, desde que não prevaleçam os direitos e liberdades fundamentais do titular. A base é particularmente útil no contexto empresarial, pois permite certa flexibilidade e dispensa qualquer necessidade de consentimento, sendo compatível com operações confidenciais. No entanto, seu uso requer cautela e fundamentação rigorosa, especialmente em virtude de sua natureza subjetiva e potencial de conflito com os direitos dos titulares.

Para utilizar essa base legal de forma legítima e transparente, recomenda-se a realização de um LIA – *Legitimate Interest Assessment* (Avaliação de Interesse Legítimo), que consiste em um processo documental de avaliação no qual se demonstra: (i) a legitimidade do interesse perseguido; (ii) a necessidade do tratamento; e (iii) o equilíbrio entre esse interesse e os direitos fundamentais do titular¹⁸. O LIA atua como um mecanismo de *accountability* e pode servir de prova em caso de fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD) ou questionamento judicial, reforçando a conformidade da operação.

Por sua vez, nos termos do art. 11 da LGPD, o legítimo interesse não é admitido como base legal para o tratamento de dados pessoais sensíveis, categoria que inclui informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical, dados genéticos, biométricos, de saúde ou

¹⁶ MARANHÃO, Juliano de Souza Albuquerque; CAMPOS, Ricardo Resende. Proteção de dados de crédito na Lei Geral de Proteção de Dados. *Direito Público*, Porto Alegre, v. 16, n. 90, p. 132-154, nov./dez. 2019, pp. 149-154.

¹⁷ MARCO, Daniele Verza. Cláusulas de Confidencialidade e Proteção de Dados nas Negociações de Aquisição de Participação Societária. *Revista Semestral de Direito Empresarial*, n. 29, pp. 165-190, jul./dez. 2021, pp. 180-181.

¹⁸ OLIVEIRA, Ricardo; COTS, Márcio (coord.). O legítimo interesse e a LGPD: Lei Geral de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2020, pp. 98-106.

vida sexual. O tratamento desses dados exige fundamentos mais restritivos, como o consentimento específico e destacado, o cumprimento de obrigação legal ou regulatória, ou a proteção da vida e da incolumidade física do titular ou de terceiros. Assim, em operações de M&A que envolvam o acesso a dados de saúde ocupacional, ou dados sindicais de empregados, por exemplo, é vedado o uso do legítimo interesse como justificativa legal, exigindo-se maior cautela e fundamentação jurídica adequada para garantir a conformidade do tratamento.

Ainda que o legítimo interesse surja como uma alternativa viável e estratégica, é fundamental que seja adotada uma abordagem diligente, com documentação de respaldo e mecanismos de mitigação de riscos, a fim de garantir que o tratamento se mantenha proporcional, transparente e seguro.

Portanto, a escolha da base legal adequada dependerá das características específicas da operação, da natureza dos dados pessoais tratados e da relação entre o titular e os agentes envolvidos. Em síntese, as operações de M&A devem ser estruturadas de modo a respeitar a legalidade, a finalidade e a necessidade no tratamento de dados pessoais, evitando o uso indiscriminado de qualquer base legal. A definição correta da base jurídica, aliada à adoção de salvaguardas administrativas e técnicas, é indispensável para assegurar a conformidade com a LGPD e a estabilidade jurídica da operação.

Transferências internacionais de dados pessoais

A transferência internacional de dados pessoais é uma das temáticas mais sensíveis no contexto das operações de M&A, especialmente quando envolve investidores ou adquirentes sediados fora do Brasil. Vale notar que a simples alocação e acesso do *data room* em um servidor localizado no exterior já configura a transferência internacional de dados.¹⁹

A LGPD prevê em seu art. 33 que essas transferências apenas podem ocorrer para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na legislação brasileira. No entanto,

¹⁹ MARCO, Daniele Verza. Cláusulas de Confidencialidade e Proteção de Dados nas Negociações de Aquisição de Participação Societária. Revista Semestral de Direito Empresarial, n. 29, pp. 165-190, jul./dez. 2021, p. 181.

até o momento, o Brasil não é reconhecido como país adequado por nenhuma autoridade estrangeira — ou seja, não há “decisões de adequação” (*adequacy decisions*) em vigor em relação ao Brasil que permitam a livre circulação de dados para o exterior com base nessa presunção de equivalência legal²⁰.

De maneira recíproca, a ANPD também não emitiu até o momento nenhuma decisão de adequação reconhecendo países terceiros como detentores de grau de proteção compatível com a LGPD (art. 34 da LGPD). Isso significa que, na ausência de tais decisões, qualquer transferência internacional de dados pessoais precisa estar amparada por outros mecanismos legais previstos na legislação e regulamentados pela ANPD. A ausência de decisões de adequação, portanto, impõe um ônus adicional às partes envolvidas em M&A com componentes internacionais: é necessário recorrer a garantias contratuais e procedimentos específicos.

A Resolução CD/ANPD nº 19, de 23 de agosto de 2024, veio justamente regulamentar essas hipóteses. O normativo estabelece mecanismos autorizados para a transferência internacional de dados quando não houver decisão de adequação. Dentre os instrumentos previstos, destacam-se: cláusulas-padrão contratuais aprovadas pela ANPD, cláusulas contratuais específicas submetidas à avaliação da autarquia, normas corporativas globais (*Binding Corporate Rules* - BCR), instrumentos de cooperação jurídica internacional, ou, em último caso,

²⁰ O General Data Protection Regulation (GDPR), norma europeia de proteção de dados pessoais que inspirou a LGPD, estabelece três pilares na transferência internacional de dados, quais sejam: (i) adequação; (ii) salvaguardas adequadas; e (iii) derrogações. Nesse sentido: “At the heart of the European regulation on cross-border data transfers is the adequacy finding under Article 45 GDPR as the first tier, which certifies that a third country provides an ‘adequate level of protection’. Since Article 45 Sec. 1 sentence 2 GDPR emphasises that in the cases of a positive evaluation of the third country’s data protection framework a specific authorisation for a transfer of personal data is not needed, the adequacy finding which is taken by the Commission according to Article 45 Sec. 2 and 3 GDPR is indeed the best way to enable transfers of personal data under the EU’s data protection law. [...] The second tier of the EU’s system for cross-border flows of personal data concerns such cases where an adequacy decision is not in place. In this regard, Article 46 GDPR in conjunction with Article 47 GDPR provide for additional requirements that compensate for the lack of an adequate level of data protection in a third country thus rendering data flows permissible. Article 46 GDPR holds for the provision of “appropriate safeguards”, the two most common of which are Standard Contractual Clauses (SCCs) (Article 46 Sec. 2 (c) GDPR) and Binding Corporate Rules (BCRs) (Article 46 Sec.2 (b) GDPR). [...] Finally, the third tier of the EU system for cross-border data flows foresees derogations for data transfers where there is neither an adequacy decision nor appropriate safeguards in place. Article 49 Sec. 1 (a)–(g) GDPR lists requirements such as, for example, explicit consent to the proposed transfer, the necessity of the transfer for the performance of a contract or the implementation of pre-contractual measures as well as the necessity for important reasons of public interest that allow for an exemption of the ban on data transfers.” Cf. KALIN, Roman Pascal. *Digital Trade and Data Privacy: Cross Border Flows of Personal Data Between Data Protection and Data Protectionism*. Cham: Springer, 2023, pp. 185-187.

consentimento específico do titular. Tais mecanismos devem conter garantias suficientes de proteção, inclusive cláusulas relativas à responsabilização, medidas técnicas e acesso do titular aos seus direitos.

Na ocasião da edição do referido normativo, a ANPD disponibilizou o exato teor da sua cláusula-padrão contratual (*Standard Contractual Clause – SCC*), o que tem sido muito utilizado pelo mercado em operações de M&A para garantir conformidade.

Medidas técnicas e administrativas de segurança

A LGPD, em seu art. 6º, inciso VII, impõe a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão ilícita. A diretriz adquire relevância particular nas operações de M&A, uma vez que o compartilhamento de informações entre as partes é intenso, especialmente durante a fase de *due diligence*. A negligência na implementação de tais medidas pode não apenas comprometer a segurança das informações pessoais envolvidas, mas também gerar responsabilização do controlador e impactos reputacionais às partes.

Entre as medidas técnicas usualmente adotadas no mercado, destaca-se o uso de *data rooms* virtuais com autenticação multifator, criptografia de documentos sensíveis, registros de logs de acesso e sistemas de detecção de intrusão. Tais ferramentas garantem rastreabilidade, controle de acesso segmentado por perfis e proteção contra incidentes de segurança acidentais ou intencionais. É igualmente recomendável a aplicação de anonimização ou pseudonimização de dados pessoais sempre que possível, especialmente quando a identificação direta do titular não é essencial à análise pretendida. Assim, é possível reduzir a exposição dos dados e limitar o impacto de eventuais incidentes.

No plano das medidas administrativas, é essencial estabelecer políticas internas claras sobre o tratamento de dados pessoais durante a operação, incluindo termos de confidencialidade para os integrantes das equipes de negociação, cláusulas específicas nos contratos com assessores e consultores externos, e até mesmo treinamentos específicos para os profissionais envolvidos. A definição de um responsável interno pela gestão do projeto e governança

de dados na operação também é prática recomendada, assegurando o monitoramento da conformidade em todas as fases da operação.

Além de mitigar riscos jurídicos, a adoção dessas medidas demonstra o cumprimento do princípio da responsabilização e prestação de contas (*accountability*) previsto na LGPD. Em um cenário de crescente escrutínio regulatório e judicial, o compromisso proativo com a segurança da informação constitui não apenas um dever legal, mas também um diferencial competitivo. Ao proteger os dados pessoais envolvidos, as partes reforçam a legitimidade da operação de M&A e promovem um ambiente de confiança para todos os *stakeholders*.

DISCUSSÃO

O presente estudo revelou que operações de M&A envolvem, por sua própria natureza, uma intensa circulação de informações, que podem ser qualificadas pela legislação como dados pessoais, entre múltiplos agentes, internos e externos, o que impõe obrigações de conformidade com a LGPD. Desde os primeiros contatos negociais até a efetiva implementação da operação societária, diversos tratamentos de dados são realizados, como coleta, compartilhamento, transferência, acesso e armazenamento, todos enquadráveis no conceito amplo e exemplificativo previsto pela legislação brasileira. Tal realidade exige que os profissionais envolvidos não apenas reconheçam a incidência da LGPD, mas que também implementem uma governança de dados compatível com o risco regulatório e reputacional inerente a essas transações.

Verificou-se que a simples celebração de NDAs, Lols e MoUs não é suficiente para garantir a licitude do tratamento de dados pessoais em M&A. Embora sejam úteis para assegurar o sigilo comercial e alinhar as tratativas da negociação, esses instrumentos não substituem a necessidade de enquadramento do tratamento em uma base legal válida. A depender da natureza e da finalidade dos dados tratados, pode-se aplicar a base de execução de contrato, a proteção do crédito ou, com a devida cautela e documentação, o legítimo interesse. O consentimento, apesar de previsto na LGPD, mostra-se de difícil aplicação nesse contexto por questões de viabilidade operacional, riscos à confidencialidade e por ser juridicamente frágil diante de sua revogabilidade.

O legítimo interesse, por sua vez, mostrou-se como uma das alternativas mais plausíveis para o tratamento de dados pessoais em M&A, sobretudo pela compatibilidade com operações sigilosas e de caráter estratégico. No entanto, sua adoção demanda a realização de uma Avaliação de Interesse Legítimo (LIA), que funcione como prova de diligência e proporcionalidade na escolha dessa base legal. Além disso, a LGPD veda a utilização do legítimo interesse para dados sensíveis, o que obriga os agentes a maior rigor, com vistas à adoção de bases legais mais restritivas.

O estudo também demonstrou que operações com componentes internacionais enfrentam desafios adicionais. O Brasil ainda não é reconhecido como país com grau de proteção adequado para fins de transferência internacional, tampouco reconheceu formalmente outros países como adequados. Diante disso, os agentes econômicos devem se valer de mecanismos contratuais e institucionais previstos pela ANPD, como as cláusulas-padrão, que precisam ser cuidadosamente incorporadas à estrutura documental da operação. Ignorar tais exigências compromete a segurança jurídica da transação e expõe as partes a sanções e perda de legitimidade.

Além dos aspectos jurídicos, o trabalho enfatizou a importância de medidas técnicas e administrativas para a efetiva proteção dos dados pessoais ao longo da operação. A adoção de *data rooms* seguros, criptografia, controle de acessos, bem como políticas internas claras e treinamento das equipes envolvidas, são práticas recomendadas. A segurança da informação não é apenas uma exigência legal da LGPD, mas também um fator estratégico que agrega valor à operação e fortalece a confiança entre os agentes envolvidos.

Em síntese, a governança de dados em operações de M&A deve ser compreendida como um pilar essencial da condução negocial contemporânea. As exigências da LGPD impõem um novo padrão de diligência que integra o direito empresarial, societário, a proteção de dados e a segurança da informação. Atender a esse padrão não é apenas um requisito de conformidade, mas uma prática que confere maior previsibilidade, estabilidade e legitimidade à operação, promovendo um ambiente de negócios mais responsável e seguro para o tratamento de dados pessoais.

REFERÊNCIAS

BOTREL, Sérgio. **Fusões & aquisições**. São Paulo: Saraiva, 2012.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 19, de 23 de agosto de 2024**.

BULGARELLI, Waldírio. **Fusões, incorporações e cisões de sociedades**. 4. ed. São Paulo: Atlas, 1999.

CABRAL, Filipe Fonteles. **Proteção de dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados**. Rio de Janeiro: Lumen Juris, 2019.

EIZIRIK, Nelson. **M&A: regime societário e contratual**. São Paulo: Quartier Latin, 2024.

FERREIRA, Arnaldo Vieira. **Reorganizações societárias como meios de recuperação judicial**. São Paulo: Quartier Latin, 2024.

FORGIONI, Paula Andrea. **Os fundamentos do antitruste**. 7. ed. São Paulo: Editora Revista dos Tribunais, 2014.

KALIN, Roman Pascal. **Digital trade and data privacy: cross border flows of personal data between data protection and data protectionism**. Cham: Springer, 2023.

MARANHÃO, Juliano de Souza Albuquerque; CAMPOS, Ricardo Resende. **Proteção de dados de crédito na Lei Geral de Proteção de Dados**. Direito Público, Porto Alegre, v. 16, n. 90, p. 132-154, nov./dez. 2019.

MARCO, Daniele Verza. **Cláusulas de confidencialidade e proteção de dados nas negociações de aquisição de participação societária**. Revista Semestral de Direito Empresarial, n. 29, p. 165-190, jul./dez. 2021.

MUNIZ, Joaquim de Paiva. **Introdução às operações de compra e venda de participação societária: manual de M&A**. São Paulo: Quartier Latin, 2024.

NASCIMENTO, João Pedro Barroso do. **Medidas defensivas à tomada de controle de companhias**. São Paulo: Quartier Latin, 2011.

OLIVEIRA, Ricardo; COTS, Márcio (coord.). **O legítimo interesse e a LGPD: Lei Geral de Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2020.

SADDI, Jairo (org.). **Fusões e aquisições: aspectos jurídicos e econômicos**. São Paulo: IOB, 2002.

VAINZOF, Rony. Art. 5º. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters, 2020.

DIREITO À COMUNICAÇÃO E LACUNA DIGITAL NO NORTE DA ARGENTINA: O ACESSO À INTERNET COMO GARANTIA DE USUFRUTO DO ESPAÇO PÚBLICO

Franco-David Hessling-Ferreiro

Universidade Nacional de Salta Argentina(UNSa-INENCO-CONICET)

Andrea Paola Yanguas Xavier

Universidade Salesiana Santa Teresa de Corumbá

RESUMO

O objetivo principal deste ensaio é analisar os vínculos entre o conceito de direito e a comunicação e outras noções, antigas e novas, que fazem parte do campo de reflexão sobre cidade, espaço público e direitos -atribuições e deveres- na era digital, e em relação aos problemas de acesso e prazer da tecnologia. Para isso, propõe-se uma triangulação entre o direito à comunicação, a lacuna digital e o espaço público no marco de uma região específica, o norte argentino. Este lugar reúne características singulares como diversidade cultural interétnica, profunda desigualdade econômica e população rural misturada com população urbana. Assim, esta reflexão permite concluir a necessidade de assumir o direito à comunicação e à lacuna digital a partir de uma perspectiva localizada, uma mirada integral e um problema complexo e interativo que deve ser abordado em vermelho, resumindo vários atores. Com esta abordagem, essas discussões ocorrerão mais nos âmbitos jurídicos e acadêmicos.

Palavras-chave: digital ; cidadania ; alfabetização ; tecnologia; direitos humanos.

INTRODUÇÃO

Na sociedade contemporânea o direito à comunicação é um tema central para os debates. Este artigo propõe uma análise sobre o alcance do direito à comunicação em um país situado no capitalismo semiperiférico, onde existe um profundo fosso digital, oposto ao que ocorre nos países do Norte Global (Castells, 2001; Ávila, 2023). Para a sua conjuntura, então, tomamos aqui uma ideia sobre o espaço público num sentido mais amplo do que o convencional. Em outras palavras, não há nenhuma suposição de que o espaço público possa ser considerado apenas em oposição ao espaço privado.

Nesta abordagem, o espaço público é composto também pelo cenário digital, principalmente após o surgimento do uso generalizado da web, da internet e das mídias sociais. Este último processo ocorreu no Norte da Argentina ao longo do século 21, visto que a tecnologia da inovação traz tarde para o quintal do quintal: esta região é a mais pobre da Argentina (INDEC, 2024).

O espaço público vem das ferramentas jurídicas do quadro dos direitos humanos. Por exemplo, num acordo inicial em 2013, a Relatoria Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos (RELE para as suas iniciais em espanhol) propôs:

Maximizar o número e a diversidade de vozes que podem participar no debate público é ao mesmo tempo um meio e um fim para o processo democrático. Nesse sentido, garantias robustas do exercício da liberdade de expressão através da Internet são atualmente condição para a abertura da esfera pública (RELE, 2013, p. 14).

O acesso a tecnologias inteligentes de qualidade e à rede Wi-Fi deveria ser garantido como um direito básico, sobretudo em contextos urbanos marcados por exclusões históricas. No entanto, o que se observa, especialmente nas periferias, é a persistência de barreiras estruturais, como a falta de recursos financeiros, que inviabilizam esse acesso. A desigualdade social, nesse sentido, não apenas limita a conectividade digital, como reforça a exclusão de populações inteiras de um serviço que deveria ser público, gratuito e universal.

Principais motivos que geram essas desigualdades para os consumidores domésticos são os preços dos produtos elevados nas tecnologias inteligentes trazendo custos caros para maiorias dos argentinos. O salário mínimo

do ano de 2024 permanece sem aumento e o valor da tarefa de Wi-Fi sem fio e da tecnologia inteligente por possuir alto custo representaria uma grande parcela da renda familiar. Nas áreas rurais. As áreas rurais a infraestrutura de comunicação não é suficiente regiões afastadas não possui redes de internet seguras e de qualidade.

No Norte da Argentina possui variados grupos étnicos ampla diversidade cultural, que são admitidos pelos governos e provinciais da região, o que propõe questionamentos sobre o livre acesso à internet e aos bens tecnológicos. A interculturalidade acrescenta outro problema como o grau de alfabetização tecnológica da população. A menor disponibilidade de tecnologia inteligente e os caminhos da diversidade cultural, que vão da linguagem aos hábitos alimentares, conferem ao local vários graus com interfaces e formas tecnológicas para o digital.

Dado este complexo contexto de análise, com vários impulsionadores e múltiplas situações, uma perspectiva local confronta-nos com limites concretos para garantir o direito à comunicação. No Norte da Argentina, a desigualdade torna o “gap digital” mais profundo do que em lugares do Global Norte (Sousa Santos, 2009; Milão e Treré, 2019). A forma desta etapa obriga a um conhecimento situado em cada contexto, embora sempre procurando o diálogo de saberes. Ao acompanhar esta busca, contribuições situadas ajudam a remodelar e repensar os estudos no campo das ciências da comunicação sobre os alcances do direito à comunicação. Sem acesso total à “esfera digital” não há direito real na sua interpretação mais ampla.

O artigo possui o objetivo de analisar as desigualdades culturais, socioeconômicas, territoriais existentes ao direito a comunicação no norte da Argentina, realizando indagações sobre a falta de acesso equitativo à internet como algo que compromete a plena participação da população de Salta, Jujuy, Tucumán e Catamarca.

Este artigo está dividido em sete seções. A primeira é a introdução, a segunda parte apresenta o referencial teórico, abordando os antecedentes sobre a lacuna digital no norte da Argentina. A terceira seção analisa sobre o conceito de Direitos Digitais. Em seguida, a quarta seção discute o conceito de Lacuna digital, muito mais do que acesso à tecnologia. A quinta seção os aspectos metodológicos. A sexta seção propõe um debate dos resultados e

discussões da pesquisa, e por fim, a sétima seção apresenta as considerações finais, com recomendações para políticas públicas e a formulação de uma perspectiva de justiça digital.

REFERENCIAL TEÓRICO

Antecedentes sobre a lacuna digital no norte da Argentina

De acordo com trabalhos acadêmicos que adotaram uma metodologia qualitativa e quantitativa para estudos de caso no Norte da Argentina (Chachagua, 2019; Ares e Venier, 2023), deve-se afirmar que a lacuna digital é uma evidência irrefutável. Isto permitiu um ponto de vista que defende que a lacuna digital nesta região é mais profunda do que qualquer outra parte do Norte Global (PNUD, 2022). O acesso ao serviço wifi, como produtos de tecnologia inteligente, é muito difícil porque é caro. Nos casos mais terríveis, principalmente em contextos rurais com comunidades étnicas, a falta de infraestruturas leva a uma marginalização total (Hessling Herrera e Belmont Colombres, 2022).

Alguns programas públicos têm oferecido materiais e tecnologia para alívio desta situação de desigualdade. No passado, a gestão de Cristina Kirchner enrolou o programa “Conectar Igualdad” e entregou netbooks para alunos e professores de todo o país (Chachagua, 2019). Essa tarefa serviu também para impulsionar a indústria nacional, que contava com instalações para montagem de PCs no sul do país. O potencial de igualdade nunca mais foi o mesmo depois da saída de Kirchner da Pink House. Recentemente, a administração de Javier Milei encerrou o programa.

Independentemente do golpe inicial na lacuna digital que o Conectar Igualdad significou, numa perspectiva de longo prazo, o impacto real foi menor do que o esperado no início da entrega de netbooks. O principal crítico da implementação é a falta de uma visão integral sobre a lacuna digital e as formas de desfrutar da esfera digital. Tomando o contexto intercultural descrito anteriormente, a falta desse ponto de vista não ajudou a diminuir a lacuna. A desigualdade não é resolvida apenas por causa de muitos computadores novos nas mãos dos pobres.

Uma perspectiva integral que acrescente uma visão intercultural necessita de maior comprometimento com o desenvolvimento de competências para

utilização desses bens tecnológicos inteligentes (Tello, 2023). Grande parte do cumprimento da meta de redução da lacuna digital está vinculada ao trabalho de construção de novas competências de alfabetização tecnológica (Albarelo, 2019), ainda mais em etapas rurais e interculturais como o Norte da Argentina. Para isso, não só estudantes e acadêmicos precisam de mais capacitação, mas também professores e pesquisadores. Sem formação em competências ligadas à alfabetização tecnológica, a sua verdade impossível reduzirá a desigualdade no direito à comunicação.

A maioria dos professores e pesquisadores dos municípios de Salta, Jujuy, Tucumán e Catamarca ainda hoje devem aprender muito sobre produtos de tecnologia inteligente. Devido ao baixo orçamento contemporâneo para infraestrutura comunicacional e à pequena inversão nos programas de transferência de tecnologia, a questão da alfabetização tecnológica permanece em segunda ordem, longe de ser anterior.

O conceito de Direitos Digitais

“Direitos digitais” é uma nova noção para abordar questões sobre o acesso às tecnologias de comunicação e a aprendizagem de competências para a utilização destes dispositivos. Num contexto como o descrito anteriormente no Norte da Argentina, estes direitos parecem uma tentativa para vários assuntos: acesso à tecnologia, enfoques de políticas públicas, intervenções do terceiro setor e alfabetização digital. Em seu lugar, este artigo optou por pensar que não precisamos despendar esforços para moldar uma noção única que agregasse todos os conceitos sobre a famosa lacuna digital. No final das contas, as necessidades reais estão ligadas à oferta de soluções para as comunidades locais, algumas com particularidades interculturais, sem prestar atenção se existem um ou diversos conceitos acadêmicos. Estas necessidades reais de um problema de lacuna digital devem, então, ser mais importantes do que a procura de noções únicas como “direitos digitais”, ou outras como “direito à comunicação” ou “direito à informação” ou “vida digna”.

A discussão sobre os direitos digitais exige a construção de um diálogo constante entre a academia, as ciências sociais e as próprias comunidades envolvidas, considerando suas trajetórias locais e experiências individuais. Para

tanto, este estudo qualitativo propõe a realização de entrevistas com membros da comunidade e atores locais, bem como a produção de notas etnográficas de campo e a análise de fontes documentais. Esses instrumentos permitirão revisar criticamente a agenda pública dos municípios da região da Puna argentina, a partir de uma perspectiva situada e sensível às realidades do território.

Esta reflexão aponta um campo jurídico muito específico, o nível de impacto que os “direitos digitais” têm nos instrumentos jurídicos, e existe escassez de material com citações exatas sobre esses direitos. Em parte, porque a noção de “direitos digitais” é recente, e porque estes instrumentos com ideias liberais sobre a desigualdade social, cultural, económica e de gênero. No geral, os direitos digitais estão apenas nos trabalhos de investigadores e académicos, mas não nos quadros legais, regulamentares, nem à escala nacional, provincial ou local.

Dessa forma, existe uma lacuna nos “direitos digitais”, tanto nos instrumentos jurídicos quanto nos materiais jurídicos. Além disso, também não existe uma posição sobre o alcance destes direitos que permita a sua assunção como abrangendo pessoas de baixos rendimentos e sectores marginais da sociedade. Os direitos digitais não devem apenas estar vinculados às questões digitais da lacuna, mas também à apropriação cultural com artefactos tecnológicos, à gestão da Internet e ao todo telemático da linguagem. Há até quem fale dos direitos digitais como parte dos direitos humanos (OCDE, 2022), e até foram chamados de “direitos humanos de quarta geração”:

Na literatura jurídica actual, muitas vozes já apelam à emergência de uma nova gama de direitos relacionados com a sociedade da informação que constituiria uma quarta geração de direitos humanos. São propostos aqui dois tipos de direitos: (i) vários direitos que já alcançaram reconhecimento em muitos países, como a liberdade de expressão, o direito à proteção de dados sensíveis, a privacidade e o sigilo das comunicações, entre outros; e (ii) outros novos direitos que estão apenas a surgir, como os direitos do cibernauta no mundo digital (Martínez Villalba, 2014, pp. 16).

Embora este conceito tenha a vantagem por ser uma tentativa recente de descrever a nova realidade para o acesso da Internet e das tecnologias inteligentes, tem uma limitação de aspectos desconhecidos sobre competências digitais, liderança cultural e alfabetização na esfera das TICS. Desta forma, é

necessário repensar o alcance dos “direitos digitais” antes de conseguir colocá-los no debate mais importante neste campo.

Os direitos não representam apenas atribuições dos sujeitos, mas também significam deveres destes para com toda a sociedade. Com efeito, saiba que isso deve ser sinalizado porque na maioria das vezes o que se fala em “direitos” apenas se manifesta em aspectos positivos e subjetivos, sem considerar amplamente a concepção e o alcance que eles possuem. Por exemplo, por apenas dizer algo, o direito à comunicação incita a atribuição nas pessoas de informações verdadeiras e ampla participação na esfera pública, mas, além disso, suas responsabilidades de origem correta no uso de palavras públicas (Loreti e Lozano, 2014; Hessling Herrera, 2023). Outros exemplos são o direito à educação ou o direito à saúde, que não só protegem as pessoas e as comunidades, mas também são deveres das famílias e das administrações governamentais. Dado que estes são considerados como direitos humanos, a sua “aplicabilidade” recai como obrigação dos Estados e das pessoas adultas (Abramovich e Courtis, 2004; Hessling Herrera, 2024).

Para que os direitos digitais surjam nos debates jurídicos, sociais, culturais, para além de algumas discussões académicas, é necessário compreender a alfabetização digital, as diferenças económicas no acesso à tecnologia inteligente e às tecnologias da informação e comunicação (TICs). Em outras palavras, é importante que tenham debates científicos que conceituem os direitos digitais de forma isolada.

Quanto a este último, este artigo propõe mesclar todos os direitos que referenciam o âmbito da comunicação dentro de uma noção única, já conhecida como “direito à comunicação”. Dentro desta definição inclui-se a liberdade de expressão, o direito à informação, a liberdade de imprensa e os direitos digitais (Hessling Herrera, 2023). Assim, evitar a estagnação em preocupações académicas que se confundem em outros contextos do cotidiano ajuda a trazer essas discussões e insights para cenários diversos, aumentando a influência dessas lutas pela ampliação desses direitos.

Lacuna digital, muito mais do que acesso à tecnologia

A lacuna legal mencionada na parte acima faz com que os “direitos digitais” ou “direito à comunicação” não possam ser entendidos como uma mera questão de acesso. Por outras palavras, a lacuna digital é central nestas discussões, embora não devamos pensar que o problema é apenas económico, ou de posse de dispositivos inteligentes ou máquinas informáticas (Baladrón *et al.*, 2019). A lacuna digital, como já foi dito, em lugares como a América Latina depende de vários fatores como diversidade cultural, habilidades de comunicação, alfabetização digital e qualidade da conexão wi-fi, entre outros. É verdade que estes factores também estão ligados a aspectos económicos, mas não se pode esperar que tudo seja a mesma coisa. Cada fator deve ser mencionado e analisado com características próprias, sem deixar de ver a integração completa desses elementos.

Em locais específicos do norte da Argentina, como o Grande Chaco - em lugares como as províncias de Salta, Jujuy, Formosa e Chaco - são difíceis os cenários mais pobres que lidam se pensarmos apenas na transferência de dispositivos. Acompanhar novos números sobre esta região (PNUD, 2022), e estudos qualitativos (Flores Klarik 2015; 2019), permitem perceber que a região sofre graves desigualdades, não só pelas receitas mais baixas, mas também pelas lacunas culturais e pela falta de instituições básicas, como atenção sanitária primária, centros desportivos ou representantes governamentais *Officine*.

Para citar apenas um caso, na cidade de Hickmann, na rota nacional 81, entre Salta e Formosa, um único escritório recebe e resolve questões relacionadas com a administração municipal, serviços públicos de energia e água e qualquer outro tipo de processos (Belmont Colombres, 2022). Mesmo assim, o pagamento das contas só acontece no mesmo local, na cidade de Hickmaan, que abre um dia por semana. Neste local você deve visitar todos os municípios da zona.

Neste contexto, o acesso à tecnologia inteligente ocorreu principalmente através do programa Conectar Igualdad, mas é um alcance estreito quando outras necessidades atingem os domicílios e as famílias, tanto criollas quanto nativas (Balardón *et al.* -coord., 2023). Além disso, decisões posteriores do governo nacional libertário, desde dezembro de 2023, têm como objetivo enquadrar esses programas e outras linhas políticas que focavam a população rural

e as comunidades indígenas, os pequenos agricultores e as pessoas de baixa renda. A consequência destas decisões administrativas é que estes dispositivos que trazem às pessoas tecnologia não atualizada e não recebida se mantêm, porque não há trabalhadores para a vontade que o fazem, e nem orçamento para a vontade de pagar. O slogan central da administração de Javier Milei é “não há dinheiro”.

ASPECTOS METODOLÓGICOS

A elaboração deste artigo baseia-se em uma abordagem qualitativa, de caráter exploratório e crítico-interpretativo, sustentada por uma leitura interdisciplinar do fenômeno comunicacional no contexto da exclusão digital. A pesquisa orienta-se por uma perspectiva hermenêutica crítica, na qual o objetivo não é apenas descrever empiricamente a realidade estudada, mas compreendê-la à luz de marcos teóricos que articulem categorias provenientes dos campos dos direitos humanos, estudos da comunicação, teoria social crítica e análise socioespacial. Essa orientação metodológica permite compreender o direito à comunicação não como um conceito normativo isolado, mas como uma construção histórico-política situada e em constante disputa.

O referencial teórico foi organizado a partir de dois eixos principais. O primeiro eixo trata da conceituação ampliada do direito à comunicação, incorporando contribuições da teoria crítica dos direitos humanos (Abramovich & Courtis, 2004; Herrera Flores, 2008) e dos estudos sobre cidadania digital (RELE, 2013; Castells, 2001; Loreti & Lozano, 2014), com ênfase na noção de interdependência entre direitos e sua inseparabilidade em contextos marcados por desigualdade estrutural. O segundo eixo do referencial focaliza a categoria de lacuna digital, compreendida segundo uma abordagem multidimensional, que vai além da ausência de infraestrutura, articulando desigualdades econômicas, culturais, territoriais e institucionais (Baladrón *et al.*, 2019; Tello, 2023; Ávila, 2023).

Do ponto de vista material, a curadoria bibliográfica priorizou autores e estudos que dialogam com contextos latino-americanos e, especialmente, com a realidade argentina — um recorte territorial pensado para aprofundar a compreensão dos impactos da exclusão digital em regiões periféricas. Foram incluídas fontes acadêmicas, relatórios institucionais (como o INDEC e a RELE),

documentos técnicos, obras teóricas e estudos de caso elaborados nos últimos dez anos, com especial atenção à produção crítica sobre comunicação, tecnologias e direitos.

Além disso, a construção conceitual foi articulada com pesquisas empíricas regionais, sobretudo estudos de campo, relatórios comunitários e análises etnográficas realizadas em províncias do norte argentino, como Salta, Jujuy, Tucumán e Catamarca. Embora este artigo não apresente dados primários coletados no âmbito de trabalho de campo próprio, ele se apoia em um reexame crítico de evidências empíricas previamente produzidas por autores da região que atuam junto a comunidades indígenas, rurbanas e periféricas. Essa opção metodológica visa produzir conhecimento teoricamente fundamentado e territorialmente enraizado.

Portanto, o método adotado neste trabalho compreende a construção do objeto a partir da interlocução entre teoria crítica e análise contextualizada, buscando responder à seguinte pergunta de pesquisa: de que modo a falta de acesso equitativo às TICs compromete o exercício pleno do direito à comunicação e, por consequência, da cidadania, em espaços periféricos como o norte da Argentina? A resposta a essa questão orienta a articulação dos achados bibliográficos com uma visão transformadora das políticas públicas de inclusão digital, evidenciando a urgência de uma abordagem interseccional, dialógica e situada.

RESULTADOS E DISCUSSÃO

Direito à comunicação como conceito completo

Ao colocar noções mencionadas como “direitos digitais”, “liberdade de expressão”, “liberdade de imprensa” ou “direito à informação”, escolhemos essa proposta como um conceito que integra todos eles (Hessling Herrera, 2020; Hessling Herrera 2021). No entanto, tomamos um conceito que não é completamente novo e original. Tomando como base trabalhos anteriores de outros autores, nossa proposta está reivindicando o “direito à comunicação” e serve tanto para misturar todos os conceitos que se referem à comunicação e ao espaço público quanto para penetrar esferas além dos âmbitos jurídico e acadêmico. Nossa visão desse conceito, portanto, abrange uma abordagem

ampla. Essa abordagem torna possível adicionar ao “direito à comunicação” tudo o que foi trabalhado neste documento. Pois, é necessário levar em conta que o vínculo entre comunicação e espaço público hoje é cruzado pela irrupção da internet. Isso implica que o acesso e a utilidade completa da web são condições básicas para o direito à comunicação em toda a concepção, como qualquer outro direito como o acesso à casa, à vida ou à água. O direito à comunicação é um direito fundamental como qualquer outro. Dessa forma, a região pontual que é tomada para análise neste artigo deve parecer uma zona com muitas privações e, portanto, um lugar onde as pessoas não desfrutam inteiramente do direito à comunicação. Isso ocorre porque todos os direitos fundamentais estão vinculados a um e, do contrário, em um relacionamento de codependência, por exemplo, sem acesso à energia ou à água, é impossível desfrutar do direito à comunicação.

No norte da Argentina, a questão principal não é o acesso à tecnologia ou habilidades de comunicação, nem infraestrutura sem fio nem manutenção de dispositivos. Embora seja verdade que essas questões são reais e preocupantes. O aspecto mais importante é a situação cultural e econômica geral na zona, não um fator específico ou cada um separadamente, mas todos os problemas como um todo. Este cenário complexo é incomum em outros países, mesmo dentro da própria Argentina. Historicamente, esta região é a mais pobre do país (INDEC, 2024) e onde a maioria dos conflitos deu origem à resistência indígena e à luta entre grandes e pequenos agricultores, principalmente na produção de açúcar (Iñigo Carrera, 2010). Aqui, a maioria dos litígios nos últimos anos tem sido sobre propriedade de terras e desmatamento de florestas nativas. A falta de recursos para garantir toda a vida do espaço público, incluindo as dimensões analógica e digital, está presente em todos os tipos de aspectos: político, econômico, legal, cultural, social e muito mais. Por esta razão, aqui se supõe que o direito à comunicação deve estar dentro da rede de reivindicações por uma vida digna e igualitária e acessível. Em outras palavras, o direito à comunicação é parte dos direitos humanos na concepção mais venerável. Mas, além disso, é um direito que só faz sentido dentro de uma cadeia de direitos. É o que chamamos de codependência entre direitos.

Para concluir este artigo de reflexão, serão destacados três pontos-chave em relação ao anterior. Primeiro, a necessidade de pensar de forma integral

e complexa o direito à comunicação como atribuição e deveres, públicos e privados, e em rede com outros direitos humanos. Este aspecto é fundamental para ultrapassar as esferas jurídicas e acadêmicas, bem como para transformar estes direitos em fortalecimento estratégico de litígios complexos (Rodríguez Garavito, 2022), cuja “exequibilidade” será possível e rotineira, portanto, “progressividade” (Stinco, 2019). Esta visão sobre o direito à comunicação não é nova e completamente original, mas é inevitável manter e repensar seu conteúdo com aspectos atuais como o acesso à Internet, a utilidade das tecnologias inteligentes, a alfabetização do processo digital e as políticas públicas sobre o espaço público, a esfera digital e a cidadania nestes lugares.

Essa forma de pensar a codependência entre vários direitos humanos, como uma rede, oferece possibilidades de participação intersetorial nos processos de luta onde se busca o reconhecimento de atores ou problemas invisíveis ou a melhoria das condições de vida. Por isso, é importante olhar os direitos humanos a partir de uma perspectiva crítica, cuja principal referência é Joaquín Herrera Flores (2008). Nessa linha teórica, os direitos humanos não são apenas textos escritos ou elementos legais, mas processos de luta para ampliar o alcance da ideia de uma vida digna. Abrir esse caminho poderia levar esses processos de luta a vincular atores que fazem parte de campos de ação diversos, como os âmbitos político, cultural, acadêmico, econômico e ainda esportivo. Com essa participação intersetorial, objetivos mais ambiciosos vinculados aos direitos humanos como um todo seriam alcançados e, além disso, uma agenda mais ampla de questões associadas à igualdade, inclusão e cidadania democrática seria discutida.

Em segundo lugar, todas as questões abordadas neste artigo devem ser entendidas de forma localizada, dentro de cada contexto específico. A visão local nos permite considerar as particularidades de cada lugar no momento de cada projeto de pesquisa. No caso do norte da Argentina, tanto o direito à comunicação quanto a lacuna digital têm a ver com pobreza, diversidade cultural e profunda desigualdade econômica, entre outras coisas (Casadei, 2024). Então, essas características não poderiam ser evitadas se pretendêssemos uma análise completa e integral. Assim, para uma perspectiva complexa sugerida no parágrafo inicial, é necessário levar em conta um olhar situado, que ainda é mais necessário no contexto do Norte da Argentina pelas características

dadas antes sinalizadas. Reduzir a lacuna digital e garantir o direito à comunicação, em uma visão localizada, faz sentido no Sul Global como caminhos de luta para construir sociedades mais justas, não apenas em escala mundial, mas também dentro de cada país. Daí a relevância de programas e políticas como o Conectar Igualdade, mas também a promoção de outras políticas que abordem de forma abrangente os problemas das populações mistas em áreas como o norte da Argentina.

Ambas as perspectivas, do Sul Global como um todo geopolítico e a visão local para cada lugar, devem ser consideradas para uma análise complexa e para abordar propostas sobre o direito à comunicação e o combate à exclusão digital em lugares do mundo periférico. Dessa forma, políticas públicas poderiam ser planejadas entre diferentes lugares, mesmo em locais que atendem países, por exemplo, na América Latina. Muitas vezes, áreas de fronteira têm mais em comum do que outras áreas dentro de seus próprios países. Além disso, essas articulações entre diferentes lugares em diferentes países facilitariam o financiamento internacional de entidades como o Banco Interamericano de Desenvolvimento, o Banco Mundial ou a CAF, entre outros. Com a adição desses tipos de atores financeiros, o potencial para alianças internacionais crescerá significativamente.

Em terceiro e último lugar, seu destaque de assunto é que o espaço público seja composto por esferas analógicas e digitais, portanto, lidar com a lacuna digital como questão principal é fundamental para a cidadania democrática e a participação completa na vida pública, decisões políticas, processos culturais e caminhos de ensino-aprendizagem. Isso ocorre porque a perspectiva localizada sugerida acima requer a articulação inevitável entre os vários fatores que interagem em regiões como o norte da Argentina (Belli -ed.-, 2017). Outros lugares com características semelhantes também devem ser tratados da mesma forma, com a consideração de que a lacuna digital faz parte de um cenário complexo com fatores múltiplos e interativos. A lacuna digital, então, não é apenas problemas econômicos, questões culturais ou preocupação social. Esta definição não deve perder de vista em nenhum momento, principalmente em locais como o norte da Argentina, onde há uma profunda desigualdade e uma diversidade cultural muito ampla. Não há o suficiente com focos políticos nem com transferências de renda ou dispositivos tecnológicos, também intervenções

integrais que envolvam múltiplos atores sociais, além dos governos (Rodríguez Garavito e Baquero Díaz, 2020).

A cidadania é importante para assumir que o espaço que é público, que é composto por esferas analógicas e digitais. As concepções cidadãs, precisam de uma visibilidade local, com percepções mais abrangentes e com codependência do direito a comunicação e para superar a exclusão digital, podendo levar em consideração da complexidade e multifatores que fazem parte dos espaços públicos e dos direitos humanos.

CONSIDERAÇÕES FINAIS

As transformações impostas pela era digital reconfiguram os modos de ser, constituir, exercer e reivindicar cidadania no mundo contemporâneo. Nesse novo cenário, o direito à comunicação se consolida como elemento estruturante e transversal, cuja presença ou ausência determina o nível de acesso a uma série de outros direitos fundamentais — como a educação, a saúde, a livre expressão, o trabalho e até a participação política. Não se trata, portanto, de uma dimensão acessória, mas sim do reconhecimento da comunicação como elo vital entre os sujeitos e os espaços públicos, físicos ou digitais, especialmente em contextos de vulnerabilidade social.

O norte da Argentina, foco empírico e analítico deste estudo, evidencia com contundência os efeitos da persistência da lacuna digital, cujas causas não se limitam à carência de infraestrutura técnica. A exclusão digital na região tem raízes profundas, cruzadas por fatores étnicos, territoriais, econômicos e institucionais, e manifesta-se como um fenômeno multidimensional que compromete profundamente o exercício da cidadania. A análise aqui desenvolvida demonstra que a presença de conexão à internet ou o fornecimento de dispositivos são medidas necessárias, mas insuficientes se não acompanhadas por políticas públicas intersetoriais, sustentáveis, culturalmente sensíveis e enraizadas nas realidades locais.

Por outro lado, os direitos digitais, embora largamente discutidos em fóruns acadêmicos e multilaterais, carecem de reconhecimento jurídico formal e de mecanismos efetivos de garantia em muitos países latino-americanos, sendo a Argentina um caso exemplar dessa defasagem. A ausência dessas

garantias institucionais propõe vastas camadas da população à invisibilidade digital, negando-lhes o usufruto pleno do espaço público em sua nova configuração tecnológica.

Portanto, para que do direito à comunicação seja efetivo, exige mais do que o tradicional enfoque em liberdade de expressão e acesso à informação. Requer a compreensão como um direito fundamental interdependente, transversal e relacional, em que para concretizar depende também do direito à moradia digna, à energia, à educação, à cultura, e à conectividade de qualidade. Nesse sentido, a luta pela justiça comunicacional não pode ocorrer de forma fragmentada ou isolada, mas deve estar em articulação às lutas territoriais por justiça social, inclusão e reconhecimento.

A partir da análise teórico-empírica realizada, apontamos três direções centrais para pensar soluções emancipadoras no enfrentamento da exclusão digital e para a construção de um espaço público verdadeiramente democrático na era da informação:

Em primeiro lugar a perceber a integralidade e interdependência dos direitos é criada a partir da necessidade de compreender a comunicação digital, como parte dos direitos humanos que são interconectados. Essa abordagem sobre políticas integradas entre os setores da educação, cultura, tecnologia, assistência social e infraestrutura, articulando esforços dos Estados e das comunidades.

Em segundo lugar criar a análise situada e escuta ativa dos territórios, a partir da complexidade dos contextos das periferias, como o norte argentino, exige mais que políticas genéricas. É necessário dar atenção aos saberes locais, respeitar a diversidade da cultura e da língua, e atentar para os processos de decisões participativas para que as próprias comunidades se reconheçam como coprodutoras de soluções tecnológicas e políticas públicas.

Em terceiro é importante o reconhecimento do espaço público digital como território de cidadania, em que o acesso à internet, a existência de competências digitais e o direito de expressão online, precisam ser reconhecidos como direitos políticos inalienáveis. Em que a marginalização digital representa uma nova forma de exclusão contemporânea, que deve ser enfrentada com a mesma seriedade das lutas históricas por inclusão educacional e territorial.

Para finalizar defendemos que o direito à comunicação deve ser o eixo normativo e político central para todas as tentativas de garantir a cidadania na

era digital, especialmente em regiões marcadas por privação histórica e desigualdades persistentes. Para superar a exclusão da comunicação é necessário permitir que sujeitos historicamente silenciados, passem a exercer plenamente o direito de protagonizar, interagir e disputar no espaço público, seja ele físico e digital. E isso será possível por meio de um compromisso ético e político com os princípios da equidade, escuta intercultural e da justiça social conectada.

REFERÊNCIAS

ABRAMOVICH, V.; COURTIS, C. **Los derechos sociales como derechos exigibles**. Buenos Aires: Editorial Trotta, 2004.

ALBARELLO, F. **Lectura transmedia. Leer, escribir, conversar en el ecosistema de pantallas**. Buenos Aires: Ediciones Ampersand, 2019.

ARES, M.; VENIER, E. Acceso a internet en comunidades indígenas del norte de Salta, Argentina. **Revista Argentina de Comunicaciones**, v. 11, n. 4, p. 181-211, 2023. Recuperado el 18 nov. 2023 de: <https://fadeccos.ar/revista/index.php/rac/issue/view/5/6>.

ÁVILA, R. La lacuna digital en América Latina como barrera para el ejercicio pleno de derechos. *In*: **Derechos digitales en Iberoamérica: situación y perspectivas**. Madrid: Fundación Carolina, 2023. p. 147-159.

BALADRÓN, M.; DE CHARRAS, D.; RIVERO, E.; ROSSI, D. Argentina. Derecho a la conectividad, desigualdad y actores no lucrativos. *In*: MONJE, D. (coord.). **(Des)iguales y (des)conectados: políticas, actores y dilemas info-comunicacionales en América Latina**. Ciudad Autónoma de Buenos Aires: CLACSO, 2021. p. 31-58.

BALADRÓN, M.; KEJVAL, L.; ROSSI, D. (coord.). **Conectividad popular: organizaciones sociales prestadoras de internet en barrios populares y áreas rurales de Argentina**. Buenos Aires: Editorial Mil Campanas, 2023.

BELLI, L. (ed.). **Community networks: the Internet by the people, for the people**. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2017.

BELMONT COLOMBRES, M. E. Reactualizando la ontología política del territorio de la comunidad San Ignacio de Loyola: el caso del cacicazgo de Dino Salas. **Cuadernos de Antropología**, v. 28, p. 38-62, 2022. Recuperado de: <https://plarci.org/index.php/cuadernos-de-antropologia/article/view/1314>.

CASADEI, T. Brechas digitales: el reto de las nuevas tecnologías para los derechos humanos. **Revista de la Facultad de Derecho de México**, v. 74, n. 290, p. 149-178, 2024. DOI: 10.22201/fder.24488933e.2024.290.90069.

CASTELLS, M. **La galaxia internet: reflexiones sobre internet, empresa y sociedad**. Barcelona: Editorial Areté, 2001.

CHACHAGUA, M. R. **Políticas de diseminación tecnológica, escuelas y jóvenes: sentidos de las TICs en el campo y la ciudad (Salta 2015-2017)**. 2019. Tese (Doutorado) – Universidad Nacional de La Plata. Disponível em: http://sedici.unlp.edu.ar/bitstream/handle/10915/73552/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y. Acesso em: out. 2020.

FLORES KLARIK, M. El ingreso a la ciudadanía de los Pueblos Indígenas del área de Tartagal. In: ÁLVAREZ LEGUIZAMÓN, S. (ed.). **Neocolonialismo, capitalismo, pobreza y resistencias subalternas**. Rosario de Santa Fe: ICSO, 2015. p. 105-154.

FLORES KLARIK, M. Agronegocios, pueblos indígenas y procesos migratorios rururbanos en la provincia de Salta, Argentina. **Revista Colombiana de Antropología**, v. 55, n. 2, p. 65-92, 2019. DOI: 10.22380/2539472X.799.

HESSLING HERRERA, F. D. Libertad de expresión y periodismo en la doctrina de la Corte Interamericana de Derechos Humanos. **Revista Cálamo**, Quito, p. 19-34, 2020.

HESSLING HERRERA, F. D. Genealogía de la libertad de expresión en el sistema interamericano de derechos humanos. De los orígenes a los debates actuales. **Revista de Derechos Humanos y Estudios Sociales**, p. 175-196, 2021.

HESSLING HERRERA, F. D. Clausura de conciencia: libertad de expresión y periodismo en los derechos humanos, desplazarse de la mirada liberal. Salta: ICSO-CONICET-UNSa, 2023. Disponible en: <https://www.icsoh.unsa.edu.ar/new/libros.php?lib=40>.

HESSLING HERRERA, F. D. Hacia la exigibilidad del derecho a la energía: instrumento del derecho a la vida y vivienda adecuadas. **Revista de la Facultad de Derecho de México**, v. 74, n. 290, p. 101-124, 2024. DOI: 10.22201/fder.24488933e.2024.290.89529.

HESSLING HERRERA, F. D.; BELMONT COLOMBRES, M. E. Hábitat y vida digna a partir de las alianzas socio-técnicas de la comunidad wichí San Ignacio de Loyola (Salta, Argentina). **Hábitat y Sociedad**, n. 15, p. 211-232, 2022. DOI: 10.12795/HabitatySociedad.2022.i15.10.

INDEC. **Informes técnicos: condiciones de vida**. v. 8, n. 21: incidencia de la pobreza y la indigencia en 31 aglomerados urbanos, primer semestre de 2024. Buenos Aires: Instituto Nacional de Estadística y Censos, 2024. Disponível em: https://www.indec.gov.ar/uploads/informesdeprensa/eph_pobreza_09_241C2355AD3A.pdf.

IÑIGO CARRERA, N. **Génesis, formación y crisis del capitalismo en el Chaco 1870-1970**. Salta: Universidad Nacional de Salta, 2010.

LORETI, D.; LOZANO, L. **El derecho a comunicar: los conflictos en torno a la libertad de expresión en las sociedades contemporáneas**. Buenos Aires: Siglo XXI Editores, 2014.

MARTÍNEZ-VILLALBA, J. C. R. La cuarta ola de derechos humanos: los derechos digitales. **Revista Latinoamericana de Derechos Humanos**, v. 24, n. 1, 2014. Disponível em: <https://www.corteidh.or.cr/tablas/r33897.pdf>.

MILAN, S.; TRERÉ, E. Big Data from the South(s): Beyond Data Universalism. **Television & New Media**, v. 20, n. 4, p. 319-335, 2019. DOI: 10.1177/1527476419837739.

OECD. **Rights in the digital age: challenges and ways forward**. OECD Digital Economy Papers, n. 347, 2022. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf.

PNUD. **Acesso y uso de internet en América Latina y el Caribe. Resultados de las encuestas telefónicas de alta frecuencia de ALC 2021.** Sept. 2022. Disponível em: <https://www.undp.org/sites/g/files/zskgke326/files/2022-09/undp-brlac-Digital-ES.pdf>.

RELE. **Libertad de expresión e internet.** Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos, 2013. Disponível em: https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf.

RODRÍGUEZ GARAVITO, C. (ed.). **Litigar la emergencia climática: la movilización ciudadana ante los tribunales para enfrentar la crisis ambiental y asegurar los derechos básicos.** Buenos Aires: Siglo XXI Editores, 2022.

RODRÍGUEZ GARAVITO, C.; BAQUERO DÍAZ, A. **Conflictos socioambientales en América Latina: el derecho, los pueblos indígenas y la lucha contra el extractivismo y la crisis climática.** Ciudad de México: Siglo XXI Editores, 2020.

SOUSA SANTOS, B. **Hacia una concepción intercultural de los derechos humanos: sociología jurídica crítica. Para un nuevo sentido común del derecho.** Madrid-Bogotá: Trotta-ILSA, 2009.

STINCO, J. El principio de progresividad en materia de derechos fundamentales. **Ab-Revista de Abogacía**, v. 5, p. 49-62, 2019. Disponível em: <https://unpaz.edu.ar/sites/default/files/inline-files/5.El%20principio%20de%20progresividad.pdf>.

TELLO, A. Sobre el colonialismo digital: datos, algoritmos y colonialidad tecnológica del poder en el sur global. **InMediaciones de la Comunicación**, v. 18, n. 2, p. 89-110, 2023. DOI: 10.18861/ic.2023.18.2.3523.

JUSTIÇA EM RISCO: O PASSIVO OCULTO DA LGPD E A AMEAÇA DE INSOLVÊNCIA ESTATAL

Lydia de Jesus Azêdo Neta

Centro Integrado de Educação Superior do Amazonas (CIESA)

Pablo Oliva Souza

Universidade Federal do Amazonas (UFAM)

Taís Viga de Albuquerque Oliva Souza

Centro Integrado de Educação Superior do Amazonas (CIESA)

RESUMO

O presente artigo analisa as implicações sistêmicas da proteção de dados pessoais no Poder Judiciário Brasileiro, transcendendo a perspectiva do direito individual do titular. O estudo se inicia sublinhando a importância dos dados e informações humanas em paralelo com os direitos fundamentais de privacidade e intimidade e algumas das consequências com eventuais vazamentos de dados constantes em lides judiciais. A partir da constitucionalização do tema pela Emenda Constitucional nº 115/2022 e da aplicabilidade da Lei nº 13.709/2018 (LGPD) ao setor público, investiga-se como incidentes de segurança em larga escala podem gerar um “efeito dominó”, com potencial para desencadear uma crise fiscal para o Estado. A análise distingue a responsabilidade decorrente da atividade de gestão de dados daquela oriunda da função jurisdicional. Adicionalmente, explora-se a responsabilidade do Judiciário na qualidade de controlador, não apenas em relação aos jurisdicionados, mas também no tratamento das informações de seus próprios magistrados e servidores, no enfoque da responsabilidade civil em casos de vazamentos de informações sob a salvaguarda do Judiciário, na ótica do ordenamento jurídico vigente. Enfatiza-se a governança institucional como ferramenta central para a conformidade e mitigação de riscos, analisando criticamente a efetividade das resoluções do CNJ e o impacto de incentivos institucionais, como o Prêmio CNJ de Qualidade. Por fim, são propostas alternativas estratégicas que combinam medidas técnicas e a criação de um órgão de auditoria independente *Data Trust Judicial*, visando fortalecer o ecossistema de proteção de dados e assegurar a sustentabilidade do Estado.

Palavras-chave: Proteção de dados pessoais; poder judiciário; responsabilidade do estado; risco sistêmico; LGPD.

INTRODUÇÃO: A DIMENSÃO OCULTA DO RISCO CIBERNÉTICO JUDICIAL

A vida quotidiana no século XXI pauta-se de realidades informadas a partir do que consta na internet, em especial, dos dados, conhecimentos e informações que são produzidas, coletadas, filtradas e aplicadas acerca dos comportamentos humanos registrados em ambiente virtual. A doutrina acerca do tema, bem explicita sobre o assunto:

Dados podem ser entendidos como vestígios de fenômenos: por exemplo, eventos, experiências e experimentos. Dessa forma, dados referem-se a diferenças discerníveis e experienciáveis que fornecem os recursos a partir dos quais a informação (comunicável) é posteriormente construída. (...) Em termos de dados, realidades informadas algoritmicamente se baseiam nos rastros deixados por pessoas e objetos à medida que interagem por meio de tecnologias digitais. (FLYVERBOM E WHELAN, 2019, p. 56-64).

Na ordem jurídica internacional, a enorme escala de dados que constam sobre a vida das pessoas na rede mundial de computadores trouxe a preocupação imediata com a salvaguarda destes dados e suas implicações no ordenamento jurídico mundial. Na vanguarda dessa tendência, sobreleva-se a Recomendação CM/Rec(2018) do Comitê de Ministros aos Estados-Membros sobre as funções e responsabilidades dos intermediários da Internet (Comitê de Ministros do Conselho da Europa, 2018). Senão vejamos:

As Diretrizes têm um foco duplo: obrigações dos Estados e responsabilidades dos intermediários da Internet. As obrigações identificadas dos Estados incluem garantir a legalidade das medidas adotadas; segurança jurídica e transparência; salvaguardas da liberdade de expressão, privacidade e proteção de dados; e acesso a um recurso efetivo. As responsabilidades dos intermediários da internet incluem o respeito aos direitos humanos e às liberdades fundamentais, a transparência e a responsabilização, as responsabilidades em relação à moderação de conteúdo, o uso de dados pessoais e a garantia do acesso a um recurso efetivo. (MCGONAGLE, 2019, p. 239-240).

A constitucionalização da proteção de dados pessoais consubstanciou-se, no Brasil, por meio da Emenda Constitucional nº 115/2022, representou a resposta

do ordenamento jurídico brasileiro a uma realidade social inegável: a centralidade dos dados na vida contemporânea e a ascensão de um “capitalismo de vigilância” (ZUBOFF, 2020). As implicações do “capitalismo de vigilância” operam efeitos contundentes nas demandas apresentadas ao Judiciário, especialmente, no que tange a sua ofensa aos direitos humanos fundamentais. Destaca-se:

Apesar dos muitos esplendores do meio digital, o capitalismo de vigilância e o poder instrumental agora inscrevem nossas vidas com sua assinatura única de destruição, desafiando os direitos humanos de maneiras que não previmos e não poderíamos antecipar. Muitas antigas desigualdades são aprofundadas, enquanto eixos inteiramente novos de exclusão e dominação ameaçam todos. Disputas anteriores por direitos políticos são retomadas, direitos humanos elementares são revogados e até mesmo o “direito de ter direitos” está sob cerco. (ZUBOFF, 2019, p.06).

Nesse espectro, a análise de suas implicações para o Poder Judiciário tem se concentrado, majoritariamente, na esfera dos direitos individuais do jurisdicionado. É imperativo transcender essa visão e analisar duas dimensões interconectadas e de consequências sistêmicas: primeiro, como um incidente de segurança de dados em larga escala no Judiciário pode desencadear um efeito dominó, culminando em uma crise fiscal e de governabilidade para o Estado; e segundo, como a responsabilidade do Judiciário, na qualidade de controlador, abrange não apenas as partes de um processo, mas também o universo de dados de seus próprios magistrados e servidores, cuja proteção é igualmente crítica para a estabilidade institucional.

A análise sob enfoque distingue a função jurisdicional em si do papel do Judiciário como gestor de dados, focando nas responsabilidades gerenciais deste último e nos riscos sistêmicos que delas emanam.

O RISCO FISCAL CASCATA: DA FALHA NA GESTÃO DE DADOS À INSOLVÊNCIA ESTATAL

Entre os múltiplos lugares onde as informações e dados das pessoas encontram-se armazenados estão as demandas judiciais e processos de toda natureza, onde a vida dos jurisdicionados está minudenciada, inclusive a sua intimidade, suas particularidades e seus segredos, constitucionalmente protegidos

pelos direitos fundamentais de privacidade, patrimônio imaterial de todos. Consequentemente, eventuais vazamentos e exposições não autorizadas têm o condão de provocar prejuízos incalculáveis aos jurisdicionados e de responsabilização civil àqueles que deram causa a estes danos. Veja-se:

O vazamento de dados pessoais é basicamente a exposição de uma série de informações, incluindo dados pessoais. Dessa forma, evidenciado o valor do processamento de dados na perspectiva da sociedade informacional e o elevado risco do vazamento de dados, tem-se que o tratamento dos dados pessoais deve ser realizado de maneira adequada, tendo em vista a proteção ao titular de dados e o desenvolvimento econômico. (ABDO, 2024, p. 04).

Dentro deste prisma, a discussão sobre a responsabilidade civil por vazamento de dados no Judiciário precisa ser deslocada do plano individual para a análise de risco macroeconômico. A estrutura jurídica brasileira estabelece que o Poder Judiciário não possui personalidade jurídica própria para figurar no polo passivo de ações indenizatórias.

Conforme o art. 37, § 6º, da Constituição Federal, a responsabilidade civil por atos de seus agentes é do ente federativo ao qual o órgão pertence (a União, no caso da Justiça Federal e Tribunais Superiores, e os Estados, no caso das Justiças Estaduais).

Este desenho institucional cria um potencial de risco fiscal sem precedentes. A materialização deste risco não é um exercício de futurologia, mas uma realidade constatável. Incidentes de segurança recentes, como o acesso indevido a dados do sistema Sisbajud do Conselho Nacional de Justiça (CNJ) em julho de 2025 e o ataque coordenado à Justiça do Trabalho em outubro de 2025, que paralisou diversos Tribunais Regionais do Trabalho (TRTs), demonstram a vulnerabilidade sistêmica.

O mais grave é que, em muitos desses casos, a real extensão dos danos e os impactos concretos para os milhões de jurisdicionados cujos dados foram potencialmente comprometidos permanecem uma incógnita. Diante deste quadro, um ataque cibernético de maior escala que exfiltre e exponha publicamente a base de dados de um grande tribunal é um cenário plausível. O resultado imediato seria uma avalanche de ações de responsabilidade civil contra o respectivo ente federativo.

É crucial sublinhar que esta responsabilidade civil do Estado não emana do conteúdo das decisões judiciais – atos protegidos pela soberania da coisa julgada – mas sim da falha na atividade de custódia e gestão dos dados pessoais. A LGPD, em seu art. 42, estabelece que o controlador que causar dano a outrem em violação à legislação é obrigado a repará-lo. Embora a lei não especifique a modalidade de responsabilidade para o Poder Público, uma interpretação sistêmica e hermenêutica aponta para a responsabilidade objetiva.

Essa conclusão decorre da harmonização da LGPD com o art. 37, § 6º, da Constituição Federal, que já consagra a responsabilidade objetiva para o Estado. Desse modo, para a configuração do dever de indenizar, não se exige a comprovação de dolo ou culpa do agente público, bastando a demonstração do nexo causal entre o incidente de segurança (a falha na gestão) e o dano sofrido pelo titular (BERCI; LANNES; STEFANELLI, 2023).

A magnitude do passivo estatal se agrava com a controvérsia sobre a natureza do dano moral em casos de vazamento. A jurisprudência do Superior Tribunal de Justiça tem evoluído para consolidar uma tese intermediária, que busca equilibrar a proteção ao titular com a prevenção da chamada “indústria do dano moral”.

Conforme decidido no REsp n. 2.121.904/SP, a corte estabeleceu um critério de distinção crucial: o vazamento de dados pessoais genéricos (como nome e CPF) não gera, por si só, um dano moral presumido, exigindo que o titular comprove o prejuízo sofrido. Contudo, a mesma decisão reafirma que, na hipótese de vazamento de dados sensíveis (como informações sobre saúde, vida sexual, convicção religiosa ou política), o dano moral é presumido (*in re ipsa*), pois a mera exposição de tais informações já representa uma violação grave à privacidade e à dignidade do indivíduo.

Essa tese, que refina o entendimento anterior (BERCI; LANNES; STEFANELLI, 2023), é particularmente alarmante para o contexto judicial, pois a vasta maioria das informações contidas em processos judiciais se enquadra na categoria de dados sensíveis.

Assim, a consolidação desse entendimento tem o potencial de validar um volume massivo de pedidos indenizatórios em caso de incidente, transformando o risco fiscal em uma ameaça concreta à sustentabilidade do Estado.

Esse passivo não seria apenas uma questão de pagar indenizações. Um volume de condenações dessa magnitude poderia inviabilizar o orçamento público, comprometendo a prestação de serviços essenciais.

O pagamento de precatórios decorrentes dessa “litigância de dados” poderia consumir a capacidade de investimento do Estado por anos, gerando uma crise de governabilidade. Portanto, a segurança da informação no Judiciário deixa de ser uma mera questão de conformidade e se torna um pilar da responsabilidade fiscal.

O CONTROLADOR VOLTADO PARA DENTRO: A GOVERNANÇA INSTITUCIONAL SOB TENSÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) define o controlador como aquele a quem competem as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018).

Esta definição não admite exceções para o Poder Judiciário, que, em todas as suas instâncias, se enquadra perfeitamente no conceito. A lei é explícita em sua aplicação às pessoas jurídicas de direito público (art. 1º, parágrafo único, II), impondo-lhes as mesmas obrigações de segurança e governança.

O Conselho Nacional de Justiça, ciente deste novo cenário, editou normativos importantes, como a Resolução CNJ nº 363/2021, que estabelece medidas para o processo de adequação à LGPD, e a Resolução CNJ nº 370/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação (ENTIC-JUD).

Embora meritórias, a efetividade de tais resoluções é questionável diante da realidade operacional. A ENTIC-JUD traça diretrizes macro, mas a implementação é descentralizada, resultando em um mosaico de maturidade digital e de segurança entre os mais de 90 tribunais do país. Essa fragmentação cria elos fracos na corrente de proteção de dados, que podem ser explorados por agentes maliciosos, como evidenciado pelos recentes ataques.

Agrava-se a este cenário a cultura institucional fomentada pelo Prêmio CNJ de Qualidade. A “corrida por medalhas”, que premia tribunais por produtividade e inovação tecnológica, pode gerar um efeito colateral perverso: a priorização da celeridade no desenvolvimento e na implementação de novas ferramentas

digitais em detrimento de uma análise de riscos aprofundada e da incorporação de salvaguardas de privacidade desde a concepção *privacy by design*.

A pressão por atingir metas e obter reconhecimento pode levar a um *compliance* teatral, onde a segurança da informação torna-se um item de *checklist* a ser cumprido formalmente, e não um pilar estruturante da gestão de dados.

Nesse contexto, a estrutura de governança institucional deixa de ser uma mera recomendação para se tornar o epicentro da estratégia de conformidade e mitigação de riscos.

Uma governança robusta é o que permite ao Judiciário demonstrar o seu dever de cuidado e prestação de contas (*accountability*). Sem ela, a responsabilidade por um incidente torna-se quase indefensável.

O vazamento de dados de magistrados, servidores e terceirizados, tratados em sistemas de RH e administrativos, representa uma ameaça direta à independência do próprio Judiciário, podendo expô-los a coação e extorsão.

A falha em proteger seus agentes internos, muitas vezes negligenciada em prol da tecnologia voltada ao processo judicial, pode ser o gatilho para a crise fiscal sistêmica descrita anteriormente.

SUGESTÕES ESTRATÉGICAS: DA MITIGAÇÃO TÉCNICA À GOVERNANÇA DE RISCO FINANCEIRO

Diante deste cenário de risco amplificado e em cumprimento aos deveres impostos pela LGPD ao controlador, uma postura meramente reativa é insustentável. A adoção de uma robusta estrutura de governança é mandatória, e as seguintes sugestões estratégicas compõem os pilares de uma defesa em profundidade:

1. Governança Centralizada e Auditoria Externa (Modelo *Data Trust*):

os incidentes de segurança e a cultura da “corrida por medalhas” demonstram que o modelo de governança descentralizada e auto declaratória é insuficiente.

É imperativo evoluir para um sistema de verificação externa. Sugere-se a criação, sob a égide do CNJ, de um órgão técnico central com autonomia — um

Data Trust Judicial — cuja função seria estabelecer padrões mínimos obrigatórios de segurança cibernética e, crucialmente, realizar auditorias externas e testes de penetração periódicos e independentes em todos os tribunais.

A conformidade deixaria de ser uma meta para um prêmio e passaria a ser uma condição de funcionamento continuamente verificada.

2. Contratação de Seguro de Responsabilidade Cibernética pelo Estado: para mitigar o risco fiscal, os entes federativos (União e Estados) deveriam ser compelidos a contratar apólices de seguro de responsabilidade cibernética de larga escala. Essa medida transforma um passivo potencial e incalculável em um custo fixo e orçamentável.

3. Desenvolvimento de Protocolos de Gestão de Litígios em Massa: a Advocacia-Geral da União (AGU) e as Procuradorias-Gerais dos Estados (PGEs) devem, proativamente, desenvolver planos de contingência e protocolos jurídicos específicos para a gestão de litígios em massa decorrentes de incidentes de dados.

A implementação articulada destas sugestões materializa o programa de governança em privacidade exigido pela LGPD (art. 50). Trata-se de uma resposta lógica e necessária ao atual estágio de desenvolvimento tecnológico, exigindo dos entes estatais uma adaptação que vá além da mera digitalização de processos.

CONSIDERAÇÕES FINAIS

Ao longo deste estudo, buscou-se descortinar a importância da preservação dos dados no âmbito das demandas judiciais e das informações que constam no bojo destes processos sob a salvaguarda do Judiciário, levando-se em conta, possível exposição indevida destes dados e a consequente responsabilização por vazamentos, nos moldes do arcabouço jurídico em vigor no Brasil.

Dentro desta premissa, a proteção de dados no Poder Judiciário revela-se uma questão de segurança nacional e estabilidade fiscal. A falha em tratar o tema com a seriedade que ele exige pode resultar em consequências que

vão muito além da violação de direitos individuais, ameaçando a capacidade operacional e financeira do Estado.

A responsabilidade do Judiciário como controlador é um dever de dupla face: proteger o cidadão que busca seus serviços e proteger a si mesmo e seus agentes para garantir a continuidade e a independência de sua missão constitucional.

A adoção de medidas proativas, que enxerguem o problema de forma sistêmica e questionem os próprios incentivos institucionais, não é mais uma opção, mas uma condição de sobrevivência institucional na era digital.

REFERÊNCIAS

ABDO, Bianca Maria Marinoni. **Responsabilidade civil por incidentes de segurança e vazamento de dados**. Revista Foco. Indisciplinary Studies, São Paulo, v.17, n. 11, p. 01-20, Outubro, 2024.

BERCI, Luan; LANNES, Yuri Nathan da Costa; STEFANELLI, Stefania. **A responsabilidade civil do poder judiciário frente ao vazamento de dados dos tribunais sob a óptica da lei geral de proteção de dados**. Revista Jurídica Direito & Paz, São Paulo, Ano XVII, n. 48, p. 4-18, 1º Semestre, 2023.

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

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 out. 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir no rol dos direitos e garantias fundamentais o direito à proteção de dados pessoais, inclusive nos meios digitais. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 11 out. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 out. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 2.121.904 - SP**. Relatora: Ministra Nancy Andrighi. Terceira Turma. Julgado em 11/02/2025. Diário da Justiça Eletrônico, 17/02/2025.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 363, de 12 de janeiro de 2021**. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) a serem observadas por todos os órgãos do Poder Judiciário. Diário da Justiça Eletrônico, Brasília, DF, n. 16, p. 2-5, 19 jan. 2021.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 370, de 28 de janeiro de 2021.** Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD). Diário da Justiça Eletrônico, Brasília, DF, n. 32, p. 2-15, 1 fev. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Thomson Reuters Brasil, 2019.

FLYVERBOM, Mikkell; WHELAN, Glen. **Transformações digitais, realidades informadas e conduta humana.** In: JORGENSEN, Rikke Frank. Direitos Humanos na era das plataformas. Massachusetts: IMT, 2019. p. 53-72.

JORGENSEN, Rikke Frank. **Direitos Humanos na era das plataformas.** Massachusetts: IMT, 2019.

MACGONAGLE, Tarlach. **O conselho da Europa e os intermediários da internet: um estudo de caso de postura provisória.** In: JORGENSEN, Rikke Frank. Direitos Humanos na era das plataformas. Massachusetts: IMT, 2019. p. 227-254.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados Comentada.** São Paulo: Thomson Reuters Brasil, 2021.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014.

CONSULTOR JURÍDICO. **Onda de invasões hackers expõe fragilidades nas estruturas tecnológicas de tribunais.** Consultor Jurídico, 15 abr. 2022. Disponível em: <https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais/>. Acesso em: 11 out. 2025.

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

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119/1, 4 maio 2016.

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

ZUBOFF, Shoshana. **Nós os fazemos dançar: capitalismo de vigilância, a ascensão do poder instrumental e a ameaça a Direitos Humanos.** In: JORGENSEN, Rikke Frank. Direitos Humanos na era das plataformas. Massachusetts: IMT, 2019. p. 03-52.

A ESCALADA DAS DEEPPFAKES E CRIPTOFRAUDES NO BRASIL: ANÁLISE DA RESPOSTA JURÍDICA E DESAFIOS ESTRATÉGICOS FRENTE À INTELIGÊNCIA ARTIFICIAL

Jaison Sfogia Ricardo

RESUMO

O avanço exponencial da inteligência artificial (IA) tem impulsionado a proliferação de deepfakes – conteúdos multimídia sintéticos ultrarrealistas – que, em conjunto com a pseudonimidade dos criptoativos, configuram um vetor crescente para fraudes financeiras e crimes cibernéticos. Esquemas como *pig butchering*, *rug pulls*, manipulação de mercado e fraudes de identidade são amplificados pela IA, resultando em perdas financeiras globais que alcançaram US\$ 79,1 bilhões desde 2022. Um estudo da Sumsb (2024) posiciona o Brasil entre os dez com maior número de ataques baseados em deepfakes, com um aumento significativo de ocorrências no período analisado, especialmente no segmento de criptomoedas. Diante dessa complexidade, o Brasil tem adaptado sua legislação, com destaque para a Lei nº 14.478/2022, que regulamenta os prestadores de serviços de ativos virtuais (PSAVs), aprimora o combate à lavagem de dinheiro (PLD/FT) e introduz o tipo penal de fraude com ativos virtuais (Art. 171-A do Código Penal). Este artigo analisa criticamente a evolução e os impactos das deepfakes e criptofraudes, a resposta legislativa e operacional brasileira, e os desafios remanescentes na mitigação desses riscos, propondo medidas estratégicas para fortalecer a resiliência nacional.

Palavras-chave: Deepfake; Criptoativos; Fraude Digital; Inteligência Artificial.

INTRODUÇÃO

A era digital, embora catalisadora de inovações, é igualmente palco de novas e complexas ameaças cibernéticas. Dentre estas, as deepfakes – conteúdos multimídia (vídeo, imagem e áudio) criados ou manipulados por inteligência artificial (IA) para simular autenticidade – emergiram como um fenômeno de rápido crescimento e disseminação, impulsionadas pelo acesso a aplicativos intuitivos e tecnologias generativas avançadas, como autoencoders¹ e Redes Adversárias Generativas (GANs).

A previsão de 8 milhões de deepfakes compartilhados em 2025, em contraste com 500 mil em 2023, e a projeção da Europol de que 90% do conteúdo on-line será sinteticamente gerado até 2026, sublinham a dimensão do desafio imposto à confiança institucional e social (NEGREIRO, 2025).

Embora a tecnologia de deepfake possua aplicações legítimas em setores como entretenimento e comunicação, seu uso criminoso tem se intensificado. No âmbito financeiro, a IA amplifica a capacidade de fraudadores, viabilizando golpes sofisticados em larga escala.

Relatórios recentes indicam que as perdas globais de operações fraudulentas envolvendo criptomoedas atingiram US\$ 79,1 bilhões desde o início de 2022, com projeção de crescimento trimestral para US\$ 10 bilhões até 2025. Estima-se que a participação de crimes de deepfake no espaço cripto possa alcançar 70% até o início de 2026, caso medidas eficazes não sejam implementadas (BITGET, 2024).

Um estudo da Sumsb (2024) posiciona o Brasil entre os dez com maior número de ataques baseados em deepfakes, com um aumento de 830% entre 2021 e 2023, e 82% somente no segmento de criptomoedas. Essas ocorrências, frequentemente enquadradas como estelionato, abrangem modalidades diversas, incluindo vendas fraudulentas, aplicações financeiras enganosas, pedidos de Pix e pirâmides financeiras.

¹ Autoencoder: Tipo de rede neural que aprende codificações eficientes de dados não rotulados por compressão seguida de reconstrução (BANK; KOENIGSTEIN; GIRYES, 2020).

Este artigo se insere na interseção entre a IA aplicada ao cibercrime e o direito penal, visando aprofundar os marcos conceituais de segurança cibernética e responsabilização digital.

A análise crítica aqui desenvolvida é sustentada por uma metodologia que integra a aplicação de um arcabouço teórico-conceitual em segurança cibernética e direito penal, assegurando a robustez da pesquisa e a coerência argumentativa.

Em resposta à materialização dessas ameaças no contexto nacional, este estudo busca: (i) definir o conceito de deepfakes e identificar as principais modalidades de criptofraude impulsionadas por IA; (ii) investigar os padrões e a dinâmica desses crimes no Brasil, com foco nas plataformas mais vulneráveis; (iii) analisar o impacto da Lei nº 14.478/2022 e de outras normas no enfrentamento dessas práticas ilícitas; e (iv) avaliar os desafios enfrentados por autoridades e pelo setor privado na detecção e prevenção de deepfakes e criptofraudes, culminando na proposição de medidas estratégicas (tecnológicas, regulatórias e educativas) para fortalecer a resiliência nacional.

DEEPPAKES E MODALIDADES DE CRIPTOFRAUDE AMPLIFICADAS POR IA

Esta seção estabelece os conceitos fundamentais para a compreensão das ameaças analisadas, detalhando a natureza das deepfakes e as principais modalidades de fraudes em criptoativos potencializadas pela inteligência artificial.

Deepfakes: Definição, Geração e Desafios de Detecção

De acordo com Negreiro (2025), Deepfakes são mídias sintéticas – vídeos, imagens e áudios – geradas ou manipuladas por inteligência artificial (IA) para simular autenticidade e distorcer a realidade, parecendo autênticas.

A tecnologia subjacente emprega IA generativa avançada, notadamente autoencoders e Redes Adversárias Generativas (GANs), para criar conteúdo hiper-realista. Embora o termo tenha se popularizado em 2017, a facilidade de criação de deepfakes tem aumentado exponencialmente, exigindo apenas um dispositivo móvel e software adequado (NEGREIRO, 2025).

A detecção de deepfakes, no entanto, persiste como um desafio complexo. Apesar do surgimento de soluções corporativas desde 2022, usuários comuns, desprovidos de conhecimento técnico, permanecem altamente vulneráveis.

Para Papasavva *et al* (2025), as ferramentas de detecção frequentemente se mostram ineficazes frente aos avanços dos geradores de deepfakes, resultando em um constante “jogo de gato e rato” entre fraudadores e provedores de segurança.

Essa limitação decorre do fato de que os algoritmos de detecção dependem de dados falsos criados por essas mesmas ferramentas de geração, em um ciclo contínuo de adaptação e superação.

Modalidades de Criptofraude Impulsionadas por IA

A IA e as tecnologias de deepfake não apenas diversificam, mas também amplificam a escala e a sofisticação dos crimes financeiros e cibernéticos. As principais modalidades de criptofraude potencializadas por essas tecnologias incluem:

Golpes de *Pig Butchering* (Engorda de Porcos): Originário da China, este golpe de investimento estabelece uma relação de confiança com a vítima, manipulando-a para realizar grandes investimentos em plataformas fraudulentas antes de desaparecer com os fundos. A IA é instrumentalizada para gerar respostas contextualmente apropriadas 24 horas por dia e para viabilizar interações por vídeo deepfake em tempo real, conferindo maior credibilidade ao golpista. Sistemas de IA podem, ainda, analisar vastos volumes de dados públicos para personalizar o ataque e explorar vulnerabilidades pessoais em larga escala (CHAI-NALYSIS, 2025a).

Rug Pulls: Neste esquema, desenvolvedores de novos projetos de criptomoedas promovem um token para atrair investidores e, subsequentemente, abandonam o projeto, retirando todos os fundos de liquidez e tornando os ativos dos investidores sem valor. A IA pode ser empregada para criar consenso artificial e disseminar desinformação, explorando falhas de código ou a ausência de bloqueio de liquidez inicial (WU et al., 2025).

Pump & Dump: Diferente dos *rug pulls*, estes esquemas de manipulação de mercado podem ser orquestrados por qualquer indivíduo ou grupo com grandes posses de um token e capacidade de influenciar outros a comprá-lo. Grupos coordenados utilizam-se de desinformação e criação de publicidade extravagante ou enganosa para inflacionar artificialmente o preço de um token (*pump*), atraindo novos compradores. Os golpistas então vendem (*dump*) o ativo supervalorizado com lucro, deixando os investidores com ativos desvalorizados (ELLIPTIC, 2024).

Phishing e Ice Phishing: Embora não sejam modalidades recentes, esses ataques são intensificados pela IA. O *phishing* visa enganar as vítimas para que revelem credenciais ou transfiram criptomoedas. O *ice phishing* refere-se a casos em que contratos inteligentes maliciosos drenam a carteira de uma vítima que concedeu acesso, geralmente após falsas promessas de tokens gratuitos inexistentes ou oportunidades de investimento. A IA é utilizada para criar e-mails de *phishing* sofisticados, sites falsos e mensagens diretas que imitam com perfeição a linguagem natural. Adicionalmente, *scambots* alimentados por IA podem ser tão eficazes, ou mais, que engenheiros sociais experientes em conduzir conversas telefônicas em tempo real com vozes clonadas e consciência contextual (FATF, 2023).

ANÁLISE E DISCUSSÃO: CENÁRIO BRASILEIRO, RESPOSTA LEGISLATIVA E DESAFIOS

Esta seção aprofunda o contexto nacional dos cibercrimes impulsionados por deepfakes e IA, examina a resposta jurídica e institucional do Brasil, e discute os desafios persistentes.

Cenário Brasileiro de Cibercrime e Deepfakes

Dados recentes apontam uma transformação expressiva no perfil da criminalidade no Brasil. Segundo o Fórum Brasileiro de Segurança Pública (2024), os crimes de estelionato ultrapassaram, pela primeira vez, os registros de roubo. Em 2023, foram contabilizados 1.965.353 casos de estelionato, contra

870.320 roubos, revertendo completamente o cenário de 2018, quando os roubos superavam os estelionatos em mais de 1 milhão de ocorrências.

Esse crescimento está fortemente vinculado ao avanço das fraudes digitais. Os estelionatos cometidos por meio virtual aumentaram 13,6% entre 2022 e 2023, com elevações especialmente expressivas na Paraíba (+153,7%), Roraima (+143,3%), Piauí (+111,6%) e Amazonas (+109,3%) (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2024). Essa dinâmica sinaliza uma reconfiguração da criminalidade patrimonial, marcada pela prevalência de golpes virtuais em detrimento dos crimes tradicionais.

Paralelamente, constata-se uma escalada no uso malicioso de tecnologias avançadas, como deepfakes, e no crescimento das criptofraudes. O *Sumsb Identity Fraud Report 2024*, que analisa tendências globais e estratégias de prevenção à fraude de identidade, destaca o Brasil entre os 15 países com menor proteção contra esse tipo de crime (SUMSUB, 2024).

O *Índice Global de Fraude 2024* (SUMSUB, 2024) revela que o país apresentou um aumento médio de 137% nos casos de fraude de identidade, figurando entre os dez países latino-americanos com maior crescimento — 144% entre 2023 e 2024. As taxas brasileiras passaram de 0,37% em 2022 para 0,67% em 2023 e atingiram 0,96% em 2024, refletindo uma tendência de crescimento sustentado.

A sofisticação crescente dos métodos empregados pelos criminosos representa um desafio central. Tecnologias de inteligência artificial têm sido instrumentalizadas para a criação de conteúdos fraudulentos altamente verossímeis — como textos, áudios e vídeos manipulados — facilitando a prática de crimes. Casos emblemáticos ilustram a gravidade do problema:

- **Operação Voiceover (PCDF, 2025):** desarticulou quadrilha que utilizava deepfakes da imagem e voz do apresentador Marcos Mion para promover promoções falsas e direcionar vítimas a sites fraudulentos, com o intuito de coletar dados pessoais e aplicar golpes financeiros (FORBES BRASIL, 2025).
- **Fraudes Bancárias e de Identidade:** operações como *Deep Fraud* (Bahia) e *Deep Fake* (Goiás) evidenciaram o uso de identidades sintéticas para burlar sistemas bancários e acessar créditos por meio de

mecanismos que contornam políticas de KYC (Conheça seu Cliente) e autenticação de dois fatores (CHAINALYSIS, 2025b).

- **Abuso Sexual Infantil e Cyberbullying:** o uso de IA também se estende à criação de conteúdos abusivos, como nos casos ocorridos em Maceió (abril de 2024), em que imagens pornográficas manipuladas de adolescentes foram compartilhadas via WhatsApp (GOVERNO DE ALAGOAS, 2025). A gravidade da prática impulsionou alterações legislativas, como a Lei nº 15.123/2025, que agravou as penas de violência psicológica quando cometida com uso de IA para manipulação de imagem ou som (BRASIL, 2025; NEGREIRO, 2025).

Além disso, relatórios apontam o crescimento da atuação de organizações cibercriminosas no país. A Kaspersky (2025) identificou a atuação de 30 grupos de ransomware, com 114 ataques executados e o vazamento de 309 bancos de dados corporativos pertencentes a 185 organizações brasileiras.

A Europol (2025) corrobora esse diagnóstico ao indicar que o crime organizado tem intensificado sua atuação em ambientes digitais, aproveitando-se da infraestrutura tecnológica para operar em maior escala e velocidade.

Grupos especializados em fraudes facilitadas por tecnologia (cyber-enabled fraud – CEF) e em lavagem de dinheiro por meio de contas bancárias virtuais internacionais (vIBANs) recorrem com frequência a táticas como mulas de dinheiro e empresas de fachada para ocultar a origem e o destino dos fundos ilícitos (FATF, 2023).

Casos como as operações Flying Dutchman, com R\$ 4,1 bilhões movimentados por meio de empresas de fachada e laranjas, e Kryptos, que revelou R\$ 38 bilhões em esquemas de pirâmide financeira com criptoativos, evidenciam a sofisticação das estruturas criminosas (POLÍCIA FEDERAL, 2025).

O cenário é agravado pelo crescimento do roubo de dados pessoais e credenciais. Relatório da Kaspersky (2025) identificou mais de 37 milhões de registros de domínios .br comprometidos em 2024, além da atuação de facções criminosas que utilizam celulares furtados para realizar golpes via Pix.

Essa intersecção entre criminalidade física e digital reforça o diagnóstico do Fórum Brasileiro de Segurança Pública (2024): o Brasil se tornou um alvo

atraente para o cibercrime em virtude de seu tamanho populacional, dinamismo econômico e diversidade digital.

Marco Regulatório Nacional: A Lei nº 14.478/2022 e a LGPD

A crescente preocupação com a criminalidade envolvendo criptoativos impulsionou a criação de um marco regulatório no Brasil, com destaque para a Lei nº 14.478/2022, em vigor desde junho de 2023.

Lei nº 14.478/2022 (Lei dos Criptoativos)

Esta lei estabelece diretrizes para a prestação de serviços de ativos virtuais (PSAVs) e a regulamentação de suas prestadoras, sendo crucial para a segurança jurídica e o combate à lavagem de dinheiro.

- **Conceitos Legais:** Define ativo virtual como representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para pagamentos ou investimento, alinhando-se ao Grupo de Ação Financeira Internacional (FATF, 2023). A prestadora de serviços de ativos virtuais (PSAVs) é a pessoa jurídica que executa, em nome de terceiros, serviços como troca entre ativos e moedas fiduciárias, transferência, custódia, ou participação em ofertas de ativos virtuais (BRASIL, 2022).
- **Diretrizes e Equiparação das PSAVs a Instituições Financeiras:** A lei exige a observância de diretrizes como livre iniciativa, boas práticas de governança, transparência, segurança da informação, proteção de dados pessoais, proteção de consumidores e usuários, e, crucialmente, prevenção à lavagem de dinheiro (PLD) e ao financiamento do terrorismo (FT). Um avanço fundamental é a alteração da Lei nº 7.492/1986 (Lei de Crimes Contra o Sistema Financeiro Nacional), equiparando as PSAVs a instituições financeiras para fins penais. Isso permite a aplicação de crimes contra o Sistema Financeiro Nacional (SFN), como gestão fraudulenta (Art. 4º) ou operação clandestina (Art. 16), aos seus dirigentes, conferindo maior segurança jurídica à per-

seção penal em esquemas complexos como a Operação Kryptos (BRASIL, 2022).

- **Aprimoramentos no Combate à Lavagem de Dinheiro (PLD/FT):** A Lei nº 14.478/2022 fortalece significativamente o sistema de PLD/FT:
 - **Nova Majorante:** Cria-se uma nova causa de aumento de pena (de 1/3 a 2/3) para o crime de lavagem de dinheiro quando cometido por meio da utilização de ativo virtual, justificando-se pela maior dificuldade de rastreamento, apreensão, volatilidade e pseudoanonimato desses ativos (BRASIL, 2022).
 - **Inclusão de PSAVs como Sujeitos Obrigados:** O rol de pessoas que devem cumprir obrigações de compliance PLD/FT é ampliado para incluir as PSAVs no Art. 9º da Lei nº 9.613/1998, impondo-lhes deveres como análise de risco, KYC, registro detalhado de operações, comunicação de operações suspeitas ao COAF e desenvolvimento de sistemas de compliance (BRASIL, 2022).
 - **Inclusão de Ativos Virtuais em Comunicações Automáticas:** De acordo com a Lei nº 9.613/1998 (art. 10, II; art. 11, II, "a"), os ativos virtuais devem ser registrados e comunicados automaticamente ao COAF sempre que ultrapassarem o limite estipulado pelas autoridades (BRASIL, 1998).
 - **Cadastro Nacional de Pessoas Expostas Politicamente (CNPEP):** Conforme o art. 12-A da Lei 9.613/1998, regulamentado pelo Poder Executivo e operacionalizado pelo COAF, foi instituído o CNPEP para sistematizar dados sobre pessoas politicamente expostas, reforçando o compliance em prevenção à lavagem de dinheiro e ao financiamento do terrorismo ao exigir consulta obrigatória aos PEPs pelos sujeitos obrigados (BRASIL, 1998).
- **O Novo Crime de Fraude (Art. 171-A do Código Penal):** Foi introduzido o Art. 171-A no Código Penal, estabelecendo como crime a "fraude com a utilização de ativos virtuais, valores mobiliários ou quaisquer ativos financeiros", e prevê pena de reclusão de 4 a 8 anos e multa. Configura-se quando alguém "organizar, gerir, ofertar ou distribuir

carteiras, ou intermediar operações” com esses ativos com o objetivo de obter vantagem ilícita, em prejuízo de outrem, “induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento” (BRASIL, 2022). É crucial notar que nem toda fraude com criptoativos se enquadrará no Art. 171-A. De acordo com Aras (2023), quando a fraude se refere à gestão, oferta ou intermediação de operações envolvendo ativos virtuais, valores mobiliários ou ativos financeiros, é um crime contra o SFN, de competência federal e ação penal pública incondicionada. Contudo, quando a fraude atinge o patrimônio da vítima sem essas circunstâncias elementares (ex: acesso à chave criptográfica privada por engenharia social e transferência de bitcoins), trata-se de um crime patrimonial como estelionato comum (Art. 171, *caput*) ou fraude eletrônica (Art. 171, §2º-A do CP).

A Lei Geral de Proteção de Dados (LGPD) e Outras Normas

A Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – constitui um alicerce fundamental para a proteção dos dados pessoais, uma categoria particularmente sensível frente ao aumento de deepfakes e fraudes em criptoativos (BRASIL, 2018).

- **Proteção de Dados Pessoais como Diretriz Legal para PSAVs:** A Lei nº 14.478/2022 estabelece, em seu art. 4º, como diretriz fundamental para as Prestadoras de Serviços de Ativos Virtuais (PSAVs), a “segurança da informação e proteção de dados pessoais” (BRASIL, 2022). Com isso, essas entidades são obrigadas a tratar os dados conforme os parâmetros da LGPD — Lei nº 13.709/2018 — especialmente em procedimentos de KYC para prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo, garantindo que dados sensíveis sejam coletados, tratados e armazenados com segurança, finalidade específica e respaldo do consentimento (BRASIL, 2018). A mesma Lei nº 14.478/2022, ao alterar a Lei nº 9.613/1998, impõe ainda às PSAVs dever legal de manter sigilo e cadastros de clientes continuamente atualizados, com registro detalhado de operações, reforçando

controles contra fraudes e irregularidades (BRASIL, 2022).

- **Combate a Fraudes de Identidade e Deepfakes:** Negreiro (2025) destaca que deepfakes manipulam dados pessoais como imagem e voz para criar conteúdos sintéticos e burlar controles de segurança. A LGPD, ao garantir direitos dos titulares de dados (acesso, correção, eliminação), oferece arcabouço legal para vítimas de deepfakes buscarem reparação. A Lei nº 15.123/2025, que aumentou a pena para violência psicológica contra a mulher com uso de IA que altere imagem ou som da vítima, demonstra o reconhecimento legislativo do dano causado pela manipulação de dados pessoais via deepfake, sendo a LGPD um complemento essencial para o tratamento ético da IA (BRASIL, 2025).
- **Impacto nos Dados Pessoais (PL 2338/2023):** O Projeto de Lei (PL) nº 2338/2023, que visa estabelecer normas para a governança responsável de sistemas de IA, reforça a importância da LGPD, preconizando o “direito à privacidade e à proteção de dados pessoais” como princípio fundamental (BRASIL, 2023). O PL prevê que a “avaliação de impacto algorítmico” poderá ser realizada em conjunto com o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) da LGPD, garantindo que riscos à privacidade e segurança de dados sejam avaliados desde a concepção de sistemas de IA. Além disso, o PL determina que agentes de IA generativa com risco sistêmico devem processar apenas conjuntos de dados coletados e tratados em conformidade com as exigências legais, especialmente dados pessoais, conforme a LGPD (BRASIL, 2023).

Em suma, a LGPD atua como uma camada essencial de proteção, garantindo que o avanço tecnológico e o combate a crimes digitais não comprometam os direitos fundamentais à privacidade e proteção de dados pessoais, ao mesmo tempo em que oferece uma base para responsabilização e reparação de danos.

Análise Crítica da Resposta Legislativa e Desafios Remanescentes

A resposta legislativa brasileira, embora posterior à velocidade da inovação tecnológica, tem demonstrado esforços significativos para se adaptar às novas realidades criminosas.

A Lei nº 14.478/2022 representa um marco importante ao regulamentar o mercado de criptoativos e introduzir ferramentas penais e de compliance.

Pontos Fortes da Lei nº 14.478/2022

- **Segurança Jurídica:** Ao definir legalmente ativo virtual e prestador de serviços de ativos virtuais (PSAVs) em consonância com padrões internacionais (GAFI), a lei confere maior segurança jurídica para a aplicação de normas penais e administrativas, eliminando incertezas anteriores (ARAS, 2023).
- **Equiparação das PSAVs a Instituições Financeiras:** A alteração na Lei nº 7.492/1986, que equipara as PSAVs a instituições financeiras para fins penais, é um avanço crucial, permitindo a aplicação de crimes contra o SFN aos seus dirigentes e administradores.
- **Combate à Lavagem de Dinheiro (PLD/FT):** A inclusão das PSAVs no rol de sujeitos obrigados da Lei nº 9.613/1998 e a majoração da pena para lavagem de dinheiro com uso de ativo virtual fortalecem o sistema PLD/FT. Segundo Aras (2023), as obrigações de compliance (KYC, registro de transações, comunicação ao COAF) e a criação do CNPEP são instrumentos vitais para rastrear e combater fluxos financeiros ilícitos.
- **Novo Tipo Penal (Art. 171-A CP):** A criação de um crime específico para fraudes com ativos virtuais, valores mobiliários ou ativos financeiros, com pena elevada e natureza de crime contra o SFN, é uma resposta direta à sofisticação dessas fraudes. Sua competência federal e ação penal incondicionada agilizam a persecução penal em casos de alta complexidade e impacto sistêmico (ARAS, 2023).
- **Proteção ao Consumidor e Usuário:** As diretrizes legais garantem

a defesa dos consumidores e usuários, reduzindo os impactos de fraudes e golpes. Reconhecendo sua vulnerabilidade, a lei estabelece mecanismos de prevenção, reparação e responsabilização, além de promover maior transparência nas operações e reforçar a confiança do público nos mercados financeiros e de consumo (SILVA; PEREIRA, 2025).

Desafios e Lacunas Remanescentes

Apesar dos avanços, a legislação enfrenta desafios inerentes à natureza dinâmica da tecnologia e do crime.

- **Velocidade da Inovação Criminal:** De acordo com Dowbor (2017), a legislação sempre tenderá a ser mais lenta que a evolução tecnológica. Deepfakes e métodos de fraude aprimoram-se constantemente, exigindo atualização contínua das normas e das ferramentas de detecção.
- **Descentralização e Anonimato:** A natureza descentralizada do mercado cripto e o pseudoanonimato das transações dificultam o rastreamento e a identificação dos responsáveis (ELLIPTIC, 2025a). Mesmo com a regulamentação das PSAVs, criminosos podem preferir operar em meios descentralizados para burlar o controle estatal.
- **Prova de Materialidade e Autoria:** A dificuldade em identificar operações realizadas fora do escopo das PSAVs e em comprovar a prática reiterada do crime (elemento da majorante de lavagem de dinheiro) pode dificultar a aplicação das novas penas (ARAS, 2023).
- **Regulamentação Infralegal:** A efetividade da Lei nº 14.478/2022, de acordo com Aras (2023), dependerá da agilidade e abrangência das regulamentações infralegais que delegam a órgãos do Poder Executivo a definição de parâmetros e a disciplina do funcionamento das PSAVs.
- **Harmonização Internacional:** A natureza transnacional dos crimes exige cooperação internacional robusta. Desafios como a dissimilari-

dade de prioridades de cooperação e a lentidão da assistência jurídica mútua formal persistem (FATF, 2023).

- **Fator Humano e Escassez de Habilidades em Cibersegurança:** O fator humano permanece uma das vulnerabilidades mais sérias, e a escassez de pessoal qualificado em cibersegurança aumenta o custo das violações de dados, impactando a capacidade de resposta das organizações (IBM, 2024).

Resposta Institucional e Estratégias para o Futuro

A resposta eficaz aos deepfakes e às criptofraudes é multifacetada, exigindo a colaboração de diversos atores e o investimento em estratégias adaptativas.

- **Tecnologia de Detecção e Prevenção:** Ferramentas como Chainalysis Alterya e RPHunter utilizam IA para escalar a detecção de golpes e automatizar a resposta a ameaças (CHAINALYSIS, 2025a). Contudo, Papasavva et al (2025) destaca que essas ferramentas frequentemente ficam aquém dos geradores de deepfakes, pois o treinamento dos algoritmos de detecção depende dos dados falsos criados pelas ferramentas de geração, num ciclo contínuo de aprimoramento. Medidas preventivas essenciais incluem a tokenização de conteúdo, autenticação biométrica com verificação de *liveness*², monitoramento de anomalias comportamentais e verificações multifatoriais para transações de alto risco. O treinamento de funcionários e o uso da IA e da Aprendizagem de Máquina são destacados como fatores cruciais para reduzir os custos médios de violação de dados (CROWDSTRIKE, 2025).
- **Capacitação e Ferramentas:** A capacitação de agentes públicos no rastreamento de ativos virtuais e combate à lavagem de dinheiro, como o Programa Nacional de Capacitação e Treinamento para a Recuperação de Ativos do Ministério da Justiça e Segurança Públi-

² Liveness: Verificação automatizada analisando se a amostra biométrica (como rosto, impressão digital ou voz) provém de uma pessoa viva (CHAINALYSIS, 2025).

ca (2025), é fundamental. O desenvolvimento de sistemas de alerta precoce e a desarticulação de infraestruturas criminosas que experimentam com IA são prioritários para a atuação das autoridades de segurança (CHAINALYSIS, 2025a).

- **Cooperação Internacional:** Dada a natureza transnacional das fraudes, a cooperação multilateral é imperativa. Mecanismos como o INTERPOL Global Rapid Intervention of Payments (I-GRIP) e o Egmont BEC Project Team permitem o compartilhamento rápido de informações e a intervenção para recuperação de ativos (FATF, 2023).
- **Educação e Conscientização:** A educação e a conscientização são fundamentais para tornar os usuários on-line menos propensos à manipulação. Fortalecer a alfabetização midiática e em IA para crianças, pais e educadores é uma necessidade crescente. Para Negreiro (2025), o ensino de pensamento adversarial e o reconhecimento de sinais de deepfake (movimento de olhos, boca, iluminação, qualidade de voz) são medidas práticas recomendadas.
- **Pesquisas Futuras e Implicações Práticas:**
 - **Aprofundamento na Aplicação Jurisprudencial:** Monitorar a aplicação prática do Art. 171-A do Código Penal pelos tribunais brasileiros para verificar sua efetividade e eventuais controvérsias subsidiará diretrizes para promotores, juízes e policiais, otimizando a aplicação da nova lei e garantindo consistência decisória.
 - **Estudos Empíricos sobre Impacto Social:** Investigar os impactos psicossociais e de saúde mental de deepfakes em vítimas, especialmente crianças e adolescentes, e a eficácia de intervenções de apoio e prevenção, direcionará políticas públicas de saúde mental e bem-estar digital, capacitando profissionais da saúde e educação para identificação e intervenção precoce.
 - **Desenvolvimento de Ferramentas de Detecção Adaptativas:** Estimular pesquisas interdisciplinares entre direito, ciência da computação e psicologia para desenvolver algoritmos de detecção de deepfakes e criptofraudes mais adaptativos e resilientes

às táticas criminosas, resultará em soluções tecnológicas de ponta que podem ser integradas em plataformas digitais e sistemas bancários, fortalecendo a capacidade de identificação e neutralização em tempo real.

- **Análise da Geodistribuição e Sentimento do Investidor:** Mapear a distribuição regional das vítimas de criptofraudes e a correlação com o sentimento dos investidores permitirá às autoridades direcionar recursos e operações policiais de forma mais eficiente para as áreas de maior incidência, e auxiliará reguladores e empresas na criação de campanhas de conscientização personalizadas.
- **Avaliação de Programas Educacionais:** Mensurar a eficácia de programas de alfabetização em IA e mídia digital na capacidade dos usuários de identificar e se proteger contra deepfakes e criptofraudes fornecerá dados para otimizar e expandir iniciativas de letramento digital e educação pública, tornando os cidadãos mais resilientes a manipulações online.
- **Estudo de Mecanismos Descentralizados:** Investigar o uso de redes sociais e de confiança informal por golpistas em esquemas como *rug pulls* e *pig butchering* capacitará plataformas de redes sociais e provedores de serviços on-line a desenvolver políticas de moderação de conteúdo mais eficazes e mecanismos de alerta preditivo contra esquemas que exploram a confiança humana.

CONCLUSÃO

A presente investigação evidenciou que deepfakes e criptofraudes configuram ameaças emergentes de elevada complexidade e impacto substancial, tanto global quanto nacional, amplificadas pela inteligência artificial e sua capacidade de facilitar golpes sofisticados e escaláveis.

O ecossistema de criptoativos, intrinsecamente descentralizado e pseudônimo, revela-se particularmente vulnerável a modalidades fraudulentas como *pig butchering*, *rug pulls* e fraudes de identidade e investimento.

No contexto brasileiro, a crescente incidência de deepfakes em fraudes bancárias e esquemas de lavagem de dinheiro via criptoativos, como demonstrado em diversas operações policiais, reforça a urgência de uma abordagem sistemática para enfrentar essas ameaças.

A promulgação da Lei nº 14.478/2022 representa um marco significativo na regulação do mercado de ativos virtuais no Brasil e no fortalecimento do aparato jurídico contra criptofraudes.

Ao incorporar definições centrais, equiparar provedores de serviços de ativos virtuais (PSAVs) a instituições financeiras sob a ótica penal, introduzir o tipo penal de fraude contra o Sistema Financeiro Nacional (Art. 171-A do Código Penal) e aprimorar mecanismos de prevenção à lavagem de dinheiro, a lei estabelece um arcabouço jurídico mais robusto, apto a viabilizar segurança jurídica e eficácia institucional.

Entretanto, o enfrentamento dessas ameaças exige uma abordagem multifacetada e contínua. A velocidade de inovação nos métodos ilícitos, aliada às barreiras impostas pelo pseudoanonimato e descentralização, impõe a necessidade de constante evolução normativa infralegal, aplicação de tecnologias avançadas de detecção com IA, articulação integrada entre órgãos de segurança pública, estabelecimento de parcerias público-privadas e investimento substancial em educação e letramento digital.

A escassez de habilidades em cibersegurança e o elevado custo das violações de dados reforçam a urgência de investimentos em segurança e capacitação.

Este artigo contribui significativamente aos estudos de Direito Penal e Segurança Cibernética ao: (i) sistematizar e integrar dados contemporâneos sobre deepfakes e criptofraudes, oferecendo uma visão atualizada do panorama; (ii) realizar uma análise crítico-jurídica da Lei nº 14.478/2022, destacando seus avanços e desafios; (iii) apresentar casos concretos de operações ilícitas e respostas institucionais no Brasil, enriquecendo o debate com evidência empírica nacional; e (iv) consolidar a compreensão da fundamentação jurídica do Art. 171-A do Código Penal como crime federal contra o SFN, com competência federal e ação penal pública incondicionada.

Reconhecem-se, contudo, limitações inerentes à alta volatilidade das tecnologias e práticas criminosas, que podem tornar esta análise um recorte temporal. A escassez de dados públicos detalhados sobre perdas financeiras

transnacionais e a dependência de análise manual na verificação de deepfakes representam obstáculos a estudos quantitativos aprofundados.

Para avanços futuros, recomenda-se o monitoramento jurisprudencial do Art. 171-A, estudos psicossociais sobre os impactos em vítimas, o desenvolvimento tecnológico adaptativo de ferramentas de detecção, mapeamentos geográficos e comportamentais, avaliação de programas educacionais e investigações sobre mecanismos *off-chain* empregados por golpistas.

Ao aprofundar essas vertentes, pesquisas futuras poderão ampliar a compreensão e eficiência da resposta jurídica e institucional, contribuindo para a mitigação eficaz de uma das ameaças mais relevantes da era digital.

REFERÊNCIAS

ARAS, Vladimir. Marco regulatório da criptoeconomia e sua repercussão no campo penal. **Revista do Ministério Público do Estado do Rio de Janeiro**. Rio de Janeiro, n. 88, p. 268–298, abr.–jun. 2023.

BANK, D.; KOENIGSTEIN, N.; GIRYES, R. Autoencoders. **arXiv**, 12 mar. 2020. Disponível em: <https://arxiv.org/abs/2003.05991>. Acesso em: 17 jul. 2025.

BITGET. **Bitget Research**: Deepfakes may reach 70% of crypto crimes in two years. Victoria, Seychelles: Bitget Blog, 26 jun. 2024. Disponível em: <https://www.bitget.com/blog/articles/bitget-research-deepfake-report-2024>>. Acesso em: 15 jul. 2025.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/L9613compilado.htm>. Acesso em: 17 jul. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 17 jul. 2025.

BRASIL. **Lei nº 14.478, de 21 de dezembro de 2022**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais. Diário Oficial da União, Brasília, DF, 21 dez. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14478.htm>. Acesso em: 15 jul. 2025.

BRASIL. **Projeto de Lei nº 2338, de 2023**: dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Senado Federal; Câmara dos Deputados, 17 mar. 2025. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262>>. Acesso em: 15 jul. 2025.

BRASIL. **Lei nº 15.123, de 24 de abril de 2025.** Altera o art. 147-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena para crimes praticados com o uso de inteligência artificial. Diário Oficial da União, Brasília, DF, 25 abr. 2025. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15123.htm>. Acesso em: 15 jul. 2025.

CHAINALYSIS. **AI-powered crypto scams: How artificial intelligence is being used for fraud.** Nova York: Chainalysis, 28 maio 2025a. Disponível em: <<https://www.chainalysis.com/blog/ai-artificial-intelligence-powered-crypto-scams/>>. Acesso em: 15 jul. 2025.

CHAINALYSIS, Inc. **The 2025 Crypto Crime Report.** [S.l.], 2025b. Disponível em: <<https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf>>. Acesso em: 15 jul. 2025.

CROWDSTRIKE, Inc. **CrowdStrike 2025 Global Threat Report.** Austin, Texas: CrowdStrike, 2025. Disponível em: <<https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf>>. Acesso em: 15 jul. 2025.

DOWBOR, Ladislav. O desafio da revolução digital. In: CAMPILONGO, Celso Fernandes; GONZAGA, Álvaro de Azevedo; FREIRE, André Luiz (coords.). **Enciclopédia Jurídica da PUC-SP.** Tomo: Direito Econômico. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

ELLIPTIC. **AI-enabled crypto crime: Emerging risks and best practices for law enforcement agencies.** Londres: Elliptic, 2025a. Disponível em: <<https://www.elliptic.co/blog/ai-enabled-crypto-crime-emerging-risks-and-best-practices-for-law-enforcement-agencies>>. Acesso em: 15 jul. 2025.

ELLIPTIC. **The State of Crypto Scams 2025: Keeping our industry safe with blockchain analytics.** Elliptic, 13 jun. 2025b. Disponível em: <<https://www.elliptic.co/blog/the-state-of-crypto-scams-2025-keeping-our-industry-safe-with-blockchain-analytics>>. Acesso em: 15 jul. 2025.

ELLIPTIC. **What is... a scam?** Elliptic, 23 ago. 2024. Disponível em: <<https://www.elliptic.co/blockchain-basics/what-is-a-scam>>. Acesso em: 15 jul. 2025.

EUROPOL. **EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025:** The changing DNA of serious and organised crime. Haia: Europol, 2025. Disponível em: <<https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>>. Acesso em: 15 jul. 2025.

FINANCIAL ACTION TASK FORCE (FATF); INTERPOL; EGOMONT GROUP OF FINANCIAL INTELLIGENCE UNITS. **Illicit Financial Flows from Cyber-Enabled Fraud.** Paris: FATF, nov. 2023.

FORBES BRASIL. **Após golpe com Marcos Mion, deepfakes entram na mira da Justiça brasileira.** Forbes Brasil, 17 jan. 2025. Disponível em: <<https://forbes.com.br/forbes-tech/2025/01/apos-golpe-com-marcos-mion-deepfakes-entram-na-mira-d-a-justica-brasileira/>>. Acesso em: 15 jul. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública:** 2024. São Paulo: Fórum Brasileiro de Segurança Pública, 2024.

GOVERNO DE ALAGOAS. **Polícia Civil deflagra operação para coibir manipulação de imagens pornográficas em Maceió e região metropolitana.** Governo de Alagoas, 15 jan. 2025. Disponível em: <<https://alagoas.al.gov.br/noticia/policia-civil-deflagra-operacao-para-coibir-manipulacao-de-imagens-pornograficas-em-maceio-e-regiao-metropolitana>>. Acesso em: 15 jul. 2025.

IBM. **Cost of a Data Breach Report 2024.** [S.l.], 2024. Disponível em: <<https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>>. Acesso em: 15 jul. 2025.

KASPERSKY. **Dark Web Threats Landscape – DFI Expert Report**. [S.l.], 2025. Disponível em: <<https://content.kaspersky-labs.com/se/media/br/enterprise-security/dark-web-threats-landscape-dfi-expert-report.pdf>>. Acesso em: 15 jul. 2025.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Capacitação do MJSP aborda os riscos dos criptoativos para a corrupção e a lavagem de dinheiro**. MJSP, 4 jun. 2025. Disponível em: <<https://www.gov.br/mj/pt-br/assuntos/noticias/capacitacao-do-mjsp-aborda-os-riscos-dos-criptoativos-para-a-corrupcao-e-a-lavagem-de-dinheiro>>. Acesso em: 15 jul. 2025.

NEGREIRO, M. Children and deepfakes. **Briefing EPRS – European Parliamentary Research Service**, n. 775.855, julho 2025. Disponível em: <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf)>. Acesso em: 15 jul. 2025.

PAPASAVVA, Antonis; JOHNSON, Shane; LOWTHER, Ed; LUNDRIGAN, Samantha; MARICONTI, Enrico; MARKOVSKA, Anna; TUPTUK, Nilufer. **Application of AI-based Models for Online Fraud Detection and Analysis**. *Crime Science Journal*, 2025. Disponível em: <<https://arxiv.org/pdf/2409.19022v2>>. Acesso em: 15 jul. 2025.

POLÍCIA FEDERAL. **Foragido internacional ligado à Operação Kryptos é preso nos EUA**. Polícia Federal, 4 mar. 2025a. Disponível em: <<https://www.gov.br/pf/pt-br/assuntos/noticias/2025/03/foragido-internacional-ligado-a-operacao-krypto-s-e-preso-nos-eua>>. Acesso em: 15 jul. 2025.

SILVA, João da; PEREIRA, Maria de Souza. Aspectos criminais da Lei 14.478/2022. **Boletim do IBCCRIM**, São Paulo, v. 1993, n. 34, p. 123-145, jul. 2025.

SUMSUB. **Identity Fraud Report 2024**. London: Sumsb, jan. 2025. Disponível em: <https://sumsub.com/files/sumsub_identity_fraud_report_2024.pdf>. Acesso em: 16 jul. 2025.

WU, Hao; WANG, Haijun; LI, Shangwang; WU, Yin; FAN, Ming; JIN, Wuxia; LIU, Ting. **RPHunter: Unveiling Rug Pull Schemes in Crypto Token via Code-and-Transaction Fusion Analysis**. arXiv, 13 jun. 2025. Disponível em: <<https://arxiv.org/pdf/2506.18398v3>>. Acesso em: 15 jul. 2025.

SOBRE OS ORGANIZADORES

Marília Rulli Stefanini

Pós-doutorada e estágio pós-doutoral em Direitos Humanos e Democracia pelo "Ius Gentium Conimbrigae" (IGC) na Faculdade de Direito, Universidade de Coimbra (FD-UC), Portugal (2021-2022), sob a supervisão do Professor Doutor Efetivo Rui Cunha Martins. Doutora em Direito pela PUC-SP (2017- 2021). Mestra em Direito pelo programa de Mestrado ofertado pelo Centro Universitário Eurípides Soares da Rocha - UNIVEM - Marília-SP (2014-2015), com área de concentração em Teoria do Direito e do Estado. Especialista em Educação, com área de concentração em Docência para o Ensino Superior, na Universidade Estadual de Mato Grosso do Sul - UEMS, Unidade Universitária de Paranaíba-MS (2009). Especialista, também, em Direito do Estado (2011) e Direito e Processo do Trabalho (2011) pela Rede de Ensino ANHANGUERA - UNIDERP. Possui graduação em Direito pela Universidade Estadual de Mato Grosso do Sul-UEMS - Unidade Universitária de Paranaíba - MS (2007); Graduada em Pedagogia pela FAR - Faculdades Reunida.

Lattes: <http://lattes.cnpq.br/2076890399249480>

Ernane Rosa Martins

Pós-Doutorado em E-learning pela Universidade Fernando Pessoa (UFP). Doutor em Ciência da Informação com ênfase em Sistemas, Tecnologias e Gestão da Informação, na Universidade Fernando Pessoa (UFP), em Porto/Portugal, reconhecido como equivalente ao curso de Doutorado em Ciência da Informação, da UnB. Mestre em Engenharia de Produção e Sistemas pela UCG, possui Pós-Graduação em Tecnologia em Gestão da Informação, Graduação em Ciência da Computação e Graduação em Sistemas de Informação. Professor de Informática, com dedicação exclusiva, do Instituto Federal de Educação, Ciência e Tecnologia de Goiás - IFG (Câmpus Luziânia), ministrando disciplinas nas áreas de Engenharia de Software, Desenvolvimento de Sistemas, Linguagens de Programação, Banco de Dados e Gestão em Tecnologia da Informação. Pesquisador líder do grupo de pesquisa NITE (Núcleo de Inovação, Tecnologia e Educação), certificado pelo IFG no CNPq.

Lattes: <http://lattes.cnpq.br/5566965064833628>

ÍNDICE REMISSIVO

A

Alfabetização: 12, 46, 48, 50, 51, 52, 53, 57

Algoritmo: 9, 13, 14, 15, 16, 18, 19

Auditoria Jurídica: 29, 33

B

Bases Legais: 28, 29, 35, 36, 43

C

Cidadania: 21, 46, 54, 55, 57, 58, 59, 60

D

Digital: 10, 11, 12, 17, 18, 21, 22, 23, 24, 25, 26, 40, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 67, 70, 73

Direitos Humanos: 46, 47, 51, 52, 54, 56, 57, 59, 60, 66, 67, 74

E

Ética: 8, 9, 10, 16, 17, 20, 21, 23, 24, 25

F

Fusões e Aquisições: 29, 30, 31, 44

L

LGPD: 20, 25, 29, 32, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 64, 65, 69, 70, 71, 72, 73, 74

P

Poder Judiciário: 65, 67, 68, 70, 72, 73, 74

Proteção de Dados Pessoais: 9, 20, 25, 29, 34, 35, 38, 39, 40, 44, 65, 66, 70, 73, 74

R

Responsabilidade do Estado: 65

Risco Sistêmico: 65

S

Sociedade: 8, 9, 10, 12, 17, 18, 19, 21, 22, 23, 24, 25, 30, 31, 32, 33, 37, 47, 51, 52, 68, 74

T

Tecnologia: 9, 10, 11, 12, 13, 14, 19, 22, 23, 24, 25, 26, 35, 46, 47, 48, 49, 50, 52, 53, 54, 56, 60, 70, 71, 74

Tecnologia: 9, 10, 11, 12, 13, 14, 19, 22, 23, 24, 25,

26, 35, 46, 47, 48, 49, 50, 52, 53, 54, 56, 60, 70, 71, 74

Tratamento de Dados Pessoais: 28, 29, 34, 35, 36, 38, 39, 41, 42, 43, 70, 74



científica digital



VENDA PROIBIDA - ACESSO LIVRE - OPEN ACCESS



www.cientificadigital.org | contato@cientificadigital.org