

MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 20 | NUMBER 1 | SUMMER 2026 | ISSN 1802-5943

PEER REVIEWED



CONTENTS:

EHIRIM | RASHICA | WITTLIN | MIKE | KRAVCHENKO | HOFFMANN |
JACKSON | KATANA

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology

issued by Institute of Law and Technology

Faculty of Law, Masaryk University

www.mu.jlt.law.muni.cz

Editor-in-Chief

Jakub Harašta, Masaryk University, Brno

Deputy Editor-in-Chief

Ondřej Böhm, Masaryk University, Brno

Founding Editor

Radim Polčák, Masaryk University, Brno

Editorial Board

Tomáš Abelovský, Swiss Re, Zurich

Zsolt Balogh, Corvinus University, Budapest

Michael Bogdan, University of Lund

Joseph A. Cannataci, University of Malta | University of Groningen

Josef Donát, ROWAN LEGAL, Prague

Julia Hörnle, Queen Mary University of London

Josef Kotásek, Masaryk University, Brno

Leonhard Reis, University of Vienna

Naděžda Rozehnalová, Masaryk University, Brno

Vladimír Smejkal, Brno University of Technology

Martin Škop, Masaryk University, Brno

Dan Jerker B. Svantesson, Bond University, Gold Coast

Markéta Trimble, UNLV William S. Boyd School of Law

Andreas Wiebe, Georg-August-Universität Göttingen

Aleš Završnik, University of Ljubljana

Editors

Tina Mizerová, Andrej Krištofik

Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o. (<https://rowan.legal>)

Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions

Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

listed in HeinOnline (www.heinonline.org)

listed in Scopus (www.scopus.com)

reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME 20 | NUMBER 1 | SUMMER 2026

LIST OF ARTICLES

Ugochukwu Godspower Ehirim: Regulating the Emerging Mobile Money Services and National Digital Currencies in Nigeria and South-Africa.....3

Viona Rashica: The Evolution of Digital Diplomacy: The Impact of Technological Advancements on Diplomatic Practice.....33

Jan Wittlin: Legal and Regulatory Compliance Challenges for Equity Token Secondary Market Operators in the European Union.....59

Nimrod Mike: Another View on Article 22 GDPR: The Future of Automated Decision-Making.....87

Yuliia Kravchenko, Thomas Hoffmann, Eric Blake Jackson: Embedding a Harmonised EU Identity System into a Mature National E-State: An Estonian Case Study.....119

LIST OF BOOK REVIEWS

Katarzyna Katana: Overcoming Technology’s Myths – A Review of Law and Technology: A Methodical Approach.....145

DOI 10.5817/MUJLT2026-40380

REGULATING THE EMERGING MOBILE MONEY SERVICES AND NATIONAL DIGITAL CURRENCIES IN NIGERIA AND SOUTH-AFRICA

by

UGOCHUKWU GODSPOWER EHIRIM *

The evolution of digital financial platforms and other species of 'internet banking', has enabled new opportunities for greater participation of people, particularly the masses, in the official payment arrangements in Nigeria and South Africa. Smart-technology-enabled- financial market has resulted in financial inclusivity by affording the poor the leverage to transact in the money market and sundry economic activities previously seen as a preserve of the elite. The emergence of internet financial solutions constitutes part of an amazing circle in the evolving financial technology (fintech) which has birthed the recognition of digital currencies in most countries. This paper adopts the doctrinal method of legal research in evaluating the attempts to bureaucratically govern internet financial platforms and their products by legislation and regulatory mechanisms in Nigeria, South Africa and other African countries like Zimbabwe, particularly the proposed introduction of National (Central Bank) Digital Currencies. Leveraging the African Union (AU)'s economic blueprint of promoting trade synergy amongst member states, also known as Agenda 2063. This paper advocates for synergy while making a case for a robust statutory framework to sustain fintech operations in Nigeria and South Africa, which in turn would drive the African regional economic integration through the evolving cashless policy design.

KEY WORDS

Banking, Digital Currencies, Financial Technology, Mobile Money, Regulation

* Ugochukwu Godspower Ehirim, Ph. D.; Delta State University, Department of Private Law, Oleh Campus, Nigeria; E-mail: attorneyugo@gmail.com; ORCID: 0009-0001-0540-4907

1. INTRODUCTION

The exponential patronage for internet-powered financial services has afforded opportunities for the mass of unbanked population, particularly the low-income earners, to have access to financial services in most countries of the global south, including Nigeria and the Republic of South Africa.¹ In Nigeria, a large number of the poor, particularly those who live outside the frontline cities have no convenient and suitable access to useful and workable financial services. The digital revolution is sweeping through every facet of the economy,² and particularly the banking sector resulting in enhanced inclusion of earners of low-income hitherto excluded from the banking index into the banking net.³ Consequently, the traditionally unbanked population has been enabled to take advantage of internet financial services like mobile money to benefit from convenient, affordable and purposeful financial products.⁴ These services are so designated as digital financial services because they are generally routed through mobile phones, powered by internet. Some of the services are adaptable to the extent that connection to the internet may not be fundamental in respect of when to send, receive or conduct money transactions. To this end, digital financial services have introduced a twist in who, how and when to participate in financial markets, the *modus operandi* of financial organisations as well as the overall operationality of money business in South Africa and Nigeria. The proliferation of mobile money platforms demonstrates the capacity of artificial intelligence and tools of financial technology (fintech) to recalibrate the financial markets in Nigeria and South Africa.⁵

Mobile money and other fintech platforms are assisting businesses to grow beyond subsistence level, making such business owners capable of

¹ Guild, J. (2017) Fintech and the Future of Finance. *Asian Journal of Public Affairs*, pp. 3-4.

² Ehirim, U. G. (2025) Artificial Intelligence and Healthcare Delivery in Nigeria: Legal and Ethical Dimensions of Patients' Rights to Safety. *The Indonesian Journal of Sharia and Socio-Legal Studies*, 1 (1), pp. 47-71. See also, Ehirim, U. G. (2025) Ethical Legal Practice and the Integration of AI into Legal Profession: Striking the Balance. *Open Journal for Legal Studies (OJLS)*, 8 (1), pp. 13-34. Available from: <https://doi.org/10.32591/coas.ojls.0801.02013e> [Accessed 3 August 2025]

³ Tapainainen, T. (2020) Toward Fintech Adoption Framework for Developing Countries - A Literature Review Based on the Stakeholder Perspective. *Journal of Information Technology Applications & Management*, pp. 2-3.

⁴ Mobile money is the most common nomenclature for digital financial products. See, Prasad, E. (2021) *The Future of Money: How the Digital Revolution is Transforming Currencies and Finance*. Belknap Press: Harvard University Press, pp. 1-2.

⁵ Okoye, N. J. et al. (2024) Financial Technology (Fintech) and the Performance of Firms in Nigeria. *International Journal of Social Science, Technology and Economics Management*, 2 (1). Available from: <https://doi.org/10.59781/1524NEOM> [Accessed 16 February 2025]. See also, Oturu, D. (2024) *Fintech Law and Practice in Nigeria*, Aberdeen: Davidson Oturu, pp. 3-5.

meeting their financial needs and remaining afloat in business. The visible financial assess provided by the fintech solutions were hitherto impossible with structured, institutional banking.⁶ Guild posits that digital financial products fortified communities' stoicism to economic shocks during the COVID-19 global lockdown.⁷ Internet financial services is internet-driven and so advances and improves with technological advancements.⁸ For instance, it is a lot easier, faster and cheaper to access fintech products with 5G enabled mobile devices than 3G.⁹ The requirements for valid transactions contrast with institutional bank requirements for validation of the minutest transactions. Banks may demand customers' residential and employment addresses, utility bills, proofs of income, purposes of transaction, customers' identifying documents, verifiable relationships with cash recipients, and other onerous conditionalities such as the provisions of BVN.¹⁰ Most of these unnecessary demands dwindle customers' preferences for institutional financial service providers in Nigeria and other countries with entrenched institutional banking infrastructure, like South Africa.¹¹ The patronage that the evolving fintech has recorded demonstrates an existential threat to regular financial institutions which currently may have to play the catch-up to remain globally relevant in business.

This paper evaluates the legal regime of digital financial services with a view to ascertaining the adequacy of regulatory frameworks that would boost nations' economy while reducing incidents of criminality. The paper focuses on the benefits of using internet financial services or the implementation of well-regulated electronic currencies to enhance financial inclusivity of the low-income earners and unbanked community in Nigeria and South Africa.¹² It addresses the efficacy of the extant statutory regulatory infrastructure of the

⁶ Trautman, L. J. (2016) Is Disruptive Blockchain Technology the Future of Financial Services? *The Consumer Finance Law Quarterly Report*, pp. 233-234.

⁷ Guild, J. (2017), *op. cit.* pp. 3-4.

⁸ Zetzsche, D. A., Buckley, R. P. and Amer, D. W. (2019) Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses. *University of New South Wales Research Series*, pp. 11-12.

⁹ Alexandru, T. and Tabusca, S. (2019) Impact of 5G Technologies in Global Economy, Cybersecurity and Legal Issues. *Journal of Information Systems & Operations Management*, pp. 177-189.

¹⁰ Biometric (Bank) Verification Number. This is a mandatory requirement to hold and operate a bank account in Nigeria.

¹¹ Chitimira, H. and E. Torerai, E. (2021) The Nexus between Mobile Money Regulation, Innovative Technology and The Promotion of Financial Inclusion in Zimbabwe. *Potchefstroom Electronic Law Journal*, p. 21. See also Tamburi, M. Y. (Jnr.) and Kong, Y. (2019) Digitizing Payments: Opportunities for Financial Inclusion for Sub-Saharan Africa. *Case Studies Journal*, pp. 21-22.

¹² Torerai, E. (2022) *A Comparative Statutory Analysis on the Use and Regulation of Mobile Money to Promote Financial Inclusion for the Poor in Zimbabwe*. LLD Thesis: North West University, South Africa, pp. 3-4.

relevant financial sector in Nigeria and South Africa in respect of transactions in electronic monetary services and the recognition of electronic monies to engender an all-inclusive financial engagement of the poor and vulnerable who are largely unbanked, particularly in the local communities and informal settlements in both South Africa and Nigeria. India has through the monetary policies of its national bank, that is, the Reserve Bank of India engaged initiatives to transit to financially inclusive economy.¹³

This conceptual paper is divided into three broad parts for ease of appreciation. The first part is the foregoing introduction which sets the tempo for the discourse. This is followed by the research methodology under which heading the method adopted in the research and analysis of data is highlighted. The second part discusses the result and analyses the outcome of data used in the research eventually leading into the conclusion, which is the third and final part of the paper. Recommendations are made following the foregoing analysis of data and findings in this concluding part.

1.1.MATERIALS AND METHODS

The doctrinal methodology of legal writing is engaged in this paper for effective comparative evaluation of fintech regulatory regimes in Nigeria and South Africa. A rigorous library analysis and examination of the statutory and policy directives as well as other literatures bearing relevance to the administration of internet financial services in Nigeria and South Africa are made.¹⁴ The analysis carried out is focused on digital financial products, particularly the mooted recognition by the central bank of digital currencies in the focus countries. Simply put, the paper focuses on mobile money services operated by mobile network operators (MNO). Consequently, electronic financial products like crypto assets and bitcoins are not within the scope of the paper.

¹³ Agrawal, R. (2019) Review of Initiatives taken by the Government and banking regulator for successful transition to a financially inclusive economy: an empirical study of India. *Economic Analysis*, 52 (1) pp. 81-96.

¹⁴ Gasiokwu, M. O. U. (2015) *Legal Research and Methodology: The A – Z of Writing Theses and Dissertations in a Nutshell*. Chenglo Limited, pp. 14 – 16.

2. RESULT AND DISCUSSION

2.1. CAUTIONARY APPROACH: ATTEMPTS AT THE REGULATION OF DIGITAL FINANCIAL SERVICES

Notwithstanding the positive potentials of internet-powered financial services, the phenomenon poses practical challenges to regulators of financial markets and pilots of sovereign economies of the countries of the Global South such as South Africa and Nigeria. The nature of fintech transactions pose great difficulty to law enforcement because of the complex nature of tracking electronic currencies. The arrangement presents a bold front for money laundering and associated financial offences.¹⁵ Money laundering has undermined so many economies of the Global South, particularly those with corrupt leadership. Money laundering activity constitutes serious financial crime in Nigeria and goes to the root of anti-corruption crusade that birthed specialised crime bursting agencies and approaches in Nigeria.¹⁶ As a result, obsolete statutes such as the Nigeria Police Act were re-calibrated to align with the dynamics of criminality that constitutes the realities of the digital era.¹⁷ Halliday et al. conceive money laundering as an arrangement deployed by criminals to transform illicitly acquired money, profit or benefits into legitimate money, profit and gains in such a way as to make it difficult to be identified as proceeds of criminal or unlawful transactions.¹⁸ Within the electronic money market space, there are no geographical boundaries accentuating economic bureaucratic governance. The intricate features of illicit money flow situate money laundering within the comity of organised crimes as it sometimes involves third party professionals like accountants, lawyers, bankers, *bureau de change* operators and persons holding political offices.¹⁹ This level of collaboration in perfecting money laundering activities

¹⁵ Winn, J. K. and De Koker, L. (2013) Introduction to Mobile Money in Developing Countries' Financial Inclusion and Integrity Conference Special Issue. *Washington Journal of Law, Technology & Arts*, pp. 156-157. See also Weihuan, Z., Arner, D. W. and Buckley, R. P. (2015) Regulation of Digital Financial Services in China: Last Mover Advantage? *Tsinghua China Law Review*, pp. 25-62.

¹⁶ See Ahiauzu, N. and Inko-Tariah, T. (2016) Applicability of Anti-money Laundering Laws to Legal Practitioners in Nigeria: NBA V FGN & CBN. *Journal of Money Control*, p. 329. See also, *The Economic and Financial Crimes Commission (EFCC) Establishment Act 2004* (s. 6 & 7). Nigeria. In: English.

¹⁷ Ehirim, U. G. et al. (2024) Strengthening Human Rights Protection in Nigeria: Safeguards Under the Police Act 2020. *Khazanah Hukum*, 6 (3), pp. 269-293.

¹⁸ Halliday, T., Levi, M. and Reuter, P. (2019) Anti-Money Laundering: An Inquiry into a Disciplinary Transnational Legal Order. *UC Irvine Journal of International, Transnational and Comparative Law*, 4 (3), pp. 1-25.

¹⁹ Chitimira, H. and Munedzi, S. (2021) Selected Challenges Associated with the Reliance on Customer Due Diligence Measures to Curb Money Laundering in South African Banks and Related Financial Institutions. *Journal of Comparative Law in Africa*, pp. 44 – 46.

lends credence to the agitation for stringent statutory administration of electronic financial activities in Nigeria and South Africa.

However, the extant regulatory frameworks in the finance sectors of the Nigerian and South African economies have not adequately regulated electronic financial transactions. There is no specific statute governing fintech transactions, particularly crypto assets in these two countries. Consequently, legislators and regulators are encouraged to consider regulating fintech products in order to bring digital finance promoters within the state surveillance net for the purpose of ensuring a crime-free money-market space. Zimbabwe, for instance has statutes like the National Payments Systems Act,²⁰ the Exchange Control Act,²¹ the Banking Act,²² the Money Laundering and Proceeds of Crime Act.²³ and the Banking (Money Transmission, Mobile Banking and Mobile Money Interoperability) Regulations 2020,²⁴ which provide visible bureaucratic vigilance on some aspects of fintech transactions. The South African government has evolved remarkable statutory frameworks such as the National Payment System Act,²⁵ the Prevention of Organised Crime Act,²⁶ the Financial Sector Regulation Act²⁷ and the Financial Intelligence Centre Act.²⁸ Nigeria has similar laws.²⁹ These statutes which primarily bear on institutional banking include the Banks and other Financial Institution Act (BOFIA), The Central Bank Nigeria Act (CBNA) 2007, the Nigeria Deposit Insurance Corporation (NDIC) Act 2004 among others.³⁰ The CBN's New Corporate Governance Guidelines effective from 13 July 2023; the Reviewed IMTO Guidelines³¹ and sundry regulations are extensive enough to impact all financial sector including the digital financial services.³² However, these laws are inadequate

²⁰ See *The National Payments Systems Act 2001*, (s. 2 & 3). Zimbabwe.

²¹ *Exchange Control Act 1965*, (c. 22: 05), (s. 2). Zimbabwe.

²² *The Banking Act 1999*, (s. 2, 4, 6 & 7). Zimbabwe.

²³ *The Money Laundering and Proceeds of Crime Act 2013*, (c. 9:24), (s. 12a – 12d). Zimbabwe.

²⁴ *The Banking Regulations 2020*, (s. 2 & 3). Zimbabwe.

²⁵ *The National Payment Systems Act 78 of 1998*, (s. 2). South Africa [SA].

²⁶ *The Prevention of Organised Crime Act 121 of 1998*, (s. 48). (POCA) SA.

²⁷ *The Financial Sector Regulation Act No. 9 of 2017*, (c. 57: B & 58). SA.

²⁸ *The Financial Intelligence Centre Act 38 of 2001*, (c. 20: A – 21:H) (FICA). SA.

²⁹ See Akujobi, N. E., Anyanwu, G. I. and Eke, C. K. (2021) Regulatory Framework and Bank Operations in Nigeria: A VECM Approach. *International Journal of Development and Management Review*, 16 (1), pp. 148-160.

³⁰ Others include *Companies and Allied Matters Act (CAMA) 2020*. Nigeria. In: English.; *The Foreign Exchange (Monitoring and Miscellaneous Provisions) Act 1995*. Nigeria. In: English.

³¹ *The Reviewed Guidelines on International Money Transfer Services in Nigeria 2024 (the IMTO Guidelines)*, SI. Nigeria.

³² See Aidonojie, P. A., Majekudunmi, T. A. and Adeyemi-Balogun, O. J. (2023) The Legal Issues Concerning the Operations of Fin-Tech in Nigeria. *Jurnal Media Hukum*, 30 (2), p. 82.

to guarantee formidable legal regime for fintech products, including mobile money.

The evolution of mobile banking and its associated financial services align with four major theoretical economic models which explain its extensive acceptability within the economic matrix of Nigeria and South Africa. These models are the Decomposed Theory of Planned Behaviour (DTPB), Technology Acceptance Model (TAM), Theory of Planned Behaviour (TPB), and the Unified Theory of Acceptance and Use of Technology (UTAUT). Giovanis et al. posit that the DTPB model best explains the entrenchment of mobile banking around the globe since it encapsulates the perceived risk (PR) as well as integrates the three rationally evaluated features of easiness, usefulness and compatibility.³³ The foregoing position becomes imperative as the TAM is limited in application given that it incorporates the twin attributes of perceived usefulness (PU) and perceived ease of use (PEOU) to the exclusion of external fundamentals underlining consumers behaviour.³⁴ However, Badiang and Nkwei suggest that the UTAUT model is credited for the wide acceptability of mobile device-based technology in banking operations in South Africa.³⁵ The UTAUT more than any other model embraces African values of status peddling by leveraging on its inherent indices of performance expectancy, effort expectancy, social influence, and facilitating conditions to enhance its popularity as a befitting model for mobile banking in Nigeria and South Africa. Whichever theory prevails, it is posited that in all considerations for the institution and sustenance of electronic banking in Africa, the utilitarian legal theory stands out. The theory explains why the black community in South Africa, for security reasons, offers more patronage to the mobile banking concept whereas the long queues and hours spent on marginal transactions in Nigerian banks endears electronic banking to the average Nigerian. Nigerian consumers are more influenced by the ease of doing business and local consumer cultures even when the infrastructure required to facilitate such culture, such as internet facility, is at the nursery stage. The application of utilitarian theory to e-banking reflects in the security, trust, risk-management and

³³ Giovanis, A et al. (2019) Adoption of Mobile Banking Services: A Comparative Analysis of Four Competing Theoretical Models. *International Journal of Bank Marketing*, 37 (5), pp. 116-1189. Available from: <https://doi.org/10.1108/IJBM-08-2018-0200>

³⁴ Asongu, S. A. and Odhiambo, N. M. (2020) Inequality and Gender Economic Inclusion: The Moderating Role of Financial Access in Sub-Saharan Africa. *Economic Analysis and Policy*.

³⁵ Badiang, A. M. and Nkwei, E. S. (2024) Mobile Banking Adoption, Its Antecedents and Post-Adoption Effects: The Role of Consumers' Status Orientation in an African Context. *Cogent Business & Management*, 11 (1), pp. 844-845. Available from: <https://doi.org/10.1080/23311975.2321787>

privacy of customers, particularly in the area of time-management or speed, accessibility, cost-benefit, and cognitive offload.³⁶

There are veritable risks and probable dangers that may associate with internet financial services and electronic currencies. These risks which include criminal tendencies such as terrorism financing, money laundering, Ponzi networking and abuse of the market order are not within the scope of this paper.³⁷ The truth is that digital currencies and their pilot platforms such as mobile money have shown capacity to build inclusivity by bringing the poor and vulnerable who were hitherto incapable of institutional banking into the banking net. The case of Zimbabwe clearly demonstrates the foregoing position.³⁸ Zimbabwe adopted no singular official currency from January 2009. The country announced a multi-currency arrangement in January 2009 following her peculiar economic experiences resulting in hyperinflation as well as instability in polity. The country largely uses mobile money, plastic money, and multi-currency mechanism to drive its economy. Consequently, the common view on the proliferation of digital currencies like bitcoins suffices for the purposes of this paper, particularly for financial inclusion of the vulnerable in Nigeria and South Africa. To this end, the position for the recognition of internet financial services and such digital currencies that may be legally administered by the central bank would promote accommodation of persons with low income-earning within the banking infrastructure.³⁹ While maintaining regular currencies imbued with intrinsic value and regulated by national governments, particularly for purpose of taxation, electronic financial services should be evolved and regulated in like manner by the central bank to address the exclusion of the most vulnerable from financial organogram of the Nigerian and South African economies as well as those of other African countries like Zimbabwe.

³⁶ Rouse, M., Batiz-Lazo, B. and Carbo-Valverde, S. (2025) Trust and Socio-Demographic Influences on Mobile Banking Adoption in South Africa: A Longitudinal Study. *International Journal of Bank Marketing*. Available from: <https://doi.org/10.1108/IJBM-08-2024-0458>

³⁷ Chitimira, H. and Ncube, M. (2020) The Role of Regulatory Bodies and Other Role-Players in the Promotion of Financial Inclusion in South Africa. *Acta Universitatis Danubius Juridica*, p. 34.

³⁸ Chitimira, H. and Ncube, M. (2021) Towards Ingenious Technology and the Robust Enforcement of Financial Markets Laws to Curb Money Laundering in Zimbabwe. *Potchefstroom Electronic Law Journal*, pp. 1-46,

³⁹ Chilimira, H. and Magau, P. T. (2021) A Legal Analysis of the Use of Innovative Technology in the Promotion of Financial Inclusion for Low-Income Earners in South Africa. *Potchefstroom Electronic Law Journal*, pp. 1-27.

2.2.THE EMERGENCE OF INTERNET BANKING SERVICES IN SOUTH AFRICA AND NIGERIA: AN OVERVIEW

Digital financial products may be conceived as the diverse financial products accessible and rendered by digital mechanisms and tools like smartphones, computers, tablets and so on whereas mobile money services include banking without walls, electronically generated money transactions such as credits, savings, insurance, remittances, and electronic payments. Digital financial services could also encompass computer applications and software, smart technologies which include the smart phones and other technical devices connected to the Internet of Things (IoT) to deliver enhanced, affordable and swift financial services to consumers.⁴⁰ Put differently, digital financial services describe an aspect of innovative fintech outcomes that are affording seamless financial services to persons including those who were hitherto marginalised in the financial market spaces of Nigeria and South Africa.⁴¹

It becomes imperative to distinguish between mobile money and mobile banking which are sometimes fluid in definition because of their common internet denominator. Mobile Money is conceived as a financial service that channels receiving and sending of money through smartphones or other internet enabled devices such as Point of Sales (PoS). It operates as an electronic wallet in which users mobile telephone numbers are connected to their electronic account enhancing transactions at the press of the button without interactions with institutional bank channels. The frontrunner service providers of mobile money in Nigeria are Opay, Moniepoint, Palmpay, Firstmonie and Kuda which operate in similar manner as the M-PESA.⁴² Conversely, Mobile Banking is an innovative service rendered by institutional banks to enable users transact or access their bank accounts through dedicated mobile application. Mobile banking has extended the banking services beyond the banking mall as the banks' websites and other modems enable transactions round the clock. While mobile money account is easy to own, mobile banking requires the same documentations and more, which make institutional banking a cumbersome exercise. Today, every institutional bank has mobile banking app and chips enabling mobile

⁴⁰ Lawack-Davids, V. (2012) The Legal and Regulatory Framework of Mobile Banking and Mobile Payments in South Africa. *Journal of International Commercial Law and Technology*, p. 320.

⁴¹ Mhlanga, D., Dunga, S. H. and Moloi, T. (2020) Financial Inclusion and Poverty Alleviation among Smallholder Farmers in Zimbabwe. *Eurasian Journal of Economics and Finance*, pp. 171-172.

⁴² M-PESA is the pioneer mobile money platform in Kenya which model of operations is similar to the mobile money services around Africa. See Ndung'u, N. S. (2021) *A Digital Financing Services Revolution in Kenya: The M-Pesa Case Study*. Nairobi: African Economic Research Consortium, pp. 5-11.

banking out of which the Automatic Teller Machine (ATM) Cards are most prominent.

The innovative use of smart technology has permeated all governance and socio-economic environments, including the financial economies of South Africa and Nigeria. The emergence of digital financial services which market mall or business venue thrives within the cyberspace has re-ignited arguments on the governance of the cyberspace to ensure healthy economic competition insulated from criminality.⁴³ Fintech startups have collaborated with mobile network service providers to develop tools and software that have capacity to process diverse transactions, allowing all manner of users to receive and send money irrespective of geographic boundaries, using mobile phone devices and other electronic platforms. Nearly six percent of the total Nigerian population engaged the services of mobile money in 2021 with a record exceeding 124 million transactions on mobile apps.⁴⁴ By May 2024, about sixty-four percent (64%) of the Nigerian Population use mobile money apps.⁴⁵

The popularity of mobile money platforms is not peculiar to Nigeria. Chitimira and Magau posit that about eight million, constituting more than half of the fifteen million total population have their mobile phones enabled for mobile money transactions in Zimbabwe.⁴⁶ The foremost mobile money web in Zimbabwe known as Ecocash is operated by Econet Wireless, a multi-national communication services provider.⁴⁷ Mobile money operations have enabled the economy to overcome incessant cash crunch and hyperinflation which has been the lot of the country's economy most recently.⁴⁸ The pandemic COVID-19 magnified the relevance of mobile currencies to a struggling economy by enabling fast and safe transactions without the rigours of institutional banking procedures that may defy the universal social distance policy at the time.⁴⁹

⁴³ Ginsburg, T. (2022) Democracies and International Law: An Update. *Chicago Journal of International Law*, 23 (1), p. 21. See also, Zang, D. (2022) Revolt against the U.S. Hegemony: Judicial Divergence in Cyberspace. *Wisconsin International Law Journal*, 39 (1), pp. 4 & 9.

⁴⁴ *Banking Industry in Nigeria – Statistics & Facts*. [online] Statistica. Available from: <https://www.statistica.com> [accessed 18 March 2025]

⁴⁵ Sasu, D. D. (2024) *Population with Mobile Money Accounts in Nigeria 2019 – 2024*. [online] Statistica. Available from: <https://www.statistica.com/statistics/1182346/population-with-mobile-money-accounts-in-nigeria-2019-2024> [accessed 18 March 2025]

⁴⁶ Chilimira, H. and Magau, P. T. (2021), *op. cit.* pp. 3-4.

⁴⁷ Chitimira, H. and E. Torerai, E. (2021), *op. cit.* p. 12

⁴⁸ Phiri, C. and Muponda, G. (2016) Public Confidence and its Impact on the Performance and Stability of Banks in Zimbabwe. *University of Zimbabwe Business Review*, p. 3.

⁴⁹ Mann, R. J., (2020) Driver for Contactless Payments. In: K. Pistor (ed.) *Law in the Time of COVID-19*. New York: Columbia Law School, p. 177; Kasradze, T. (2020) Challenges Facing Financial Inclusion Due to the Covid-19 Pandemic. *European Journal of Marketing*

Safaricom inaugurated M-PESA in 2007 to promote financial support to unbanked individuals in Kenya.⁵⁰ The initiative which was launched as a micro-loan package advanced as a dependable means for transfer and receipt of funds, recording tremendous success because of its flexibility, state-of-the-arts security and user-friendly approach. The M-PESA model of mobile money transaction gained confidence and transparency by its operative security procedures. The process demands the generation of transaction pin and communicates details of the transaction to parties by a short message signal (SMS). The SMS serves as receipt for the transaction. Osei suggests that half of the mobile money users globally are domiciled in Africa, with M-PESA dominating the mobile money space.⁵¹ Efforts to integrate mobile money into the financial environment were not as challenging in South Africa as they were in Nigeria and Zimbabwe. The truth is that internet and formidable communication network is prerequisite for the survival of digital financial transactions. These existential technologies which Nigeria is still grappling to guarantee, are taken for granted in South Africa. The earliest initiatives to integrate mobile money platforms into South Africa's financial space was unsuccessful, principally because of an inflexible financial regulatory policy run and controlled largely by pro-banks conservatives.⁵² At the dawn of 2020, the Mobile Telephone Network (MTN) which is a foremost South Africa's telecommunications company, reintroduced its Mobile Money (MoMo) product.⁵³ The revival of the MoMo application fueled the patronage for digital cash in South Africa at the outbreak of COVID -19 pandemic.⁵⁴ However, the success of the MoMo platform has not induced flexibility into the South African financial regulatory infrastructure as in Nigeria and

and Economics, p. 70; De, R., Pandey, N. and A. Pal (2020). Impact of Digital Surge during Covid-19 Pandemic: A Viewpoint on Research and Practice. *International Journal of Information Management*, p. 3.

⁵⁰ "M" stands for mobile while "PESA" means money in Swahili. See, Kagan, J. (2023) *What is M-PESA?*. [online] Investopedia. Available from: <https://www.investopedia.com/terms/m/mpesa.asp> [accessed 18 March 2025]. See also, Buku, M. W. and Meredith, M. W. (2013) Safaricom and M-Pesa in Kenya: Financial Inclusion and Financial Integrity. *Washington Journal of Law, Technology & Arts*, p. 379.

⁵¹ Osei, C. (2021) *Evolution of Mobile Money*. [online] B & FT Online. Available from: <https://thebftonline.com/2021/11/23/evolution-of-mobile-money/> [accessed 18 March 2025]

⁵² Abrahams, R. (2017) Financial Inclusion in South Africa: A Review of the Literature. *Southern African Accounting Association*, p. 650; Chatain, P. I. et al. (2011) *Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions*. Washington D.C.: The World Bank, p. 66.

⁵³ McLeod, D. (2020) *MTN in Big E-Commerce Play with Mobile Money*. [online] TechCentral. Available from: <https://techcentral.co.za/mtn-mobile-money-can-now-be-used-for-online-shopping/176377/> [accessed 10 February 2025]

⁵⁴ Ibid.

Zimbabwe thereby raising concerns over the long term survival of the mobile money idea.

While fintech solutions are beneficial to the economy in several ways such as poverty alleviation and job creation, swift and efficient financial service delivery and so on, there are dangers and regulatory challenges. The system is fraught with fraud and corruption, criminality as well as abuse by those who are fugitives from the law. To this end, there should be an intentional balancing of access to digital financial products and counter-terrorism financing (CTF) as well as the implementation of anti-money laundering (AML) policies to contain illicit financial engagements in Nigeria and South Africa.⁵⁵

2.3.THE ADMINISTRATION OF DIGITAL FINANCIAL SERVICES IN NIGERIA

Nigeria does not have a specific statute that regulates digital financial services in express terms. Recourse may, therefore, be had to the activities of some agencies that impact on the operations of mobile money service providers. Consequently, the Nigeria's national bank⁵⁶ collaborates with the Communications Commission (NCC) to monitor and regulate mobile money services in Nigeria, in the absence of a dedicated ombudsman. While the Apex bank licenses or authorises the operations of mobile money platforms in Nigeria,⁵⁷ the NCC issues unique operational codes to them to guarantee hitch-free electronic money payment interface with other operators.⁵⁸ In 2020, the Apex Bank had issued a circular prohibiting all MMOs from continuing receipts of credits routed through international-money-transfer-operators (IMTOs). This challenged the soaring vibrancy of digital money operations and their continued relevance as a critical contributor to the economic index in Nigeria.⁵⁹ The CBN had in July 2021 released a framework for the regulation of mobile money services in Nigeria in line with the powers granted it in section 47 (2) of the enabling Act⁶⁰ and section 57 (1) of the BOFIA. It was stated by the CBN in the pre-amble to the Regulation that the

⁵⁵ Chitimira, H. and Munedzi, S. (2021) *op. cit.* pp. 48-49

⁵⁶ Nigeria's National Bank refers to the Central Bank of Nigeria (CBN), the Apex Bank or Bankers' Bank.

⁵⁷ *The CBN Act 2007*, (c. 47:2). Nigeria. In: English.

⁵⁸ See *Circular referenced PSM/DIR/CON/CWO/16/119 2020*. SI. Nigeria

⁵⁹ This mechanism is known as the Nigerian Inter-Bank Supplementary System (NIBSS) under the control of the NCC.

⁶⁰ Circular referenced PSM/DIR/CON/CWO/16/119 2020, *op. cit.*. See also *CBN Regulatory Framework for Mobile Money Services in Nigeria 2021* [online] CBN. Available from: <https://www.cbn.gov.ng/Out/2021/CCD/Framework%20and%20Guidelines%20on%20Mobile%20Money%20Services%20in%20Nigeria%20-%20July%202021.pdf> / [accessed 18 March 2025]

“Regulation was a path towards achieving availability, acceptance and usage of mobile payment service as achieving a nationally utilised and internationally recognised payment system necessitates strategies to bring informal payment transactions into the formal system.”

Idowu⁶¹ reckons that the CBN announced its preparedness to evolve Central-Bank-Digital-Currency (CBDC) as a critical driver for the proposed cashless economy in the manner of the huge success recorded with POS⁶² agent banking, online banking, ATMs,⁶³ PSBs⁶⁴ and mobile banking. It is observed that the operations of the proposed CBDC is yet to be seen in Nigeria till date.

The framework could be divided into two broad models according to bank's operative intervention.⁶⁵ The powered-by-bank or other financial entities permits partnering with a bank institution or a conglomerate of financial institutions to initiate payment systems or render such mobile money services as may be desirable. Firstmonie typifies a bank-led model. Conversely, under a non-bank-led model, the CBN issues licences to corporate entities to engage in digital money transactions as in the cases of Smartcash, Moniepoint and others. Elubode and Adejojo argue that unlike in Zimbabwe and South Africa, MTN, Glo and Airtel (Econet Wireless) were barred from providing mobile money services because the CBN would want a monopoly and complete control over the country's monetary policy.⁶⁶ Telecommunications companies were granted Payment Service Banks (PSBs) approval in principle to engage in digital financial services in Nigeria in April, 2022.⁶⁷

Besides the bureaucratic administration of banking activities in Nigeria by the CBN, there are specific statutes that bear on financial activities generally.

⁶¹ Idowu, B. (2023) *Economy: As Full Implementation of Cashless Policy Starts Today*. [online] Leadership. Available from: <https://leadership.ng/economy-as-full-implementation-of-cashless-policy-starts-today/#> [accessed 15 March 2025]

⁶² POS means Point of Sale Terminals. It is a device that accesses credit or master cards for the purpose credit and debit electronic transactions in the same manner as ATMs would do.

⁶³ ATM means Automatic Teller Machine. They are owned and structured by institutional banks to accept master cards, debit cards and other such cards for purposes of banking transactions, including limited cash payments.

⁶⁴ PSB refers to Payment System Bank.

⁶⁵ Oladokun, A., Akanni, Z. and Nnebedum, O. (2023) *Regulatory Framework for Mobile Money Operations in Nigeria*. Jackson, Etti & Edu. Available from: <https://jee.africa> [Accessed 10 March 2025]

⁶⁶ Elubode, A. E. and Adejojo, E. F. (2024) An Evaluation of Mobile Money Services as An Alternative to the Mainstream Banking System in Nigeria. *RUN Law Journal*, 7(1), pp. 10-11.

⁶⁷ The PSB is issued to the network service providers because they have the capacity to reach the unbanked Nigerians with conditions which include: 1 Minimum of five billion Naira (\$13 million) capitalization. 2. Non issuance of credit cards or loans. 3. No transactions in foreign currencies. 4. Insuring depositors' monies with Nigeria Deposit Insurance Corporation (NDIC), among others.

The BOFIA⁶⁸ primarily regulates banking in Nigeria. Although banking is a fundamental aspect of financial services, the activities of fintech companies go beyond the traditional banking business. Section 2 (1) of BOFIA stipulates that any individual conducting the business of banking in Nigeria shall be incorporated. The business shall in addition be carried on with strict compliance to the terms of a valid licence as stipulated in section 3 of BOFIA. The provision relating to incorporation is in tandem with the Companies and Allied Matters Act (CAMA) which provided options for the promoters of such business outfit to include limited liability company, unlimited liability company and company limited by guarantee.⁶⁹ Section 66 of the BOFIA defined the term “other financial institution” to implicate any person, group of persons, corporate or non-corporate other than a bank validly authorised to engage in the business of financing, and brokerage or whose main object includes project financing, management of funds, investment management, financial consultancy and so on. It therefore stands to reason that fintech financial services, being such as may conveniently be accommodated under section 66 of BOFIA, may only operate in Nigeria in compliance with section 59 of the Act.⁷⁰ The provision ensures transparency and caution against criminality as incorporation of a company brings such company’s activities under bureaucratic scrutiny.⁷¹ Failure to incorporate a fintech company may inform a criminal intention capable of scrutiny by investigative agencies.⁷²

The Nigeria Finance Act is a unique statute which strives to amend the myriads of financial laws in Nigeria for the purpose of aligning them into one document.⁷³ The Act, however, amended the CAMA only as it relates to shareholding and dividends.⁷⁴ It did not touch on the operationality of fintech generally. The law was expected to function like the Singaporean Financial Services and Markets Act 2022 (FSMA) which established omnibus powers for broad-based governance of monetary transactions and markets aimed at stabilising the ever-evolving landscape of fintech operations.⁷⁵ The law which is being implemented in phases has in its 2024 round of implementation introduced novel sections on technology and actuarial

⁶⁸ BOFIA 2020. Nigeria.

⁶⁹ CAMA 2020, (s. 21). Nigeria.

⁷⁰ BOFIA, *op. cit.*, (s. 59) provides for procedure for the application for licence to operate as a financial institution in Nigeria.

⁷¹ Vucinic, M. (2020) Fintech and Financial Stability: Potential Influence of Fin Tech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, 2, pp. 43-66.

⁷² EFCC (Establishment) Act 2002, (s. 5). Nigeria. In: English.

⁷³ Finance Act 2020. Nigeria.

⁷⁴ Finance Act 2020, *op. cit.* s. 60.

⁷⁵ *Financial Services and Markets Act 2022*. Singapore. In: English. Available from: <https://www.mas.gov.sg/regulation/acts/financial-services-and-markets-act-2022> [accessed 14 March 2025]

science.⁷⁶ Like the Finance Act, the Cyber Crimes Act⁷⁷, is not primarily designed to regulate fintech activities in Nigeria.⁷⁸ The Acts are lost opportunities to set up customised legal frameworks for digital monetary transactions in Nigeria.

2.4. THE ADMINISTRATION OF INTERNET-POWERED FINANCIAL PRODUCTS IN SOUTH AFRICA

Like Nigeria, South Africa has no specific statute for the administration of digital monetary services. This state of things has not inhibited or limited the operationality and patronage of fintech products, particularly the mobile money transactions in the country.⁷⁹ The extant statutory framework operative in the financial industry appears to have been extended to digital financial products.⁸⁰ The current legal regime includes the South African Reserve Bank (SARB) Act 89 of 1990,⁸¹ the National Payment System Act,⁸² the FICA,⁸³ the POCA,⁸⁴ and the FSR Act.⁸⁵

The SARB Act stipulates two broad functions for the SARB. The bank is primarily mandated to preserve and defend the purchasing power of the South African fiat currency to enhance a sustainable and balanced development of the economy.⁸⁶ It is further obligated to preserve and sustain stable financial environment in South Africa.⁸⁷ It is responsible for monetary circulation and in that portfolio, it has the power to issue currencies and coins, supervise payments, or settlement arrangements in the country.⁸⁸ To this end, since digital financial services function to enhance payments and settlement arrangements, SARB may validly regulate the activities.

⁷⁶ (2024) *Fintech Laws and Regulations 2024 – Singapore*. [online] Global Legal Insights (Gli). Available from: <https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/singapore/> [accessed 14 March 2025]

⁷⁷ *Cybercrime (Prohibition, Prevention etc.) Act 2015*. (c. 37) Nigeria. Section 37 of the Act made a passive reference to financial institutions carrying out electronic transactions by mandating the provision of certain documents for identification purposes only.

⁷⁸ Owolabi, K. M. W. (2023) Understanding the Place of Islamic Arbitration within the Nigerian Law. *Jurnal Hukum Novelty*, 14 (1), pp. 69-87.

⁷⁹ Chitimira, H. and Torerai, E. (2023) A Regulatory Analysis of Digital Financial Services and the Adoption of Central Bank Digital Currencies in Zimbabwe and South Africa. *Juridical Tribune*, 13 (3), p. 379.

⁸⁰ Ibid.

⁸¹ See SARB Act 1990, (ss. 2-38). SA.

⁸² *National Payment Systems Act*, (s. 2). SA.

⁸³ *Financial Intelligence Centre Act 38 of 2001*, (c. 20 – 21:H). SA.

⁸⁴ *Prevention of Organised Crime Act 121 of 1998*, (s. 48). SA

⁸⁵ *Financial Sector Regulation Act 2017*, (s. 57: B & 58). SA.

⁸⁶ *The South African Reserve Bank Act 90 of 1989*, (s. 3:1). SA.

⁸⁷ *The South African Reserve Bank Act 90 of 1989*, *op. cit.* (s. 3:2).

⁸⁸ *The South African Reserve Bank Act 90 of 1989*, *op. cit.* (s. 10:1 (c)(i)).

Under the NPSA, the powers to operate, establish, regulate and oversee the South African payment settlement and clearing systems is exclusively donated to the SARB.⁸⁹ The law does not specifically make provisions for digital financial service providers as stakeholders in the national payment arrangements. This is because the services are not mentioned to constitute payment, clearing or settlement systems in South Africa.⁹⁰ However, records show that over 576 billion South African Rand worth of transactions are routed on daily basis through the NPS.⁹¹ The authority of SARB extends to the recognition of payment systems and the delisting or proscription of non-recognised actors in the financial sector.⁹² The law further empowers SARB to intercept and possess any information relating to the financial settlement arrangements in South Africa.⁹³ This implicates that all actors in the payment circle have the duty to avail data relating to transactions they have enabled upon being requested to do so by SARB.

The primary target of POCA is to tackle issues relating to laundering of money, organised crime, and related activities through the penal arrangement. Corruption and the associate act of laundering of money are very grave offences in South Africa. The offences are punishable with up to 30 years prison sentence or prohibitive fine of about R100 million upon conviction.⁹⁴ POCA does not particularly refer to digital financial services, it nonetheless covers offences such as proceeds of crime, wealth acquisition without credible explanation, among others fears that have been associated with fintech innovations. The law has not specified what obligations are required of the fintech companies in respect of users' transactions as a check against money laundering or terrorism financing, particularly to ascertain the source of funds. According to De Koker, to identify users in the circumstances with identification documents such as identity cards (IDs) or passports may not suffice for a comprehensive profiling that should aid the detection of suspicious financial transactions.⁹⁵ However, digital financial services promoters are under obligation to conduct their businesses in compliance

⁸⁹ *National Payment Systems Act*, (s. 2). SA.

⁹⁰ *National Payment Systems Act*, *op. cit.* (s. 1).

⁹¹ Kariuki, P., Ofusori, L. O. and Goyayi, M. L. J. (2025) Internet of Things on Banking Processes in South Africa: A Systematic Reflection on Innovations, Opportunities and Challenges. *Digital Business*, 5 (1) 100097. Available from: <https://doi.org/10.1016/j.digbus.2024.100097> [Accessed 2 August 2025]

⁹² Kariuki, P., Ofusori, L. O. and Goyayi, M. L. J. (2025), *op. cit.* p. 3:1-5.

⁹³ Kariuki, P., Ofusori, L. O. and Goyayi, M. L. J. (2025), *op. cit.* p. 10.

⁹⁴ Prevention of Organised Crime Act 121 of 1998, *op. cit.* (s. 8:1). SA

⁹⁵ De Koker, L. (2014) The FATF's Customer Identification Framework: Fit for Purpose? *Journal of Money Laundering Control*, p. 285. See also, Chitimira, H. (2020) The Reliance on Artificial Intelligence Measures to Curb Money Laundering Practices in the South African Banking Institutions and Real Estate Sector. *Acta Universitatis Danubius Juridica*, p. 29.

and with the awareness of POCA and other legislations in force in South Africa.

The most important economic benefit of fintech innovation is inclusivity of bankable persons within the community. The Prudential Authority (PA),⁹⁶ like the Financial Sector Conduct Authority (FSCA)⁹⁷ is a creation of the FSR mandated to administer the operations of financial institutions in order to promote inclusivity of all bankable persons in the country.⁹⁸ The implication is that FSCA functions in collaboration with SARB in the supervision of the activities of financial institutions in South Africa. However, the PA and FSCA lack clear-cut responsibilities impacting directly on fintech activities in the Republic of South Africa.⁹⁹ Chitimira and Torerai suggest an amendment of the FSR to clearly stipulate the bureaucratic administration of fintech products within South Africa.¹⁰⁰

It is evident from the foregoing regulatory frameworks that the Nigerian and South African approach to internet financial services squarely identifies with the Institutional Regulatory Theory (IRT) or the corporate governance model underpinning operations of mobile banking.¹⁰¹ The concept may be examined from the two angles of regulatory support, and institutional influence. The theory conceives that what is needed for business to thrive is a positive regulatory landscape which fosters innovations and guarantees consumers protection. Consequently, the two countries abide by the strengthening of existing banking institutions to support internet banking operations. This explains why the sector is regulated generally, without specifications in respect of internet financial services and the available products overtime with South Africa towering over Nigeria in terms of well-defined licensing procedure for Fintech operations. The development has worsened the global rating of both countries in financial transactions tainted with criminality.¹⁰² The model poses a great challenge to the industry in the advent of technological twist such as mobile banking.

⁹⁶ Financial Sector Regulation Act 2017, *op. cit.* (s. 32-55)

⁹⁷ Financial Sector Regulation Act 2017, *op. cit.* (ss. 56-72)

⁹⁸ Financial Sector Regulation Act 2017, *op. cit.* (s. 34:1)

⁹⁹ Financial Sector Regulation Act 2017, *op. cit.* (s. 56 - 58)

¹⁰⁰ Chitimira, H. and Torerai, E. (2023), *op. cit.* p. 400.

¹⁰¹ Amune, M. S. (2024) Legal Regime of Electronic Banking in Nigeria and the Evidence Act 2011: An Examination of the Intersection between Technology and Law. *Iconic Research and Engineering Journals*. 8 (6), p. 844.

¹⁰² Kariuki, P., Ofusori, L. O. and Goyayi, M. L. J. (2025), *op. cit.*

2.5.DIGITAL FINANCIAL SERVICES: STATUTORY REGULATION IN ZIMBABWE

Like Nigeria and South Africa, there is no legislation with specific or express regulatory intendment of digital financial services in Zimbabwe. The realities leave regulators with community implementation of several related statutes in the attempt to bring fintech products within the operations of enabling statutes.

The National Payment Systems Act came into force in 2001 at a time when fintech services were yet to disrupt the financial monopoly of institutional banks in Zimbabwe.¹⁰³ Digital financial services were consequently not within the contemplation of the policymakers at the time and so were not recognised. The National Payment Systems Act¹⁰⁴ initiates the recognition, regulation and operation of clearing and payments arrangements between financial houses in Zimbabwe. The Reserve Bank of Zimbabwe (RBZ) has a clearing department known as the National Payments Systems Division (NPSD) with regulatory and supervisory mandate covering digital financial transactions in Zimbabwe.¹⁰⁵ The Banking Act mandates the registration, regulation and supervision of banks and other financial institutions in Zimbabwe.¹⁰⁶ The Act provides a retinue of financial institutions in Zimbabwe which includes banks, pension funds managers, insurance companies and building societies.¹⁰⁷ Although the list did not include digital financial services powered by fintech, its provision on the meaning assigned to mobile banking testifies to the effect that the lawmakers intended to cover banking transaction outside the operations of institutional banks.¹⁰⁸ It is safe to posit that despite the seeming relatedness, the terms “digital financial services” and ‘mobile banking’ are not one and the same. This is because the requirement of the Act for registration of financial service providers may not be readily available to mobile money operators.¹⁰⁹

Another law which has operative bearing on digital financial services is the Exchange Control Act.¹¹⁰ The Act which seeks to combat illicit

¹⁰³ *The National Payments Systems Act 2001* (c. 24:23), Zimbabwe was enacted on 16 November 2001. The first digital financial service in Africa, M-PESA, was introduced in 2007 by Safaricom, a subsidiary of the British group of Vodafone.

¹⁰⁴ *The National Payments Systems Act 2001, op. cit.* (s. 2)

¹⁰⁵ *The National Payment Systems Act 2001, op. cit.* (s. 3:1 (a)-(c)) read with *The Banking Act 2001*, (s. 7:(a), (d)&(f) and 1), Zimbabwe.

¹⁰⁶ See the Long Title of the Banking Act.

¹⁰⁷ *The Banking Act 2001, op. cit.* (s. 2)

¹⁰⁸ *Ibid.*

¹⁰⁹ Lawack-Davids, V. (2012), *op. cit.* p. 319; Mbengo, P. and Phiri, M. A. (2015) Mobile Banking Adoption: A Rural Zimbabwean Market Perspective. *Journal of Corporate Ownership & Control*, p. 197.

¹¹⁰ *The Exchange Control Act (Chapter 22:05) 1965*, (s. 2:2 (a)). Zimbabwe.

peddling of foreign currencies by unauthorised persons requires the licensing and registration of persons who deal in currencies, gold, or securities in Zimbabwe.¹¹¹ Mobile money operators exploited the lack of specifics in the law to engage illicit foreign exchange dealings. In *Ecocash Zimbabwe v Reserve Bank of Zimbabwe*,¹¹² it was established that certain persons operated diverse mobile money agent-accounts as conduit for illicit forex trading which undermined the official markets.¹¹³ According to Chitimira and Ncube, the mobile financial infrastructure of Ecocash, OneWallet, Telecash, Skwama and OneMoney were used to launder about two billion Zimbabwean dollars in 2020.¹¹⁴

The Banking Regulations 2020 demonstrates the most intentional measure adopted by policymakers to bureaucratically administer digital financial services in Zimbabwe. The Regulations defines mobile banking in the same vein with the Banking Act.¹¹⁵ In its broadest interpretation, the Regulation equates mobile money wallet to a regular bank account though the instrument was silent on digital financial services. MNOs were safely captured under the definition of money “transmission providers” who were mandated to operate a trust account for the security of customers’ funds.¹¹⁶ The trust accounts attract regulatory prowess of the RBZ which should ensure the integrity of the financial sector by routine monitoring.¹¹⁷

2.6.THE ADOPTION OF CBDC IN NIGERIA AND SOUTH AFRICA

Digital currencies constitute fundamental part of innovative financial evolution in the payment arrangements of several countries that have recognised virtual or electronic versions of legal tenders.¹¹⁸ Many countries of the world are in the incubation stages of adopting central bank digital money.¹¹⁹ These currencies are minted and statutorily produced as well as regulated by the Central Bank or National Bank of a given country unlike

¹¹¹ Ibid. See also Tuba, M. D. (2014) The Regulation of Electronic Money Institutions in the SADC Region Some Lessons from the EU. *Potchefstroom Electronic law Journal*, p. 2270.

¹¹² *Ecocash Zimbabwe v Reserve Bank of Zimbabwe* (2020), HH 333-20 (HC 3007/20) ZWHC 333.

¹¹³ *Ecocash Zimbabwe v Reserve Bank of Zimbabwe*, *op. cit.* p. 10

¹¹⁴ Chitimira, H. and Ncube, M. (2020), *op. cit.* p. 10

¹¹⁵ The Banking Regulations 2020, *op. cit.* (art. 2); The Banking Act, *op. cit.* (s. 2)

¹¹⁶ The Banking Regulations 2020, *op. cit.* (s. 4:3)

¹¹⁷ The Banking Regulations 2020, *op. cit.* (s. 5:1)

¹¹⁸ Klein, M. et al. (2020) The Digital Euro and the Role of DLT for Central Bank Digital Currencies. *Frankfurt School of Finance & Management GmbH FSBC Working Papers*, pp. 2-6; Glass, J. E. (2017) What is Digital Currency. *The Journal of the Franklin Pierce Center for Intellectual Property*, pp. 481-482.

¹¹⁹ Klein, M. et al. (2020), *op. cit.* pp. 2-3

bitcoins and crypto assets.¹²⁰ There is no unified conception of “central bank digital currency” but a working definition of central bank digital currencies refers to the adoption and engagement of electronic or virtual version of the national currencies as alternative to the conventional fiat currency, that is, crisp banknotes and coins for financial settlements within the given jurisdiction.¹²¹

The evolution of CBDC signals a paradigm shift towards a cashless economy and improved state surveillance capabilities. For an attainable cashless economy, the CBDC must either be linked with other country’s models across-the-border or be evolved by regional synergy. This is demonstrated by the new digital solutions being developed by the World Bank Group’s International Finance Corporation and the ASEAN Bankers Association with the object of serving as a global, open-framework for collaborative designing and experimentation of digital financial products as the world pulls toward cashless economy. Arvidsson conceives a cashless society as a society where individuals transact more with virtual currency than fiat currencies.¹²² Mobile money has tremendously contributed in demonstrating that a cashless society is possible, particularly in Nigeria and South Africa where individuals no longer grapple with heavy loads of crisp currencies for huge transactions as just an ATM card would do to move massive cash. The domestic experience with ATM cards could be reinvented using electronic tokens otherwise known as the CBDC, to be issued by some clearing institutions to which apex banks of countries may subscribe for the benefit of the bureaucracy and individual commercial transactions requiring huge payments. This is a milestone towards cashless economy which Africa may leverage on to achieve economic integration within the region by 2063.

The COVID-19 pandemic demonstrates the convenient, hygienic, and safer health advantages of cashless transactions over cash transactions, hence the growing patronage of the cashless trend across the globe.¹²³ Cashless transactions are accepted as measures to contain escalation of pandemic or viruses. The adoption of digital currencies would enhance financial inclusivity of the most economically vulnerable, with low-income earnings, which constitute the bulk of the unbanked community in the era of banking monopoly of the institutional banks. Digital currencies have the capacity to eradicate issues of cash heists in economies such as Nigeria and South Africa.

¹²⁰ Arvidsson, N. (2019) *Building a Cashless Society: The Swedish Route to the Future of Cash Payments*. Switzerland: Springer Nature, pp. 64-65.

¹²¹ Lu, L. (2018) Decoding Alipay: Mobile Payments, A Cashless Society and Regulatory Challenges. *Butterworths Journal of International Banking and Financial Law*, p. 41.

¹²² Arvidsson, N. (2019), *op. cit.*

¹²³ Mann, R. J. (2020), *op. cit.* pp. 177-179; Kasradze, T. (2020), *op. cit.*

Nigeria and South Africa have not formally issued or recognised digital Currencies. The central banks of both countries are toying with the idea which has reached an advance stage. South Africa is blazing the trail in this direction, with the collaborative consent of the Bank for International Settlements (BIS) under the initiative of “Project Khokha” and “Project Dunbar”.¹²⁴ The initiatives target interbank settlements instead of direct end users. To this end, SARB is currently test-running the viability of a digital currency to be adopted by financial institutions for managing interbank transfers.¹²⁵ The South African Government has built an alliance with Singapore, Australia and Malaysia for a mutual cross-border digital currency initiative.¹²⁶ Such alliance is intended to demonstrate the utility of digital financial platforms tending towards cashless economy when multiple countries are linked to the platform. Under the arrangement, CBDC becomes a viable instrument for international transactions under the governance of countries’ apex banks working through unified clearing outfit. The medium has been successfully engaged at different times by Bank of Canada and Banque de France in 2021.¹²⁷ The success of the arrangement would depend on functional linkages of monetary bureaucratic platforms which may transcend economic considerations to transnational political ideological linings. The PayNow Corporate which was evolved to enable businesses and government to make instant financial transactions has been successfully linked with Thailand’s National Bank (Bank of Thailand) as well as India’s National Bank (Reserve Bank of India) under the on-going Unified Payments Interface in 2023.¹²⁸ Private merchants could harness the availability of official electronic financial codes such as DuitNow QR for seamless transactions across boarder.¹²⁹

¹²⁴ Chitimira, H. and Torerai, E. (2023), *op. cit.* p. 402

¹²⁵ Ibid.

¹²⁶ Fuje, H., Quavyom, S. and Qutrama, F. (2022) *More African Central Banks are Exploring Digital Currencies*. [online] IMF Blog. Available from: <https://blogs.imf.org/2022/06/23/more-african-central-banks-are-exploring-digital-currencies/> [accessed 17 March 2025]. See also Klein, M. et al. (2020), *op. cit.* pp. 11-13.

¹²⁷ CBDC – Singapore’s Successful Experiment with France. [online] MAS. Available from: <https://www.mas.gov.sg/news/media-releases/2021/singapore-and-thailand-launch-worlds-first-linkage-of-real-time-payment-system/> [accessed 18 March 2025]

¹²⁸ (2023) *Launch of Real-time Payments between Singapore and India*. [online] MAS. Available from: <https://www.mas.gov.sg/news/media-releases/2023/launch-of-real-time-payments-between-singapore-and-india/> [accessed 18 March 2025]. The Unified Payments Interface uses electronic financial code recognised by countries that subscribe to the arrangement.

¹²⁹ (2023) *Launch of Cross-border QR Payments Linkage between Indonesia and Singapore*. [online] MAS. Available from: <https://www.mas.gov.sg/news/media-releases/2023/launch-of-cross-border-qr-payments-linkage-between-indonesia-and-singapore/> [accessed 18 March 2025]

Consequently, the snail-speed with which Nigeria is embracing digital currency switch is disturbing given Nigeria's leadership role in Africa and its rating as the second to mute the idea, after the Bahamas. The country's attempt to adopt CBDC works for image laundering as it would limit flow of illicit funds because of the CBDC's traceability. Conversely, the individual users' privacy may be infringed in the process of documentation and retention of data. The e-Naira's focus is on the urban elite (partial or class inclusivity) rather than the unbanked community of primary consumers in contrast with the South African project with wholesale concentration on bank-to-bank transactions, particularly cross-border payments, focused more on consumer protection. Other countries of Africa such as Zimbabwe and Kenya are settled at the nursery stage of researches to determine the direction of the banking policy in the circumstances.¹³⁰ It would be safe to state that South Africa's walk towards digital currency switch advancement notwithstanding, no specific statutory framework has evolved in South Africa and Nigeria to govern digital currencies. The necessity for synergy between policymakers of both countries with a view to evolving workable model of digital currency switch should engage economy players. This move would facilitate trade and business linkages between both countries which would in turn drive the African regional economy in line with the African Union (AU)'s Agenda 2063 for shared economic growth and opportunities.¹³¹

3. CONCLUDING REMARKS

As has been discussed elsewhere in this discourse, digital financial services promote financial inclusivity and the fortification of financial shopping fora in Nigeria and South Africa. The invasive innovative fintech are enhancing participation of the unbanked poor and vulnerable individuals in Nigeria and South Africa through their services and products. The gains of these electronic financial services have become much more persuasive from the dawn of the COVID-19 pandemic.¹³² In the circumstances, mobile money afforded swift, safe and seamless financial transactions, reducing the fears

¹³⁰ (2023) Launch of Cross-border QR Payments Linkage between Indonesia and Singapore. *op. cit.*

¹³¹ African Union Commission. (2015) *Agenda 2063: The Africa We Want*. [press release] 10 June. Available from: https://au.int/Agenda2063/popular_version, pp. 2-10.

¹³² Aboh, P. B. and Aloamaka, P. C. (2022) COVID-19 Pandemic and Administration of Criminal Justice in Nigeria: A Call for a Better Application. *Cogito: Multidisciplinary Research Journal*, 14, p. 116; Buheji, M. et al. (2020) The Extent of Covid-19 Pandemic Socio-Economic Impact on Global Poverty: A global Integrative Multidisciplinary Review. *American Journal of Economics*, pp. 215-216.

and realities of the pandemic being capable of escalation through cash transactions which engage inevitable contacts.¹³³

However, the general acceptance and extensive patronage of mobile money services has not enjoyed a corresponding statutory regulatory reaction from policymakers in Nigeria and South Africa. It is clear that both the BOFIA and CBNA do not provide for strict electronic banking regulations for Nigeria thereby leaving the CBN's mandate to issue guideline with much flexibility, tending towards exposure to fraud. The laws regulate the corporate service providers, not the services or products. Consequently, a robust statutory framework should be put in place to regulate the services and products of internet financial services providers. The new law should prescribe the specific licensing regime of Fintech banks. It is suggested that a requirement by Fintech operators to first acquire a Microfinance Bank or Payment Service Bank licence would build confidence and security in the e-banking sector as well as cater for consumer protection against double taxation, inexplicable and unjustifiable charges. It would provide compensatory remedies to issues of ATM dispensing errors, frequent system failures/technical glitches, and issues of app compatibility. The law should also prescribe ways of verifying the validity of digital banking transactions for regulatory and legal uses to stem the vulnerability of such documents to alteration. Furthermore, policy makers should create online community of mobile bank users to enlist an interactive or feedback channel instead of leaving the fate of consumers entirely with the service providers. Both countries should enact laws that strictly guarantee digital privacy and implementation of smart solutions such as facial and voice recognition, multi-layered biometric authentication, encryption protocols in order to protect customers data and prevent cyberattacks, fraud and identity theft that have become commonplace in the era of IoT.

On the issue of digital currency, the Central Banks of Nigeria and South Africa may begin with evolving a central bank digital currency to test-run the financial digital switch. The alternative to specific statutes on the subject is a surgical amendment of the extant laws impacting financial transactions in both countries to integrate the peculiar features and dynamics of digital financial services for adequate bureaucratic governance. South Africa's leadership role in Africa, particularly with respect to the evolution of central bank digital currencies, is a welcome and applaudable development. Conversely, Nigeria's lag in harnessing the financial market economy created by the invasive fintech platforms through the adoption of digital currency is worrisome. Nigeria's stance demonstrates a suspicion of distrust resulting

¹³³ Mann, R. J. (2020), *op. cit.*

in unpreparedness for the evolving financial market economy driven by smart technology. Both countries should take all legitimate steps to capture the unbanked community of persons within the banking net for broader economic benefits. The opportunities have been presented by digital finance service models and could be realised through viable legislation.

LIST OF REFERENCES

- [1] Aboh, P. B. and Aloamaka, P. C. (2022) COVID-19 Pandemic and Administration of Criminal Justice in Nigeria: A Call for a Better Application. *Cogito: Multidisciplinary Research Journal*, 14.
- [2] Abrahams, R. (2017) Financial Inclusion in South Africa: A Review of the Literature. *Southern African Accounting Association*.
- [3] African Union Commission (2015) *Agenda 2063: The Africa We Want*. [press release] 10 June. Available from: https://au.int/Agenda2063/popular_version
- [4] Agrawal, R. (2019) Review of Initiatives taken by the Government and banking regulator for successful transition to a financially inclusive economy: an empirical study of India. *Economic Analysis*, 52 (1). Available from: <https://doi.org/10.28934/ea.19.52.12.pp81-96> [accessed 18 March 2025]
- [5] Ahiauzu, N. and Inko-Tariah, T. (2016) Applicability of Anti-money Laundering Laws to Legal Practitioners in Nigeria: NBA V FGN & CBN. *Journal of Money Control*, p. 329. Available from: <https://doi.org/10.1108/JMLC-09-2015-0038> [accessed 15 March 2025]
- [6] Aidonjio, P. A., Majekudunmi, T. A. and Adeyemi-Balogun, O. J. (2023) The Legal Issues Concerning the Operations of Fin-Tech in Nigeria. *Jurnal Media Hukum*, 30 (2). Available from: <https://dx.doi.org/10.18196/jmh.v30i2.18337>
- [7] Akujuobi, N. E., Anyanwu, G. I. and Eke, C. K. (2021) Regulatory Framework and Bank Operations in Nigeria: A VECM Approach. *International Journal of Development and Management Review*, 16 (1).
- [8] Alexandru, T. and Tabusca, S. (2019) Impact of 5G Technologies in Global Economy, Cybersecurity and Legal Issues. *Journal of Information Systems & Operations Management*.
- [9] Amune, M. S. (2024) Legal Regime of Electronic Banking in Nigeria and the Evidence Act 2011: An Examination of the Intersection between Technology and Law. *Iconic Research and Engineering Journals*. 8 (6).
- [10] Arvidsson, N. (2019) *Building a Cashless Society: The Swedish Route to the Future of Cash Payments*. Switzerland: Springer Nature.

- [11] Asongu, S. A. and Odhiambo, N. M. (2020) Inequality and Gender Economic Inclusion: The Moderating Role of Financial Access in Sub-Saharan Africa. *Economic Analysis and Policy*.
- [12] Badiang, A. M. and Nkwei, E. S. (2024) Mobile Banking Adoption, Its Antecedents and Post-Adoption Effects: The Role of Consumers' Status Orientation in an African Context. *Cogent Business & Management*, 11 (1). Available from: <https://doi.org/10.1080/23311975.2321787> [Accessed 2 August 2025]
- [13] Buheji, M. et al. (2020) The Extent of Covid-19 Pandemic Socio-Economic Impact on Global Poverty: A global Integrative Multidisciplinary Review. *American Journal of Economics*.
- [14] Buku, M. W. and Meredith, M. W. (2013) Safaricom and M-Pesa in Kenya: Financial Inclusion and Financial Integrity. *Washington Journal of Law, Technology & Arts*.
- [15] CBN Regulatory Framework for Mobile Money Services in Nigeria 2021 [online] CBN. Available from: <https://www.cbn.gov.ng/Out/2021/CCD/Framework%20and%20Guidelines%20on%20Mobile%20Money%20Services%20in%20Nigeria%20-%20July%202021.pdf> [accessed 18 March 2025]
- [16] Chatain, P. I. et al. (2011) *Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions*. Washington D.C.: The World Bank.
- [17] Chitimira, H. (2020) The Reliance on Artificial Intelligence Measures to Curb Money Laundering Practices in the South African Banking Institutions and Real Estate Sector. *Acta Universitatis Danubius Juridica*.
- [18] Chitimira, H. and Ncube, M. (2020) The Role of Regulatory Bodies and Other Role-Players in the Promotion of Financial Inclusion in South Africa. *Acta Universitatis Danubius Juridica*.
- [19] Chitimira, H. and Ncube, M. (2021) Towards Ingenious Technology and the Robust Enforcement of Financial Markets Laws to Curb Money Laundering in Zimbabwe. *Potchefstroom Electronic Law Journal*.
- [20] Chitimira, H. and Magau, P. T. (2021) A Legal Analysis of the Use of Innovative Technology in the Promotion of Financial Inclusion for Low-Income Earners in South Africa. *Potchefstroom Electronic Law Journal*.
- [21] Chitimira, H. and Munedzi, S. (2021) Selected Challenges Associated with the Reliance on Customer Due Diligence Measures to Curb Money Laundering in South African Banks and Related Financial Institutions. *Journal of Comparative Law in Africa*.

- [22] Chitimira, H. and Torerai, E. (2021) The Nexus between Mobile Money Regulation, Innovative Technology and The Promotion of Financial Inclusion in Zimbabwe. *Potchefstroom Electronic Law Journal*.
- [23] Chitimira, H. and Torerai, E. (2023) A Regulatory Analysis of Digital Financial Services and the Adoption of Central Bank Digital Currencies in Zimbabwe and South Africa. *Juridical Tribune*, 13 (3).
- [24] De Koker, L. (2014) The FATF's Customer Identification Framework: Fit for Purpose? *Journal of Money Laundering Control*.
- [25] De, R., Pandey, N. and Pal, A. (2020) Impact of Digital Surge during Covid-19 Pandemic: A Viewpoint on Research and Practice. *International Journal of Information Management*.
- [26] Ehirim, U. G. et al. (2024) Strengthening Human Rights Protection in Nigeria: Safeguards under the Police Act 2020. *Khazanah Hukum*, 6 (3). Available from: <https://doi.org/10.15575/KH.V6I3.39569> [accessed 18 March 2025]
- [27] Ehirim, U. G. (2025) Artificial Intelligence and Healthcare Delivery in Nigeria: Legal and Ethical Dimensions of Patients' Rights to Safety. *The Indonesian Journal of Sharia and Socio-Legal Studies*, 1 (1).
- [28] Ehirim, U. G. (2025) Ethical Legal Practice and the Integration of AI into Legal Profession: Striking the Balance. *Open Journal for Legal Studies (OJLS)*, 8 (1). <https://doi.org/10.32591/coas.ojls.0801.02013e> [Accessed 3 August 2025]
- [29] Elubode, A. E. and Adejo, E. F. (2024) An Evaluation of Mobile Money Services as An Alternative to the Mainstream Banking System in Nigeria. *RUN Law Journal*, 7 (1).
- [30] Fuje, H., Quavyom, S. and Qutrama, F. (2022) *More African Central Banks are Exploring Digital Currencies*. [online] IMF Blog. Available from: <https://blogs.imf.org/2022/06/23/more-african-central-banks-are-exploring-digital-currencies/> [accessed 17 March 2025]
- [31] Gasiokwu, M. O. U. (2015) *Legal Research and Methodology: The A – Z of Writing Theses and Dissertations in a Nutshell*. Revised ed. Chenglo Limited.
- [32] Ginsburg, T. (2022) Democracies and International Law: An Update. *Chicago Journal of International Law*, 23 (1).
- [33] Glass, J. E. (2017) What is Digital Currency. *The Journal of the Franklin Pierce Center for Intellectual Property*.
- [34] (2024) *Fintech Laws and Regulations 2024 – Singapore*. [online] Global Legal Insights (Gli). Available from: <https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/singapore/> [accessed 14 March 2025]

- [35] Guild, J. (2017) Fintech and the Future of Finance. *Asian Journal of Public Affairs*.
- [36] Giovanis, A et al. (2019) Adoption of Mobile Banking Services: A Comparative Analysis of Four Competing Theoretical Models. *International Journal of Bank Marketing*, 37 (5). Available from: <https://doi.org/10.1108/IJBM-08-2018-0200>
- [37] Halliday, T., Levi, M. and Reuter, P. (2019) Anti-Money Laundering: An Inquiry into a Disciplinary Transnational Legal Order. *UC Irvine Journal of International, Transnational and Comparative Law*, 4 (3).
- [38] Idowu, B. (2023) *Economy: As Full Implementation of Cashless Policy Starts Today*. [online] Leadership. Available from: <https://leadership.ng/economy-as-full-implementation-of-cashless-policy-starts-today/#> [accessed 15 March 2025]
- [39] Kagan, J. (2023) *What is M-PESA?*. [online] Investopedia. Available from: <https://www.investopedia.com/terms/m/mpesa.asp> [accessed 18 March 2025]
- [40] Kariuki, P., Ofusori, L. O. and Goyayi, M. L. J. (2025) Internet of Things on Banking Processes in South Africa: A Systematic Reflection on Innovations, Opportunities and Challenges. *Digital Business*, 5 (1) 100097. Available from: <https://doi.org/10.1016/j.digbus.2024.100097> [Accessed 2 August 2025]
- [41] Kasradze, T. (2020) Challenges Facing Financial Inclusion Due to the Covid-19 Pandemic. *European Journal of Marketing and Economics*.
- [42] Klein, M., Gross, J. and Sandner, P. (2020) The Digital Euro and the Role of DLT for Central Bank Digital Currencies. *Frankfurt School of Finance & Management GmbH FSBC Working Papers*.
- [43] Lawack-Davids, V. (2012) The Legal and Regulatory Framework of Mobile Banking and Mobile Payments in South Africa. *Journal of International Commercial Law and Technology*.
- [44] Lu, L. (2018) Decoding Alipay: Mobile Payments, A Cashless Society and Regulatory Challenges. *Butterworths Journal of International Banking and Financial Law*.
- [45] Mann, R. J. (2020) Driver for Contactless Payments. In: K. Pistor (ed.) *Law in the Time of COVID-19*. New York: Columbia Law School.
- [46] Mbengo, P. and Phiri, M. A. (2015) Mobile Banking Adoption: A Rural Zimbabwean Market Perspective. *Journal of Corporate Ownership & Control*.
- [47] McLeod, D. (2020) *MTN in Big E-Commerce Play with Mobile Money*. [online] TechCentral. Available from: <https://techcentral.co.za/mtn-mo>

bile-money-can-now-be-used-for-online-shopping/176377/
[accessed 10 February 2025]

- [48] Mhlanga, D., Dunga, S. H. and Moloi, T. (2020) Financial Inclusion and Poverty Alleviation among Smallholder Farmers in Zimbabwe. *Eurasian Journal of Economics and Finance*.
- [49] Ndung'u, N. S. (2021) *A Digital Financing Services Revolution in Kenya: The M-Pesa Case Study*. Nairobi: African Economic Research Consortium.
- [50] Okoye, N. J. et al. (2024) Financial Technology (Fintech) and the Performance of Firms in Nigeria. *International Journal of Social Science, Technology and Economics Management*. 2 (1). Available from: <https://doi.org/10.59781/1524NEOM> [accessed 15 March 2025]
- [51] Oturu, D. (2024) *Fintech Law and Practice in Nigeria*. Aberdeen: Davidson Oturu.
- [52] Oladokun, A., Akanni, Z. and Nnebedum, O. (2023) Regulatory Framework for Mobile Money Operations in Nigeria. *Jackson, Etti & Edu*. Available from: <https://jee.africa> [accessed 18 March 2025]
- [53] Owolabi, K. M. W. (2023) Understanding the Place of Islamic Arbitration within the Nigerian Law. *Jurnal Hukum Novelty*, 14 (1). Available from: <https://dx.doi.org/10.26555/novelty.v14i1.a25926> [accessed 15 March 2025]
- [54] Osei, C. (2021) *Evolution of Mobile Money*. [online] B & FT Online. Available from: <https://thebftonline.com/2021/11/23/evolution-of-mobile-money/> [accessed 18 March 2025]
- [55] (2023) *Launch of Real-time Payments between Singapore and India*. [online] MAS. Available from: <https://www.mas.gov.sg/news/media-releases/2023/launch-of-real-time-payments-between-singapore-and-india/> [accessed 18 March 2025]
- [56] Phiri, C. and Muponda, G. (2016) Public Confidence and its Impact on the Performance and Stability of Banks in Zimbabwe. *University of Zimbabwe Business Review*.
- [57] Prasad, E. (2021) *The Future of Money: How the Digital Revolution is Transforming Currencies and Finance*. Belknap Press: Harvard University Press.
- [58] Rouse, M., Batiz-Lazo, B. and Carbo-Valverde, S. (2025) Trust and Socio-Demographic Influences on Mobile Banking Adoption in South Africa: A Longitudinal Study. *International Journal of Bank Marketing*. Available from: <https://doi.org/10.1108/IJBM-08-2024-0458> [Accessed 2 August 2025]
- [59] Sasu, D. D. (2024) *Population with Mobile Money Accounts in Nigeria 2019 – 2024*. [online] Statistica. Available from: <https://www.statistica.com/stati>

- stics/1182346/population-with-mobile-money-accounts-in-nigeria-2019-2024 [accessed 18 March 2025]
- [60] *Banking Industry in Nigeria – Statistics & Facts*. [online] Statistica. Available from: <https://www.statistica.com> [accessed 18 March 2025]
 - [61] Tamburi, M. Y. (Jnr.) and Kong, Y. (2019) Digitizing Payments: Opportunities for Financial Inclusion for Sub-Saharan Africa. *Case Studies Journal*.
 - [62] Tapainainen, T. (2020) Toward Fintech Adoption Framework for Developing Countries - A Literature Review Based on the Stakeholder Perspective. *Journal of Information Technology Applications & Management*.
 - [63] Torerai, E. (2022) *A Comparative Statutory Analysis on the Use and Regulation of Mobile Money to Promote Financial Inclusion for the Poor in Zimbabwe*. LLD Thesis: North West University, South Africa.
 - [64] Trautman, L. J. (2016) Is Disruptive Blockchain Technology the Future of Financial Services? *The Consumer Finance Law Quarterly Report*.
 - [65] Tuba, M. D. (2014) The Regulation of Electronic Money Institutions in the SADC Region Some Lessons from the EU. *Potchefstroom Electronic Law Journal*.
 - [66] Weihuan, Z., Arner, D. W. and Buckley, R. P. (2015) Regulation of Digital Financial Services in China: Last Mover Advantage? *Tsinghua China Law Review*.
 - [67] Winn, J. K. and De Koker, L. (2013) Introduction to Mobile Money in Developing Countries' Financial Inclusion and Integrity Conference Special Issue. *Washington Journal of Law, Technology & Arts*.
 - [68] Zang, D. (2022) Revolt against the U.S. Hegemony: Judicial Divergence in Cyberspace. *Wisconsin International Law Journal*, 39 (1).
 - [69] Zetzsche, D. A., Buckley, R. P. and Amer, D. W. (2019) Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses. *University of New South Wales Research Series*.

DOI 10.5817/MUJLT2026-40703

THE EVOLUTION OF DIGITAL DIPLOMACY: THE IMPACT OF TECHNOLOGICAL ADVANCEMENTS ON DIPLOMATIC PRACTICE

by

VIONA RASHICA *

Over the centuries, dizzying technological developments have brought about radical changes in diplomacy. As a result, the role of non-state actors has been strengthened in the postmodern era, significantly impacting the traditional state-centered diplomatic model. Various forms of diplomacy have emerged as key instruments of soft power, including digital diplomacy. The latter has become an essential element for achieving states' foreign policy goals and involving non-state actors in international relations. To understand the growing importance of digital diplomacy, this research article examines its historical evolution and potential, which are the main goals of the paper. Qualitative methods, specifically document analysis and case studies, were applied to conduct the research. The research results indicate that digital diplomacy emerged from continuous technological advancements, which have fundamentally transformed diplomacy by improving communication among state actors, increasing negotiation efficiency, facilitating the targeting of global audiences, and enabling non-state actors to engage in solving global challenges. The article's conclusions enhance knowledge about the evolution of digital diplomacy, thus revealing its potential for all the subjects of international law.

KEY WORDS

Digital diplomacy, Evolution, Technological advancements, States, Non-state actors, Diplomatic practice

* Viona Rashica, Doctor of Political Sciences; South East European University; Lecturer of International Relations and European Studies; Academic Researcher of Digital Diplomacy; E-mail: vionarashica@hotmail.com; ORCID: 0000-0002-8046-8353

1. INTRODUCTION

In the contemporary system of international relations, states have traditionally been regarded as the primary actors of international law and diplomatic practice. However, political, economic, and technological developments over the past decades have contributed to the expansion of the range of actors participating in international processes. In addition to states, non-state actors (NSAs) increasingly play an important role, possessing certain attributes of international legal personality and influencing global decision-making processes. In this context, the development of communication technologies and digital platforms has significantly transformed the ways in which diplomatic communication and interaction are conducted. This transformation has led to the emergence and development of digital diplomacy, which refers to the use of digital tools and platforms by both states and NSAs to promote interests, construct narratives, and influence international public opinion.

The objective of this study is to analyze the evolution of digital diplomacy, specifically examining how technological advancements have catalyzed the transformation of diplomatic practices. Accordingly, this article seeks to address the following research question: *In what ways have technological innovations reconfigured the interaction between states and NSAs, and how have these new forms of digital engagement redefined the exercise of influence within the contemporary diplomatic sphere?*

In addition to the abstract, introduction, conclusion, and references, the article also consists of three separate sections. The second section presents the definition and the main objectives of digital diplomacy. The third section tracks the evolution of digital diplomacy and is divided into four subsections. Within them, the development of public diplomacy is elaborated, continuing with the growing role of social diplomacy, the application of e-diplomacy, and the era of social media diplomacy. The fourth section explores the real potential of digital diplomacy, highlighting its main benefits for subjects of international law. This section is divided into three subsections, thus providing data on increasing cooperation between states and NSAs to solve global issues, on facilitating international recognition of small states, as well as on protecting the cybersecurity of states through data embassy.

This paper adopts a qualitative, conceptual research framework to examine the evolving paradigm of digital diplomacy. Instead of an empirical testing of quantitative variables, the methodological approach integrates a systematic document analysis with illustrative case study examinations to map the theoretical and practical trajectory of the field. The document analysis involves a critical review of academic literature, institutional

reports, and policy documents to identify the shifting mechanisms of diplomatic engagement. Rather than pursuing a purely descriptive historical account, the study utilizes selected case studies as empirical illustrations to contextualize how digital diplomacy is operationalized in contemporary practice. The unit of analysis focuses on the strategic mechanisms through which both states and NSAs utilize digital platforms to construct narratives and exert influence. This multi-layered qualitative approach ensures a nuanced understanding of how technological advancements have reconfigured the international diplomatic landscape, providing a robust conceptual basis for evaluating the redistribution of influence in the digital sphere.

2. DEFINITION AND KEY OBJECTIVES OF DIGITAL DIPLOMACY

As a product of globalization and as a fruit of new public diplomacy, digital diplomacy is considered one of the defining trends of twenty-first-century diplomatic communication.¹ Digital diplomacy enables all subjects of international law to achieve their diplomatic objectives through the strategic use of information and communications technology (ICT), the internet, and social media.² In the contemporary era, many world leaders and diplomats conduct the vast majority of their official correspondence via email. Furthermore, the use of dedicated websites by ministries of foreign affairs (MFAs), embassies, and intergovernmental organizations (IGOs) has become standard practice. Similarly, social media has evolved into a vital diplomatic instrument, providing a platform for direct and unfiltered communication.³ While the number of social media platforms continues to expand, those most frequently utilized by both states and NSAs include X (formerly Twitter), Facebook, Instagram, YouTube, LinkedIn, and TikTok.⁴ Research into digital diplomacy reveals a wide variety of associated terminology, a multitude of prefixes and adjectives are used to describe the digitalization of diplomatic efforts or the role of the internet in public diplomacy. Ultimately, however, these terms serve as synonyms for the overarching concept of digital diplomacy.

¹ Rashica, V. (2018) The Benefits and Risks of Digital Diplomacy. *SEEU Review*, 13(1), p. 75.

² Rashica, V. (2024) *Diplomacia Digjitale në Teorinë dhe Praktikën e Diplomacisë së Shekullit Njëzet e Një*. Prishtinë: Botime Artini, p. 7.

³ Rashica, V. (2019) Digital diplomacy: aspects, approaches and practical use. *International Scientific Journal on European Perspectives*, 10(1), p. 25.

⁴ Lüfkens, M. (2024) *The DigiTips Social Media Rankings 2024: Governments and World Leaders on Social Media 2024*. [online] DigiTips. Available from: <https://digitips.ch/social-media-rankings-2024/> [Accessed 5 March 2026]

Digital diplomacy aims to leverage data from state institutions to advance foreign policy objectives through the systematic collection and analysis of information. This approach seeks to predict geopolitical outcomes, manage international relationships, and reduce strategic uncertainty. A core component of this practice is audience targeting via digital technologies and platforms, which allows policymakers and diplomats to integrate social media into their daily workflows, ranging from formal negotiations and representation to communication and policy analysis with a particular emphasis on managing emergencies and international crises. Furthermore, digital diplomacy serves to attract and utilize external expertise to advance national targets, addressing the redistribution of power in international relations and the emergence of complex challenges such as digital sovereignty, cybersecurity, data privacy, and e-commerce. These evolving dynamics have necessitated rigorous policy planning to navigate new types of conflicts and interdependencies. Ultimately, digital diplomacy also pursues an ideological goal, leveraging the inherent reach of the internet and social media to disseminate democratic values as a strategic effort to counter and minimize the influence of authoritarianism.⁵

3. TRACING THE EVOLUTION OF DIGITAL DIPLOMACY: FROM PUBLIC DIPLOMACY TO SOCIAL MEDIA ENGAGEMENT

3.1. THE DEVELOPMENT OF PUBLIC DIPLOMACY

3.1.1 Technological innovations in diplomacy: From the telegraph to television

The printing press was invented by German goldsmith Johannes Gutenberg in 1448. Before its invention, the majority of books were written and copied by hand. Consequently, hand-written books were expensive, and only the wealthy could afford them. Gutenberg created a device that would make it possible to print texts using movable blocks of letters and graphics. These blocks, used with paper, ink, and a press, would make it possible to print books much faster and more affordably than ever before.⁶ Furthermore, the printing press in the Renaissance also transformed diplomatic practices by eliminating ambiguities in diplomatic documents, as well as facilitating communication and the decision-making process.

⁵ Rashica, V. (2022) Is Digital Diplomacy Triumphant Over Political Diplomacy? *International Scientific Journal on European Perspectives*, 13(2), p. 55.

⁶ Massachusetts Institute of Technology. (n.d.) *Johann Gutenberg: Movable Type Printing Press* [online]. Available from: <https://lemelson.mit.edu/resources/johann-gutenberg> [Accessed 7 March 2026].

The late eighteenth century witnessed a pivotal technological breakthrough, the telegraph. The first mechanical version, the optical telegraph, was invented in France by Claude Chappe in 1792.⁷ Its emergence marked a significant turning point for examining the intersections between media and diplomacy. Following various experimental stages, electric telegraphy gained prominence in 1837, by 1866, the completion of the first successful transatlantic cable fundamentally altered the nature of international relations.⁸ British journalist Tom Standage aptly characterized this mid-nineteenth-century innovation as the “Victorian Internet”.⁹ Ultimately, the telegraph revolutionized diplomacy by streamlining communication and international cooperation, thereby enhancing coordination while necessitating more rapid decision-making processes.

In the late nineteenth century, the telephone emerged as a transformative yet often overlooked tool of modern diplomacy. It was Alexander Graham Bell, a Scottish engineer dedicated to teaching speech to the deaf, who integrated electromagnetism with a vibrating diaphragm to pioneer telephone technology in 1876.¹⁰ As the first device to enable real-time oral communication regardless of physical distance, it fundamentally altered diplomatic workflows. Specifically, the immediacy of the telephone strengthened the connection between envoys in the field and their home capitals, thereby reducing operational autonomy.¹¹ Furthermore, this direct contact fostered personal interactions and bypassed geographical barriers, allowing for more efficient crisis management and the resolution of urgent issues without the delays of traditional, lengthy diplomatic protocols.

At the dawn of the twentieth century, direct communication between a sending state's government and the population of a receiving state was strictly prohibited, as it was deemed a violation of national sovereignty. However, three pivotal developments in the first quarter of the century redefined diplomatic practice. The first was the rapid proliferation and immense popularity of the radio. The second was the geopolitical shift following the 1917 Bolshevik Revolution and the subsequent rise of the

⁷ Diplo. (2021) *The telegraph: How it changed diplomacy* [online]. Available from: <https://www.diplomacy.edu/histories/the-telegraph-how-it-changed-diplomacy/> [Accessed 5 March 2026]

⁸ Seib, P. (2016) *The Future of Diplomacy*. Cambridge: Polity Press, pp. 39-40.

⁹ Alexander, R. C. (ed.). (2021) *The Frontiers of Public Diplomacy: Hegemony, Morality and Power in the International Sphere*. New York: Routledge, pp. 28-29.

¹⁰ Digital Public Library of America. (n.d.) *The Invention of the Telephone* [online]. Available from: <https://dp.la/primary-source-sets/the-invention-of-the-telephone> [Accessed 5 March 2026]

¹¹ Seib, P. (2016) *op. cit.* pp. 41-43.

Nazi regime in 1933. The third involved the strategic use of radio by both regimes to broadcast ideologies beyond their borders. By addressing foreign audiences directly, Russia and Germany bypassed traditional governmental intermediaries, ushering in the era of public diplomacy.¹² Radio enabled states to reach foreign audiences by circumventing traditional diplomatic channels, allowing them to promote their image, values, and policies. During World War II and the Cold War, radio served as a propaganda instrument to counter the objectives of opponents. It possessed the power to reach audiences across borders, broadcasting news, analysis, and interviews on international issues. In fact, the origins of combating disinformation and promoting transparency can be traced back to these early uses of radio.

By the mid-1950s, radio faced increasing competition from an even more advanced technology, television. For diplomats, this marked another shift in the balance of influence. If visual broadcasts often contradicted official communications, the public was more likely, especially over time, to believe what they saw with their own eyes. Consequently, the role of diplomats as primary interpreters of world events underwent significant changes, their reports from the field sometimes contradicted the narratives presented by MFA officials on screen. Television had an even more profound impact on shaping public opinion regarding international affairs. Furthermore, the rapid dissemination of televised news created immense pressure on policymakers to react and act swiftly. Ultimately, through television, the media assumed a crucial role in shaping narratives and influencing international relations.

3.1.2 Defining public diplomacy: Terminology and concepts

The earliest use of the term “public diplomacy” is British and dates back to January 1856, from an article in the British newspaper “The London Times”. Meanwhile, the first American use of public diplomacy was in a citation from “The New York Times” newspaper in January 1871, reporting on a debate in the United States (US) Congress. During the First World War, the phrase “public diplomacy” was widely used to describe several new diplomatic practices. These ranged from public declarations of peace terms to the idealistic vision of US President Woodrow Wilson, expressed in his address to Congress proposing his “Fourteen Points” on January 8, 1918. However, many authors of that time preferred the expression “open diplomacy” for these practices, although “public diplomacy” had its admirers and it seemed

¹² Digital Diplomacy Blog. (n.d.) *What is Digital Diplomacy?*. Available from: <https://digdiplomacyblog.com/countries-on-twitter-and-facebook/> [Accessed 4 March 2026]

that the use of the French phrase “la diplomatie publique” gave it more value.¹³

According to American diplomat Edmund Gullion, public diplomacy deals with the influence of public attitudes on the formation and implementation of foreign policies. It encompasses dimensions of international relations beyond traditional diplomacy, including the cultivation of public opinion by governments in foreign states, the interaction of private interest groups across nations, and the reporting of foreign affairs. Furthermore, it involves communication between those with professional communication roles, such as diplomats and foreign correspondents, as well as the process of intercultural communication. The term “public diplomacy” gained prominence in 1965 due to a pressing need for such a concept in Washington, D.C., Gullion was the first to use the term in its modern sense.¹⁴ Since public diplomacy was seen as a synonym of propaganda, states have consistently gone to great efforts to emphasize the differences between the two terms. Propaganda and public diplomacy both aim to influence audiences, but they differ in their methods and goals. While propaganda involves the selective presentation of facts to promote a specific agenda with a hidden motive, public diplomacy aims to build understanding and trust by sharing accurate information.¹⁵

3.1.3 From classic to new public diplomacy: Key differences

The development of ICT and the media has fueled the public’s interest in information regarding government foreign policy, thereby enabling public opinion to influence the shaping of that policy. Consequently, foreign ministers and diplomats frequently appear before domestic and foreign audiences. In this manner, they promote their countries and garner international support while simultaneously representing, explaining, and defending their foreign policy to their home constituency.¹⁶ ICT provides instruments within the political sphere that, when combined with other tools, allow for the exertion and distribution of power and influence. American political scientist Joseph Nye defines power as “the ability to influence the behavior of others to obtain the results one wants,” arguing that there are three ways to achieve this: coercion through threats, inducement through

¹³ Snow, N. and Taylor, M. P. (eds.). (2008) *Routledge Handbook of Public Diplomacy*. 1st ed. New York: Routledge, pp. 19-20.

¹⁴ Snow, N. and Cull, J. N. (eds.). (2020) *Routledge Handbook of Public Diplomacy*. 2nd ed. New York: Routledge, p. 21.

¹⁵ Wolf, C. and Rosen, B. (2004) *Public Diplomacy: How to Think about and Improve it*. California: RAND Corporation, p. 3.

¹⁶ Jazbec, M. (2010) *Bazat e Diplomacisë*. Prishtinë: Kolegji Victory, p. 60.

payments, or attraction and persuasion. The first two methods constitute “hard power”, the use of military or economic force, whereas the third represents soft power.¹⁷

The end of the Cold War in 1991 resulted in the spread of democracy across many former communist countries, while facilitating increased public access to international information.¹⁸ The proliferation of various radio and television platforms introduced a new strategic asset for improving the global image of states. Public diplomacy was directly shaped by the forces of globalization and the ICT revolution. As a result, classical public diplomacy gave way to new public diplomacy, which remains one of the key instruments of soft power.

Dominant characteristics	Classic public diplomacy	New public diplomacy
Identity of international actor	State	State and non-state
Technological environment	Short wave radio, Print newspapers, Land-line telephones	Satellite, Internet, real-time news, Mobile telephones
Media environment	Clear line between domestic and international news sphere	Blurring of domestic and international news sphere
Source of approach	Outgrowth of political advocacy & propaganda theory	Outgrowth of corporate branding & network theory
Terminology	“International image”, “Prestige”	“Soft power”, “Nation Brand”
Structure of role	Top down, actor to foreign peoples	Horizontal, facilitated by actor
Nature of role	Targeted messaging	Relationship-building
Overall aim	The management of the international environment	The management of the international environment

Table 1: Differences between classic public diplomacy and new public diplomacy¹⁹

¹⁷ Seib, P. (ed.). (2009) *Toward a New Public Diplomacy: Redirecting U.S. Foreign Policy*. New York: Palgrave Macmillan, p. 4.

¹⁸ Golan, J. G., Yang, S. U. and Kinsey, F. D. (eds.). (2015) *International Public Relations and Public Diplomacy: Communication and Engagement*. New York: Peter Lang Publishing, p. 297.

¹⁹ Cull, J. N. (2009) *Public Diplomacy: Lessons from the Past*. Los Angeles: Figueroa Press, p. 14.

3.2.THE GROWING ROLE OF SOCIAL DIPLOMACY

3.2.1 The historical roots of social diplomacy

As a facet of public diplomacy, social diplomacy represents the skill of resolving difficult issues and complex problems through a specialized behavioral model of communication. It involves the ability to offer solutions in delicate situations with courtesy, demonstrating tact, wisdom, nobility, refinement, and ethics, thereby making others approve of one's points of view. By anchoring diplomacy as a social and relational practice, the concept of social diplomacy suggests that international politics is sustained by everyday social exchanges and the maintenance of a "social graph" of trust and connection. The origins of social diplomacy can be traced back to the seventeenth century and the reign of King Louis XIV of France, the longest-reigning monarch in European history. When France experienced the bitter civil war known as "La Fronde," Louis XIV sought to demonstrate his capability to lead. As a form of political propaganda, he began staging performances to convince the public of his leadership. In 1653, Louis XIV created his first dance performance, the "Ballet de la Nuit" (Ballet of the Night). This performance presented a metaphorical image of France in "darkness" until Louis XIV appeared as the light that would save the country and bring hope to his people.²⁰

3.2.2 Key elements of social diplomacy: NGOs, lobbying and informal communication

Postmodern diplomacy combines traditional functions such as interstate representation, negotiation, and the protection of interests with messaging and relationship-building between societies and groups. As a result, MFAs must learn to share the diplomatic space with think tanks, universities, non-governmental organizations (NGOs), and other groups engaged in international activities.²¹ NGOs play a crucial role in social diplomacy, and their number has grown spectacularly over the last century. These organizations can be local, national, or international and comprise individuals who have come together to promote common interests and

²⁰ Align Ballet Method Official Site. (n.d.) *Louis XIV and the Beginning of Ballet*. [online]. Available from: <https://alignballetmethod.com/louis-xiv-and-the-beginning-of-ballet/> [Accessed 7 March 2026]

²¹ Pisarska, K. (2016) *The Domestic Dimension of Public Diplomacy: Evaluating Success through Civil Engagement*. London: Palgrave Macmillan, p. 1.

ideals.²² NGOs generally undertake one of the following two forms of activity:

- Delivering basic services to vulnerable populations;
- Conducting policy advocacy and public campaigns to drive social and political change.

At the same time, NGOs have also become active in a wide range of more specialized roles, such as emergency response, democracy building, conflict resolution, human rights advocacy, cultural preservation, environmental activism, policy analysis, and information gathering and dissemination.²³ Furthermore, NGOs exert a powerful influence on diplomacy because by acting as advocates, mediators, and monitors, they play a major role in political decision-making and the promotion of international cooperation.

Lobbying encompasses any action designed to exert influence over the activities of government institutions. Effectively, it is the process of persuading decision-makers to adopt specific positions or policies. Since these actors often initially reject such proposals, the strategic essence of lobbying lies in shifting those positions toward a favorable consensus. Lobbying occurs at all three levels of government: local, state, and national. When developing a lobbying strategy, the following points should be considered:

- Environment, what is the change you are looking to make, what are the current policies, has anything been said about your case?;
- Outcome, what do you aim to achieve?;
- People who are in government or in the wider policy-making environment to be contacted, ministers, councillors, members of parliament and civil servants;
- Approach, how will you convince them that a change is needed, what do you need to be able to prove your case, what is your rationale and do you need to undertake an activity that increases political pressure on them?;
- Messages, showing what you are saying?;
- Your allies, are there other like-minded people who can offer support to your cause?;

²² Jr., Kegley, W. C. (2009) *Politikat Botërore: Tendenca dhe Transformimi*. bot. 12-të. Tiranë: UFO Press, pp. 182-183.

²³ Berridge, R. G. and Lloyd, L. (2012) *The Palgrave Macmillan Dictionary of Diplomacy*. 3d ed. London: Palgrave Macmillan, pp. 262-263.

- Media, can you run the campaign?;
- In general, in terms of the timelines you are working with, are there events that need to be considered?²⁴

The practice of lobbying is highly effective in diplomacy as it has the power to elevate a multitude of issues to the attention of policymakers and diplomats, thereby fostering increased focus and decisive action.

In political diplomacy, politicians and diplomats are required to adhere strictly to diplomatic protocol, characterized by formal exchange where the flow of information follows predetermined paths and appropriate channels. In contrast, social diplomacy transcends these protocols, relying on informal interaction where communication channels are unlimited and undefined. This informal approach is a natural and effective form of dialogue that enables individuals to discuss a wide array of issues. Its structure is bottom-up, originating with citizens and employees through social relations before ascending to senior leadership. While formal communication carries greater official weight, informal channels are notably faster and more time-efficient. In these settings, information moves freely, however, because it relies on individuals, it challenges the maintenance of secrecy. Ultimately, informal communication facilitates open dialogue, fosters trust between nations, and provides essential channels for exploring potential solutions during international crises.

3.3.E-DIPLOMACY: INTEGRATING DIGITAL TECHNOLOGIES IN DIPLOMACY

3.3.1 The use of email and the internet in modern diplomacy

In the final decade of the 20th century, the digital revolution opened a new dimension in international relations. The internet fundamentally transformed diplomacy by reshaping communication and access to global data, while simultaneously increasing transparency and accelerating the dissemination of news. This era introduced new forms of engagement, most notably e-diplomacy. Similarly, electronic mail (email) significantly impacted diplomatic practice by enabling the rapid exchange of documents, improving accessibility, and fostering transparency, all while remaining remarkably cost-effective compared to traditional tools. While the prefix “e-” (electronic) originally described the early commercialization of the internet, in a diplomatic context, e-diplomacy encompasses the innovative methods

²⁴ Thomson, S. and John, S. (2007) *Public Affairs in Practice: A Practical Guide to Lobbying*. London: Kogan Page Limited, pp. 39-40.

and strategies used to conduct international relations through the integration of ICT and the internet.

While the concept of e-diplomacy originated in Britain, the French term “la diplomatie numérique” spread alongside it. This French framework defined the operational areas of the MFA as “international digital challenges,” expanding traditional diplomatic activities through digital tools. These technologies were viewed not merely as means of transferring information, but as catalysts for the transformation of diplomatic practice.²⁵ The earliest practical developments in e-diplomacy occurred in 1992 at the Earth Summit in Rio de Janeiro, where civil society utilized email for the first time as a lobbying tool during international negotiations.²⁶ Subsequently, in January 1994, the Unit for Computer Applications in Diplomacy within the Mediterranean Academy of Diplomatic Studies organized a seminal workshop in collaboration with the United Nations (UN) Secretariat and the Maltese MFA.²⁷ This project, which aimed to integrate ICT tools into diplomacy, eventually evolved into DiploFoundation (Diplo). Founded by the governments of Malta and Switzerland in 2002, this international non-profit organization specializes in capacity development and research within the fields of digital diplomacy, internet governance, and technology policy.²⁸

3.3.2 E-diplomacy and counter-terrorism strategies

E-diplomacy continued to evolve rapidly during the early years of the 21st century, particularly in response to global security threats. Terrorism involves the intimidation or coercion of populations and governments through the threat or commission of violent acts, resulting in death, serious injury, or the taking of hostages.²⁹ Terrorist organizations have established an extensive online presence, utilizing messaging platforms, high-resolution imagery, videos, and digital publications to radicalize and

²⁵ France Diplomatie. (2015) *Diplomatie numérique*. [online]. Available from: <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/> [Accessed 6 March 2026]

²⁶ Diplo. (n.d.) *Digital Diplomacy* [online]. Available from: <https://www.diplomacy.edu/topics/digital-diplomacy/> [Accessed 7 March 2026]

²⁷ Diplo. (1994) *First workshop on computer applications in diplomacy* [online]. Available from: <https://www.diplomacy.edu/event/the-first-workshop/> [Accessed 7 March 2026]

²⁸ Diplo. (n.d.) *About Diplo* [online]. Available from: <https://www.diplomacy.edu/about-diplo/> [Accessed 6 March 2026]

²⁹ Office of the United Nations High Commissioner for Human Rights. (n.d.) *OHCHR and terrorism and violent extremism* [online]. Available from: <https://www.ohchr.org/en/terrorism> [Accessed 6 March 2026]

recruit individuals receptive to extremist ideologies.³⁰ E-diplomacy has proven to be a vital tool against this phenomenon by fostering cooperation among international actors. States and organizations have utilized digital platforms to disseminate counter-narratives, identify emerging threats, and coordinate specific security tactics. Furthermore, these digital efforts help promote a positive perception of global anti-terrorism initiatives, ensuring that accurate information counters extremist propaganda across the internet.

A significant portion of US diplomatic efforts is dedicated to fostering a positive national image, primarily through long-term initiatives such as educational and cultural exchanges. However, by 2008, the primary objective of US public diplomacy shifted toward creating a hostile environment for violent extremism. This was pursued through two main strategies: undermining extremist ideologies and encouraging youth toward productive alternatives to terrorism. Organizations such as Al-Qaeda and the Taliban became significant 21st-century threats by utilizing the internet to disseminate jihadist messages. Extremist leaders often exploited the identity crises of vulnerable young people, framing their cause as a compelling narrative that linked adventure to a doctrine of hatred and hysteria. The US concluded that the most effective way to achieve its objectives was through a new communicative approach, facilitated by the emergence of Web 2.0³¹ technologies. Consequently, the “Public Diplomacy 2.0” initiative was launched, designed to serve as an interactive platform for collaboration, mediation, and perception enabling a more dynamic process of both gathering and disseminating information.³²

3.3.3 The WikiLeaks scandal: Implications for e-diplomacy

WikiLeaks, a multinational media organization and associated library, was founded by Julian Paul Assange in 2006. It specializes in the analysis and publication of large datasets containing censored or restricted official material related to war, espionage, and corruption. Through contractual relationships and secure communication channels with more than 100 major media organizations worldwide, WikiLeaks secured significant negotiating power,

³⁰ Federal Bureau of Investigation. (n.d.) *Terrorism* [online]. Available from: <https://www.ohchr.org/en/terrorism> [Accessed 7 March 2026]

³¹ Web 2.0 refers to the second generation of the World Wide Web, characterized by increased user participation, social networking, and interactive content creation. It emphasizes user-generated content, collaboration, and the sharing of information, moving beyond the static, read-only experience of Web 1.0.

³² US Department of State. (2008) *Public Diplomacy 2.0: A New Approach to Global Engagement* [online]. Available from: <https://2001-2009.state.gov/r/us/2008/112605.htm> [Accessed 7 March 2026]

influence, and technical protection.³³ On November 28, 2010, WikiLeaks released more than 250,000 US State Department diplomatic cables sent to and from US embassies globally. This constituted the largest unauthorized disclosure of classified information in history, involving dispatches from over 250 American embassies and consulates. These documents revealed the inner workings of US diplomacy, showing how the US interacted with allies and adversaries by negotiating, pressuring, and at times harshly critiquing foreign leaders, all behind secret classifications that diplomats had assumed were secure.³⁴

The WikiLeaks scandal marked a turning point in modern diplomacy, undermining the principle of confidentiality and forcing states and international organizations to adopt urgent protective measures. In the aftermath of the leak, governments responded by implementing rigorous cybersecurity protocols and restricting data access for mid-level personnel to prevent similar breaches. Parallel to these technical measures, there was a notable rise in “apology diplomacy”, as world leaders were compelled to rebuild fractured trust through intensified bilateral engagements. International organizations, meanwhile, prioritized robust encryption for their communications and revised transparency policies to mitigate the risk of future disclosures. This scandal demonstrated that in the digital age, information is simultaneously an instrument of power and a critical vulnerability, necessitating a new equilibrium between public transparency and national security.

3.4.THE ERA OF SOCIAL MEDIA DIPLOMACY

3.4.1 Social media as a catalyst in the Arab Spring

The Arab Spring is widely considered the catalyst for the emergence of social media diplomacy. In the wake of these anti-government protests, MFAs, embassies, and diplomats recognized that events unfolding “offline” were increasingly being shaped “online.” Social media emerged as a suite of digital platforms capable of providing real-time insights into public sentiment, thereby facilitating more nuanced foreign policy analysis. On December 17, 2010, Mohamed Bouazizi, a young Tunisian street vendor, set himself on fire to protest police harassment. His death on January 4, 2011, became a viral symbol of resistance, sparking nationwide protests against socio-economic hardships and the authoritarian regime of President Zine El Abidine Ben Ali.

³³ WikiLeaks. (2015) *What is WikiLeaks* [online]. Available from: <https://wikileaks.org/What-is-WikiLeaks.html> [Accessed 7 March 2026]

³⁴ Leigh, D. (2010) *How 250,000 US embassy cables were leaked* [online]. The Guardian. Available from: <https://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked> [Accessed 7 March 2026]

While such acts might have previously gone unnoticed, the rapid expansion of Facebook in Tunisia, growing from a small user base to nearly two million, ensured that the event reached a critical mass. Ben Ali's 23-year rule ended ten days later when he fled to Saudi Arabia, making him the first Arab leader to be ousted by popular uprisings. These events inspired a wave of revolts across the Arab world as populations rose up against authoritarianism, corruption, and poverty.³⁵

The international response to the Arab Spring represented a sophisticated blend of digital diplomacy and tangible interventions. States and international organizations utilized social media to monitor human rights abuses in real-time and bypass state-controlled media through unfiltered communication with the public. Spurred by global pressure amplified by these platforms, the international community implemented significant measures, including military interventions, targeted economic sanctions, and the freezing of assets belonging to autocratic leaders. Furthermore, financial aid packages were increasingly linked to democratic conditionality. These coordinated actions contributed to the collapse of long-standing regimes and fostered a heightened level of civic awareness across the region.

3.4.2 Platform-specific diplomacy: Twitter, Facebook and Instagram

The term "Twitter diplomacy" (often referred to as Twiplomacy) involves the use of the Twitter platform, now rebranded as X, by government officials, diplomats, and high-level representatives for public diplomacy and official communication. While it is not a replacement for traditional methods, Twitter diplomacy has arguably transformed the foundational structure of diplomatic engagement, representing a systemic adaptation to emerging technologies. It has become a consolidated component of foreign policy agendas, allowing states to rethink their objectives and respond effectively to contemporary challenges.³⁶ Beyond enabling policymakers to engage with global audiences, Twitter diplomacy facilitates real-time crisis management and possesses the significant power to frame international narratives and issues.

The concept of "Facebook diplomacy" gained significant prominence during the Arab Spring in 2011. Since then, it has been utilized as a communication mechanism with foreign governments, an instrument of public diplomacy for engaging foreign populations, a consular channel

³⁵ Aljazeera Online. (2020) *What is the Arab Spring, and how did it start?* [online]. Available from: <https://www.aljazeera.com/news/2020/12/17/what-is-the-arab-spring-and-how-did-it-start> [Accessed 7 March 2026]

³⁶ Sandre, A. (2013) *Twitter for Diplomats*. Switzerland: DiploFoundation, pp. 27-28.

for maintaining contact with citizens abroad, and a medium for cultural promotion.³⁷ The importance of this platform within the digital diplomacy ecosystem was further underscored by the 2020 launch of a dedicated digital diplomacy guide for Facebook. Tailored specifically for MFAs, embassies, consulates, and diplomats, this guide aims to enhance their understanding of Facebook's features and content strategies to better achieve strategic diplomatic goals. Ultimately, Facebook diplomacy has enhanced public diplomacy by fostering spaces for direct citizen engagement and promoting national culture and values on a global scale.

The term "Instagram diplomacy" emerged to describe the strategic use of Instagram within the realm of public diplomacy. As the platform became a primary communication channel for younger demographics, diplomatic services adapted their outreach strategies to align with Instagram's emphasis on visual storytelling. This shift necessitated a focus on high-quality imagery and short-form video content to convey diplomatic messages effectively. Common practices in Instagram diplomacy include heads of state and MFAs sharing curated content of official visits, cultural summits, and high-level bilateral meetings.³⁸ This visual approach has not only enhanced global engagement and promoted national tourism and culture but has also fostered unique collaborations between official diplomats and key digital influencers. Furthermore, Instagram diplomacy facilitates the building of transnational relationships among citizens, thereby promoting a more grassroots form of international cooperation.

4. EXPLORING THE POTENTIAL OF DIGITAL DIPLOMACY

4.1. ENHANCING COOPERATION BETWEEN STATES AND NSAs

International politics in the 21st century involves a diverse array of actors, beyond sovereign states, these include IGOs, ethno-nationalist groups, multinational corporations, NGOs, transnational networks, and influential individuals.³⁹ NSAs actively participate in international conferences, lobby for specific policy frameworks, and can even initiate proceedings in international courts and tribunals. Furthermore, they are increasingly involved in the implementation of international law and the monitoring of compliance.⁴⁰ Although debates regarding the legal status of NSAs

³⁷ Diplo. (n.d.) *Facebook diplomacy* [online]. Available from: <https://www.diplomacy.edu/topics/facebook-diplomacy> [Accessed 7 March 2026]

³⁸ Diplo. (n.d.) *Instagram diplomacy* [online]. Available from: <https://www.diplomacy.edu/topics/instagram-diplomacy> [Accessed 7 March 2026]

³⁹ Mingst, A. K. (2008) *Bazat e Marrëdhënieve Ndërkombëtare*. Tiranë: Albanian Institute for International Studies, p. 343.

⁴⁰ Ryngaert, C. and Noortmann, M. (eds.). (2010) *Non-State Actor Dynamics in International Law: From Law-Takers to Law-Makers*. 1st ed. London: Routledge, pp. 1-5.

persist, their growing role and responsibilities reflect the profound impact of globalization. NSAs have emerged as central players in the global arena, often challenging traditional state authority. By leveraging global interconnectedness, vast economic resources, specialized expertise, and digital platforms, these actors possess the capacity to alter the course of international events and circumvent traditional diplomatic channels.

A fundamental advantage of digital diplomacy is the opportunity it creates to foster cooperation between states and NSAs. Beyond simple information sharing and engagement, social media and other digital platforms enhance transparency and build trust, elements crucial for mitigating misunderstandings and combating disinformation through the dissemination of accurate data. Digital diplomacy plays a vital role in addressing global challenges by providing a platform not only for policymakers but also for ordinary citizens to showcase their contributions. An exemplary case is that of Swedish climate activist Greta Thunberg. By leveraging digital tools, she transformed from a local activist into a global influencer, disrupting traditional media gatekeeping to engage world leaders directly and mobilize millions. Her approach utilizes social media to build a "glocalized" movement, effectively making the climate crisis locally relevant while simultaneously applying direct pressure on global policymakers.

Digital diplomacy fosters inclusive engagement for NSAs, even in volatile contexts marked by severe human rights violations. Following the Taliban's return to power in Afghanistan in 2021, the nation faced international isolation and crippling economic sanctions. This led to a critical "brain drain" as professionals, including doctors, engineers, and educators, fled the country. Amidst a media blackout, public executions, and the systemic exclusion of women from education and social platforms,⁴¹ the international community utilized digital channels to highlight the escalating crisis. A paradigmatic case of celebrity diplomacy⁴² in this context was demonstrated by American actress Angelina Jolie. Utilizing her platform and her experience as a Special Envoy for the UN High Commissioner for Refugees (UNHCR), Jolie shared a letter on Instagram from an anonymous Afghan girl detailing the suppression of her educational aspirations under the Taliban regime. By disseminating these firsthand accounts, Jolie amplified global awareness, advocated for gender equality, and ensured the crisis remained a priority

⁴¹ Amnesty International. (n.d.) *Afghanistan 2022* [online]. Available from: <https://www.amnesty.org/en/location/asia-and-the-pacific/south-asia/afghanistan/report-afghanistan/> [Accessed 6 March 2026]

⁴² Celebrity diplomacy is a form of public diplomacy, which refers to the practice of using famous individuals, such as actors, musicians, and other public figures, to promote political or social causes on a global scale.

on the international agenda. Furthermore, she mobilized public support for legislative efforts such as the Afghan Adjustment Act⁴³, demonstrating how digital influence can be channeled into concrete political advocacy for vulnerable populations.

Social media has emerged as a powerful instrument in countering terrorism and mitigating violent extremism. A landmark case is that of Colombia, where an unaffiliated citizen, Oscar Morales, utilized Facebook to challenge the terrorist organization known as the “Revolutionary Armed Forces of Colombia” (FARC). Morales, a computer technician by profession, spontaneously created a Facebook group that rapidly garnered over 400,000 members. Within just two months of its inception, this group, titled “One Million Voices Against FARC”, successfully orchestrated a global mobilization, drawing 12 million protesters to the streets across 190 cities worldwide.⁴⁴ Morales became a pioneer in digital diplomacy, demonstrating how individual citizens can leverage social media to mobilize global public opinion and significantly influence international relations, bypassing traditional state-led diplomatic channels.

4.2. THE FACILITATION OF INTERNATIONAL RECOGNITION FOR SMALL STATES

Digital diplomacy does not necessarily demand heavy financial investment, on the contrary, it is often a cost-effective strategy that facilitates fiscal optimization. The low barriers to entry and minimal operational costs of social media, relative to traditional diplomatic methods, make it an attractive instrument for embassies and government offices facing budget constraints and increasing demands for public engagement. Therefore, digital tools empower small states to enhance their international visibility and global reach more affordably than ever before. In the digital age, these states have gained unprecedented opportunities to counter disinformation and disseminate accurate narratives. Furthermore, digital diplomacy allows small states to project their interests more effectively within multilateral frameworks. It also serves as a vital component of economic diplomacy, enabling small nations to leverage digital platforms to promote trade, attract foreign investment, and stimulate tourism.

The Republic of Kosovo serves as a paradigmatic example of how digital diplomacy can empower small states. Having declared independence in 2008

⁴³ The Afghan Adjustment Act is a bipartisan, proposed US legislation, designed to create a pathway to lawful permanent resident status for thousands of Afghan evacuees.

⁴⁴ Maastricht University. (n.d.) *Oscar Morales, 21st century soldier* [online]. Available from: <http://www.maastrichtuniversity.nl/events/oscar-morales-21st-century-soldier> [Accessed 6 March 2026]

and secured de jure recognition⁴⁵ from 121 nations,⁴⁶ Kosovo demonstrates that a small state can establish a robust international presence even without a two-thirds majority in the UN General Assembly (UNGA), provided it effectively navigates the digital landscape. In September 2013, the “Digital Kosovo” initiative was launched, which represents an innovative model of grassroots digital diplomacy that played a pivotal role in institutionalizing Kosovo’s international subjectivity within the global virtual infrastructure. By mobilizing social capital and utilizing technology as an advocacy tool, this platform successfully bypassed the barriers of formal political recognition, securing the state’s integration into hundreds of international technological, financial, and tourism platforms. This process not only mitigated “digital isolation” for citizens and businesses but also reshaped the international narrative surrounding Kosovo, positioning it as a proactive actor in modern public diplomacy. This effort yielded significant results, in 2013, the Turkish public diplomacy journal “Yeni Diplomasi” ranked Kosovo fourth globally for digital diplomacy excellence, trailing only the United Kingdom (UK), the US, and Israel.⁴⁷ This achievement underscores how strategic digital engagement can compensate for traditional diplomatic hurdles and enhance a nation’s global legitimacy.

4.3. DATA EMBASSY AND THE PROTECTION OF NATIONAL DIGITAL INFRASTRUCTURE

A primary priority for subjects of international law is the enhancement of cybersecurity, a goal increasingly supported by the implementation of data embassies. This concept involves a secure infrastructure of servers located in a host country that stores critical data under the direct jurisdiction and sovereignty of another nation⁴⁸. The data embassy represents a pioneering framework from intergovernmental, legal, and technical perspectives. It is strategically grounded in specific articles of the Vienna Convention on

⁴⁵ According to international law de jure recognition is permanent and full recognition, which includes all relations with the new state. It has retroactive value because it applies from the moment the state was actually created and cannot be withdrawn even if the recognized state has not fulfilled the obligation assumed upon recognition.

⁴⁶ Ministry of Foreign Affairs and Diaspora of the Republic of Kosovo. (n.d.) *List of recognitions* [online]. Available from: <https://mfa-ks.net/lista-e-njohjeve/> [Accessed 6 March 2026]

⁴⁷ Ministry of Foreign Affairs and Diaspora of the Republic of Kosovo. (n.d.) *Public Diplomacy and Digital Diplomacy - Digital Diplomacy* [online]. Available from: <http://www.mfa-ks.net/?page=2>, 219 [Accessed 6 March 2026]

⁴⁸ Rashica, V. (2024) Data Embassy in the European Union: The Digital Diplomacy. In: David Ramiro Troitiño (ed.) *E-Governance in the European Union: Strategies, Tools, and Implementation*. Switzerland: Springer Nature, p. 90.

Diplomatic Relations (VCDR), extending traditional diplomatic immunities to the digital realm as follows:

- Article 24 specifies that the archives and documents of the diplomatic mission of the sending state, including electronic ones, are inviolable by the receiving state;
- The first paragraph of Article 22 stipulates that the receiving state must take all necessary steps to protect the premises of the diplomatic mission of the sending state from any kind of interference or damage. The inviolability of diplomatic premises extends to computers, printers, and other digital objects located on the premises of the mission;
- Diplomatic law states that diplomatic missions enjoy the right to free, unmonitored, unimpeded communication, without surveillance or interference.⁴⁹

Estonia, where 99% of public services are accessible online 24/7, was the first nation to pioneer the concept of a data embassy.⁵⁰ The country's digital strategy was fundamentally shaped by its experience as the target of a large-scale cyber offensive in 2007. During this incident, government portals, ministries, media outlets, and financial institutions were overwhelmed by a massive Distributed Denial of Service (DDoS) attack.⁵¹ While the attacks caused economic and logistical disruption, they also highlighted Estonia's resilience and technical proficiency in cyber defense.⁵² This watershed moment provided the impetus for ensuring digital continuity through a sovereign data infrastructure located outside national borders.⁵³ As a result, Estonia and Luxembourg established a bilateral agreement in 2015, signed in 2017, to host a secure data center in Luxembourg. Although not a traditional diplomatic mission, this data embassy remains under the exclusive control of Estonia and enjoys the same diplomatic inviolability and

⁴⁹ Rashica, V. (2025) *Data embassies: Protecting nations in the cloud* [online]. Diplo. Available from: <https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/> [Accessed 6 March 2026]

⁵⁰ E-Estonia. (n.d.) *e-Governance: Data Embassy* [online]. Available from: <https://e-estonia.com/solutions/e-governance/data-embassy/> [Accessed 6 March 2026]

⁵¹ Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

⁵² NATO Strategic Communications Centre of Excellence. (n.d.). *2007 cyber attacks on Estonia* [online]. Available from: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf [Accessed 6 March 2026]

⁵³ Grand Duchy of Luxembourg. (n.d.) *E-embassies in Luxembourg: E-embassies ensure IT security and diplomatic protection* [online]. Available from: <https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html> [Accessed 6 March 2026]

immunity as a physical embassy. Luxembourg was selected as the host for this inaugural project due to its advanced technological capacity and robust digital infrastructure.⁵⁴

5. CONCLUSION

The evolution of digital diplomacy, analyzed through a conceptual qualitative methodology encompassing document analysis and case studies, demonstrates that technological advancements have initiated a new paradigm in international relations. This research confirms that technological milestones, from historical developments like the telegraph and radio to contemporary social media platforms, have fundamentally reconfigured diplomatic practices by enabling new forms of interaction and amplifying the influence of both states and NSAs.

In comparison with existing literature, the findings of this study strongly align with the “soft power” framework established by Joseph Nye, reinforcing the argument that digital engagement has become a primary vehicle for attraction and persuasion in the 21st century. Furthermore, the results support Cull’s (2009) observations regarding the transition from classic public diplomacy toward a horizontal model centered on relationship-building and real-time crisis management.

However, this study offers a more specialized perspective that diverges from traditional, state-centric diplomatic theories. While classical approaches, such as those discussed by Jazbec (2010), emphasize formal protocols and the state’s monopoly on international communication, the findings illustrate a significant decentralization of influence. Cases such as Oscar Morales and Greta Thunberg demonstrate how digital tools allow individual actors to bypass traditional diplomatic channels to mobilize global opinion and influence international relations. Moreover, while much of the literature focuses on the systemic vulnerabilities of the digital age, exemplified by the WikiLeaks scandal, this paper provides a constructive counter-narrative by highlighting the “data embassy” model pioneered by Estonia. This concept represents a critical evolution in diplomatic law, applying the VCDR to ensure digital continuity and national resilience

Ultimately, digital diplomacy emerges as a transformative force that does not merely supplement traditional practice but redefines its very infrastructure. By institutionalizing digital subjectivity for small states like

⁵⁴ See Rashica, V. (2025) *Data embassies: Protecting nations in the cloud* [online]. Diplo. Available from: <https://www.diplomacy.edu/blog/data-embassies-protecting-nation-s-in-the-cloud/>

the Republic of Kosovo, it provides a strategic mechanism for international equity and integration within the global virtual landscape.

LIST OF REFERENCES

- [1] Alexander, R. C. (ed.). (2021) *The Frontiers of Public Diplomacy: Hegemony, Morality and Power in the International Sphere*. New York: Routledge.
- [2] Align Ballet Method Official Site. (n.d.) *Louis XIV and the Beginning of Ballet* [online]. Available from: <https://alignballetmethod.com/louis-xiv-and-the-beginning-of-ballet/> [Accessed 7 March 2026].
- [3] Aljazeera Online. (2020) *What is the Arab Spring, and how did it start?* [online]. Available from: <https://www.aljazeera.com/news/2020/12/17/what-is-the-arab-spring-and-how-did-it-start> [Accessed 7 March 2026].
- [4] Amnesty International. (n.d.) *Afghanistan 2022* [online]. Available from: <https://www.amnesty.org/en/location/asia-and-the-pacific/south-asia/afghanistan/report-afghanistan/> [Accessed 6 March 2026].
- [5] Cull, J. N. (2009) *Public Diplomacy: Lessons from the Past*. Los Angeles: Figueroa Press.
- [6] Digital Diplomacy Blog. (n.d.) *What is Digital Diplomacy?* [online]. Available from: <https://digdipblog.com/countries-on-twitter-and-facebook/> [Accessed 4 March 2026].
- [7] Digital Public Library of America. (n.d.) *The Invention of the Telephone* [online]. Available from: <https://dp.la/primary-source-sets/the-invention-of-the-telephone> [Accessed 5 March 2026].
- [8] Diplo. (n.d.) *About Diplo*. [online]. Available from: <https://www.diplomacy.edu/about-diplo/> [Accessed 6 March 2026].
- [9] Diplo. (n.d.) *Digital Diplomacy* [online]. Available from: <https://www.diplomacy.edu/topics/digital-diplomacy/> [Accessed 7 March 2026].
- [10] Diplo. (n.d.) *Facebook diplomacy* [online]. Available from: <https://www.diplomacy.edu/topics/facebook-diplomacy> [Accessed 7 March 2026].
- [11] Diplo. (1994) *First workshop on computer applications in diplomacy* [online]. Available from: <https://www.diplomacy.edu/event/the-first-workshop/> [Accessed 7 March 2026].
- [12] Diplo. (n.d.) *Instagram diplomacy* [online]. Available from: <https://www.diplomacy.edu/topics/instagram-diplomacy> [Accessed 7 March 2026].
- [13] Diplo. (2021) *The telegraph: How it changed diplomacy* [online]. Available from: <https://www.diplomacy.edu/histories/the-telegraph-how-it-changed-diplomacy/> [Accessed 5 March 2026].

- [14] E-Estonia. (n.d.) *e-Governance: Data Embassy* [online]. Available from: <http://e-estonia.com/solutions/e-governance/data-embassy/> [Accessed 6 March 2026].
- [15] Federal Bureau of Investigation. (n.d.) *Terrorism* [online]. Available from: <http://www.ohchr.org/en/terrorism> [Accessed 7 March 2026].
- [16] France Diplomatie. (2015) *Diplomatie numérique* [online]. Available from: <http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/> [Accessed 6 March 2026].
- [17] Golan, J. G., Yang, S. U. and Kinsey, F. D. (eds.). (2015) *International Public Relations and Public Diplomacy: Communication and Engagement*. New York: Peter Lang Publishing.
- [18] Grand Duchy of Luxembourg. (n.d.) *E-embassies in Luxembourg: E-embassies ensure IT security and diplomatic protection* [online]. Available from: <https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html> [Accessed 6 March 2026].
- [19] Jazbec, M. (2010) *Bazat e Diplomacisë*. Prishtinë: Kolegji Victory.
- [20] Jr., Kegley, W. C. (2009) *Politikat Botërore: Tendencat dhe Transformimi*. bot. 12-të. Tiranë: UFO Press.
- [21] Leigh, D. (2010) *How 250,000 US embassy cables were leaked* [online]. The Guardian. Available from: <https://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked> [Accessed 7 March 2026].
- [22] Lüfkens, M. (2024) *The DigiTips Social Media Rankings 2024: Governments and World Leaders on Social Media 2024* [online]. DigiTips. Available from: <https://digitips.ch/social-media-rankings-2024/> [Accessed 5 March 2026].
- [23] Maastricht University. (n.d.) *Oscar Morales, 21st century soldier* [online]. Available from: <https://www.maastrichtuniversity.nl/events/oscar-morales-21st-century-soldier> [Accessed 6 March 2026].
- [24] Massachusetts Institute of Technology. (n.d.) *Johann Gutenberg: Movable Type Printing Press* [online]. Available from: <https://lemelson.mit.edu/resources/johann-gutenberg> [Accessed 7 March 2026].
- [25] Mingst, A. K. (2008) *Bazat e Marrëdhënieve Ndërkombëtare*. Tiranë: Albanian Institute for International Studies.
- [26] Ministry of Foreign Affairs and Diaspora of the Republic of Kosovo. (n.d.) *List of recognitions* [online]. Available from: <https://mfa-ks.net/lista-e-njohjeve/> [Accessed 6 March 2026].

- [27] Ministry of Foreign Affairs and Diaspora of the Republic of Kosovo. (n.d.) *Public Diplomacy and Digital Diplomacy - Digital Diplomacy* [online]. Available from: <http://www.mfa-ks.net/?page=2,219> [Accessed 6 March 2026].
- [28] NATO Strategic Communications Centre of Excellence. (n.d.). *2007 cyber attacks on Estonia* [online]. Available from: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf [Accessed 6 March 2026].
- [29] Office of the United Nations High Commissioner for Human Rights. (n.d.) *OHCHR and terrorism and violent extremism* [online]. Available from: <https://www.ohchr.org/en/terrorism> [Accessed 6 March 2026].
- [30] Pisarska, K. (2016) *The Domestic Dimension of Public Diplomacy: Evaluating Success through Civil Engagement*. London: Palgrave Macmillan.
- [31] Rashica, V. (2025) *Data embassies: Protecting nations in the cloud* [online]. Diplo. Available from: <https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/> [Accessed 6 March 2026].
- [32] Rashica, V. (2024) *Data Embassy in the European Union: The Digital Diplomacy*. In: David Ramiro Troitiño (ed.) *E-Governance in the European Union: Strategies, Tools, and Implementation*. Switzerland: Springer Nature, pp. 87-102.
- [33] Rashica, V. (2019) *Digital diplomacy: aspects, approaches and practical use*. *International Scientific Journal on European Perspectives*, 10(1), pp. 21-39.
- [34] Rashica, V. (2024) *Diplomacia Digjitale në Teorinë dhe Praktikën e Diplomacisë së Shekullit Njëzet e Një*. Prishtinë: Botime Artini.
- [35] Rashica, V. (2022) *Is Digital Diplomacy Triumphant Over Political Diplomacy?*. *International Scientific Journal on European Perspectives*, 13(2), pp. 47-67.
- [36] Rashica, V. (2018) *The Benefits and Risks of Digital Diplomacy*. *SEEU Review*, 13(1), pp. 75-89.
- [37] Ryngaert, C. and Noortmann, M. (eds.). (2010) *Non-State Actor Dynamics in International Law: From Law-Takers to Law-Makers*. 1st ed. London: Routledge.
- [38] Sandre, A. (2013) *Twitter for Diplomats*. Switzerland: DiploFoundation.
- [39] Seib, P. (2016) *The Future of Diplomacy*. Cambridge: Polity Press.
- [40] Seib, P. (ed.). (2009) *Toward a New Public Diplomacy: Redirecting U.S. Foreign Policy*. New York: Palgrave Macmillan.
- [41] Snow, N. and Cull, J. N. (eds.). (2020) *Routledge Handbook of Public Diplomacy*. 2nd ed. New York: Routledge.
- [42] Snow, N. and Taylor, M. P. (eds.). (2008) *Routledge Handbook of Public Diplomacy*. 1st ed. New York: Routledge.
- [43] Thomson, S. and John, S. (2007) *Public Affairs in Practice: A Practical Guide to Lobbying*. London: Kogan Page Limited.

- [44] US Department of State. (2008) *Public Diplomacy 2.0: A New Approach to Global Engagement* [online]. Available from: <https://2001-2009.state.gov/r/us/2008/112605.htm> [Accessed 7 March 2026].
- [45] WikiLeaks. (2015) *What is WikiLeaks* [online]. Available from: <https://wikileaks.org/What-is-WikiLeaks.html> [Accessed 7 March 2026].
- [46] Wolf, C. and Rosen, B. (2004) *Public Diplomacy: How to Think about and Improve it*. California: RAND Corporation.

DOI 10.5817/MUJLT2025-40800

LEGAL AND REGULATORY COMPLIANCE CHALLENGES FOR EQUITY TOKEN SECONDARY MARKET OPERATORS IN THE EUROPEAN UNION

by

JAN WITTLIN *

As equity tokenization using blockchain-based distributed ledgers and tokens is trying to gain traction in multiple jurisdictions, the need for compliant, reliable and scalable secondary markets has become urgent. Forming a vital component of the overall venture financing value chain exchanges and other secondary market trading facilities are necessary to provide adequate levels of liquidity, investor confidence and market access to make the tokenization value proposition viable. In contrast to cryptocurrencies and utility tokens used for Initial Coin Offering (ICO) fundraising equity tokens are classified legally in the European Union broadly as financial instruments and specifically as securities invoking extensive compliance requirements not only for the issuer of the equity token and/or primary market issuance platform, but in particular for secondary market operators. The objective of this article is to identify key legal and compliance challenges impacting operation of these secondary markets and their ability to support a viable tokenization value chain. While research questions are analyzed from a European Union-level perspective, specific examples from the jurisdictions of Luxembourg, Germany, Liechtenstein, Estonia and Poland are investigated in order to identify root causes of deficiencies and potential observations and recommendations for future European developments in this highly competitive and globalized industry. Quantitative overview of key relevant market players is also attempted with the objective of substantiation of qualitative observations and conclusions.

* dr Jan Wittlin, CFE, CISA, CISSP, CIA, PMP; Koźmiński University, Business Law and Risk Management Unit, Warsaw, Poland; E-mail: jwittlin@kozminski.edu.pl; ORICD: 0000-0002-2880-783X

KEY WORDS

Tokenization, Blockchain, Cryptoassets, Exchanges, Securities, Trading

1. INTRODUCTION

The emergence of equity tokens, which are digital representations of traditional equity-type financial instruments issued and traded on blockchain technology, represents a significant innovation in the financial ecosystem offering opportunities to enhance efficiency, improve access to funding and investment opportunities as well as reduce transactional costs and barriers in capital markets.¹ However, the actual realization of these benefits heavily depends on the development and robustness of secondary markets. Featuring trading of these securities post-issuance plays a pivotal role in fostering liquidity, market efficiency and investor confidence, providing a vital component of the overall business viability of security token offerings.²

The highly regulated nature of equity tokens, derived from underlying regulatory requirements for securities in general, imposes particular compliance challenges for operators of secondary markets. These challenges are amplified by the still incomplete harmonization of capital markets regulations in the European Union (EU)³ and remaining uncertainties concerning the nature and regulatory implications of at least some classes of digital assets. This article focusses on an analysis of the current state of the compliance requirements for secondary market platforms enabling trading in equity tokens in the EU, with particular attention given to the jurisdictions of Luxembourg, Germany, Liechtenstein, Estonia and Poland and attempts to identify potential for regulatory and/or organizational improvements. The scope is centered around some specific relevant research questions:

- what are the key elements constituting the regulatory landscape and licensing requirements of secondary market operators for equity tokens on the level of the EU and a selection of domestic legislations?

¹ Garrido, J. M. (2023) Digital Tokens: A Legal Perspective. *IMF Working Papers*, 151, p. 7

² Kreppmeier, J. and Laschinger, R. (2023) Signaling in the Market for Security Tokens, *Journal of Business Economics*, 93. Available from: <https://doi.org/10.1007/s11573-023-01175-3> [Accessed 3 January 2025], p. 1

³ For the purpose of this article whenever the EU will be mentioned the countries of the European Economic Area (EEA) should be considered as well; see *Agreement on the European Economic Area - Final Act - Joint Declarations - Declarations by the Governments of the Member States of the Community and the EFTA States - Arrangements - Agreed Minutes - Declarations by one or several of the Contracting Parties of the Agreement on the European Economic Area*, 3 January 1994 (Official Journal L 001 , 03/01/1994 P. 0003 - 0036). Available from: https://eur-lex.europa.eu/eli/agree_international/1994/1/oj/eng, p. 3.

- How are key objectives of secondary markets, in particular regarding liquidity and market access enablement impacted by regulatory constraints?
- How is cross-border operation of secondary market platforms and exchanges regulated in terms of additional compliance requirements?

The research questions under consideration are of particular importance as they directly capture the regulatory, functional, and cross-border dynamics shaping the viability of equity token secondary markets in the EU. First, clarifying the regulatory landscape and licensing requirements is essential, since Directive on Markets in Financial Instruments (MiFID II),⁴ and national instruments impose heterogeneous compliance obligations that determine whether operators can establish and maintain compliant market infrastructures.⁵ Second, analyzing how regulatory constraints affect liquidity and access is essential, since robust investor protection often conflicts with the need to achieve sufficient trading volume and cross-platform interoperability, thereby influencing the success of tokenization as a financing tool.⁶ Finally, examining cross-border compliance requirements, particularly under MiFID II passporting and the DLT Pilot Regime,⁷ is indispensable to understand whether platforms can scale beyond fragmented domestic markets and achieve the pan-European integration necessary to compete globally.⁸

While focusing on the topics indicated above the author has consciously excluded from the scope of this article questions related to issuance and primary offerings of equity tokens as well as custody of crypto assets; these have been addressed in separate research papers.

⁴ Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU. *Official Journal of the European Union* (OJ L 173, 12.6.2014) 12 June. Available from: <http://data.europa.eu/eli/dir/2014/65/oj>

⁵ Marjosola, H. (2022) Security Tokens and the Future of EU Securities Law: Rethinking the Harmonisation Project, *University of Helsinki Faculty of Law Legal Studies Research Paper Series*, 70 (2021). Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897849#, p. 10

⁶ OECD. (2020) The Tokenisation of Assets and Potential Implications for Financial Markets, *OECD Blockchain Policy Series*, 2020, Available from: www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm [Accessed 3 January 2025], p. 20

⁷ Regulation 2022/858 of the European Parliament and Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (Pilot Regime) and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU. *Official Journal of the European Union* (PE/88/2021/REV/2) 2 June. Available from: <http://data.europa.eu/eli/reg/2022/858/oj>

⁸ Jiménez-Gómez, B. (2023) Distributed Ledger Technology in Financial Markets. The European Union Experiment, *Cuadernos de Derecho Transnacional*, 15 (2), p. 671

2. THE REGULATORY LANDSCAPE

Equity tokens should be considered as a subset of security tokens, specifically representing fractional ownership of an incorporated business entity.⁹ While their substance is equal to that of traditional securities, the use of blockchain-based distributed ledger technology (DLT) architecture promises additional features such as fractional ownership, global reach, reduced transaction costs and enhanced functionality thanks to smart contracts.¹⁰ Due to their nature equity tokens broadly fall under the definition of securities under MiFID II, which implies licensing and compliance requirements for any entity enabling trading in them on a secondary market.

Although being particularly relevant for primary market-level equity token issuance it should be noted that securities in general require entry into a central securities depository (CSD) and/or a physical certificate.¹¹ The resulting requirement of integration with “conventional” registers such as Clearstream or Euroclear, not to mention physical certificates, would greatly inhibit blockchain-only operation of equity tokenization.¹² Recent regulatory changes such as e.g. Electronic Securities Act (eWpG) in Germany¹³ or Blockchain II Law in Luxembourg¹⁴ have enabled a DLT-based fulfillment of the securities registration obligation paving the way for effective end-to-end issuance and trading environments.

⁹ Nassr, I. (2021) Understanding the tokenization of assets in financial markets, *OECD Going Digital Toolkit Notes*, 19. Available from: <https://doi.org/10.1787/c033401a-en> [Accessed 3 January 2025], p. 26; See also Lambert, T. et al. (2021) Security token offerings, *Small Business Economics*, 59. Available from: <https://doi.org/10.1007/s11187-021-00539-9> [Accessed 3 January 2025], p. 4

¹⁰ As explained by J. M. Garrido: “Through smart contracts, it is possible to include the complex suite of rights that a shareholder has, for instance. In this way, a whole contractual relationship or the whole status of a shareholder can be included in the token. This overcomes the limits of literality: every acquirer of a token can know exactly the contents of all the rights attached to the instrument.” Garrido, J. M. (2023), *op.cit.* p. 21

¹¹ Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories (CSDR) and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012. *Official Journal of the European Union* (OJ L 257) 28 August. Available from: <http://data.europa.eu/eli/reg/2014/909/oj>

¹² See (2024). *Building the Digital Asset Securities Ecosystem Digital Asset Securities Control Principles: a framework for adoption, An Industry Paper from DTCC, Clearstream, and Euroclear with the collaboration of BCG.* [online] DTCC. Available from: <https://www.dtcc.com/-/media/DASCPWhitePaper.pdf> [Accessed 3 January 2025]

¹³ *Electronic Securities Act 2021*, Germany. Bundesgesetzblatt. In: German. p. 1423

¹⁴ *Law of 22 January 2021 amending the law of 5 April 1993 on the financial sector and the law of 6 April 2013 on dematerialised securities 2021*, Luxembourg: Mémorial A 2021, No. 43. In: Luxembourgish

Security token regulations at EU-level under MiFID II are complemented by provisions of the Markets in Crypto-Assets Regulation (MiCA),¹⁵ which introduces standardized licensing requirements for Crypto-asset Service Providers (CASPs), ensuring a harmonized approach to risk management, investor protection, and operational resilience. Although this dual framework under MiFID II and MiCA allows trading platforms to cover a broader range of tokens while maintaining regulatory certainty, it does not have applicability in the specific context of equity tokens, which are outside the scope of MiCA.¹⁶

The classification of equity tokens indicated above has significant implications for the licensing requirements for centralized secondary market operators. Unlike exchanges listing cryptocurrencies and utility tokens used in ICOs that were able to operate for prolonged periods without any regulatory approvals or supervision,¹⁷ trading venues for equity tokens fall in the EU in a complex regulatory framework. As already indicated above, the licensing approach on a European level is being primarily shaped by MiFID II provisions, followed by domestic financial services law. The Multilateral Trading Facility (MTF) license¹⁸ would be the most comprehensive formula of operation for equity token secondary markets¹⁹ bringing together multiple third-party buying and selling interests. MTFs operate under non-discretionary rules providing an equal playing field on which trading interests interact and transactions occur based on established protocols. Optimized for high-volume trading of standardized instruments MTFs can provide a secondary market for equity-like security tokens comparable to “conventional” stock exchanges.²⁰ However, MTFs have extensive

¹⁵ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA), and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. *Official Journal of the European Union* (PE/54/2022/REV/1) 9 June. Available from: <http://data.europa.eu/eli/reg/2023/1114/oj>

¹⁶ MiCA, *Op. cit.* Art. 2, p. 2(a)

¹⁷ At present most of their activities do fall under the scope of MiCA

¹⁸ MiFID II, *Op. cit.* Art. 4, p. 1(22)

¹⁹ Nägele, T. (2020) *Secondary Market for Security Tokens — The need for a new regulatory approach at the European Union level* [online] Medium. Available from: <https://tokencontainermodel.com/secondary-market-for-security-tokens-the-need-for-a-new-regulatory-approach-at-the-european-e922e4ca04> [Accessed 3 January 2025]

²⁰ While Organized Trading Facility (OTF) licenses share some of the trading venue features applicable to tokenized financial instruments, their specific discretionary, tailored trading character and distinct regulatory requirements make them unsuitable for operating a tokenized securities secondary market, see Review and analysis of the application of financial regulations to security tokens. See Autorité des Marchés Financiers. (2020) *Review and analysis of the application of financial regulations to security tokens*. Available from: <https://www.amf-france.org/sites/institutionnel/files/private/2020-10/legal-analysis-security-tokens-amf-en.pdf> [Accessed 3 January 2025]

obligations related to market surveillance,²¹ transparency²² and ensuring fair access to their platforms²³ that have to be met prior to authorization as a trading venue, a process that has proven to be both time-consuming and challenging for potential equity token secondary markets.²⁴ Meeting these obligations enabling actual trading of equity tokens has proven to be achievable for special purpose entities of existing stock exchange such as NXchange operating as part of the Amsterdam Stock Exchange.²⁵ It should be underscored here that MTFs are limited in their trading scope to specific asset types – in the context of this discussion the issue of a secondary market specifically for equity tokens should not be confused with MTFs already authorized for trading in crypto assets and/or their derivatives, such as e.g. Boerse Stuttgart Digital Exchange²⁶ or Nomisma.²⁷

An illustrative case study of how current MiFID II implementation practices may undermine the development of pan-European security token exchanges can be observed recently in Germany, where retail-oriented trading venues have been structured to operate formally as MTFs while relying in practice on a single market maker for order execution.²⁸ Such arrangements might raise questions about compliance with the MiFID II requirement that multilateral systems bring together multiple third-party buying and selling interests under non-discretionary rules, thereby ensuring

²¹ MiFID II, *Op. cit.* Art. 18, p. (5)

²² MiFID II, *Op. cit.* Art. 18, p. (2 and 3)

²³ MiFID II, *Op. cit.* Art. 18, p. (1)

²⁴ E.g. as can be seen in the case of BlockTrade; the company initiated a licensing process for MTF license with FMA in Liechtenstein, however discontinued it; as of 2025 operating currently under Virtual Asset Service Provider (VASP) under MiCA without trading in security tokens in scope

²⁵ See statement by M. Evertsz: *“With Nxchange positioned in Europe as the place to invest and trade alternative assets on a Regulated Market, taking on a fully established private issuance platform that can deliver the experience that our Nxchange users have come to expect was a natural fit for us.”* News Desk. (2021) *Nxchange securities token exchange acquires Bondex for tokenized shared issuance*, [online] Available from: <https://www.unlock-bc.com/news/2021-05-04/nxchange-securities-token-exchange-acquires-bondex-for-tokenized-shared-issuance/> [Accessed 3 January 2025]

²⁶ See statement by Boerse Stuttgart: *“Boerse Stuttgart Digital: the first regulated exchange for trading digital assets in Europe, with BaFin (Federal Financial Supervisory Authority) licensed custody by Boerse Stuttgart Digital Custody GmbH”* Boerse Stuttgart. (2025) *Boerse Stuttgart Digital Exchange: Multilateral Trading Facility (MTF)*, [online] Available from: <https://www.bsdigital.com/en/services/multilateral-trading-facility-mtf/> [Accessed 3 January 2025]

²⁷ Active 2020-2022, see Bossi, P. (2020) *Nomisma’s MiFID II License For A Blockchain-Based MTF*, [online] GLC, Available from: <https://globallegalchronicle.com/nomisma-mifid-ii-license-for-a-blockchain-based-mtf/> [Accessed 3 January 2025]

²⁸ Mucklejohn, L. (2025) *EU regulator to intervene in row between market makers and German exchanges*, [online] Financial News, Available from: <https://www.fn.london.com/articles/eu-regulator-to-intervene-in-row-between-market-makers-and-german-exchanges-5087c7af> [Accessed: 20 June 2025]

transparent price formation and fair competition. If transposed into the context of equity token trading, such practices could severely restrict market access, hinder transparent price discovery and fragment liquidity, ultimately weakening the possibility of establishing a genuinely integrated European secondary market.

An alternate model under MiFID II applicable to trading in equity tokens, without establishing a trading venue, is the general Investment Firm (IF) definition,²⁹ with specific licensing subject to national-level legislation. While not as comprehensive as MTF it can be used to support over-the-counter³⁰ (OTC) trading of equity tokens. Unlike MTFs IFs may exercise discretion in executing client orders, enabling brokerage services such as e.g. executing orders at set prices, making it potentially more customized to users' needs, but with significantly less market volume and liquidity than MTF-based exchanges.³¹

An important provision applicable to licensed secondary market operators is the separation of customer funds and custody over their tokens from any assets used by the exchange entity³² for their own investment activities. Lack of similar safeguards in operation of cryptocurrency exchanges has contributed to spectacular market failures in recent years, e.g. as in case of the FTX exchange.³³ Regulatory restrictions are also making the scenario of equity tokens issued by the exchange itself being listed on its own secondary market highly unlikely; similar events taking place with

²⁹ MiFID II Op. cit. Art. 4, p. 1(1)

³⁰ ESMA. (2022) *Report on the DLT Pilot Regime On the Call for Evidence on the DLT Pilot Regime and compensatory measures on supervisory data*, ESMA70-460-111, p. 22

³¹ One of the leading secondary market platform operators for trading equity tokens domiciled in the EU and successfully operating under a MiFID II-compatible investment firm license is Austria-based Bitpanda – incorporated as BPFS it is a licensed investment firm (ger. Wertpapierfirma) and subject to supervision by the Austrian Financial Markets Supervisory Authority (ger. Finanzmarktaufsichtsbehörde). See Bitpanda. (2024) *Product Terms for Security Token*, [online] Bitpanda, Available from: <https://www.bitpanda.com/pl/legal/product-terms-security-token> [Accessed 3 January 2025]; See also: (2024) *Bitpanda Pioneers Security Token Access for European Retail Investors With Steelcoin Listing*, [online] Fintech Finance News, Available from: <https://ffnews.com/newsarticle/cryptocurrency/bitpanda-pioneers-security-token-access-for-european-retail-investors-with-steelcoin-listing/> [Accessed 3 January 2025]

³² Commission Delegated Directive 2017/593 of 7 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to safeguarding of financial instruments and funds belonging to clients, product governance obligations and the rules applicable to the provision or reception of fees, commissions or any monetary or non-monetary benefits. *Official Journal of the European Union* (C/2016/2031) 31 March, Art. 5, p. 1

³³ Conlon, T. Corbet, S. and Hu, Y. (2022) *The Collapse of FTX: The End of Cryptocurrency's Age of Innocence*. [pre-print] Submitted to: *British Accounting Review*. Available from: <http://dx.doi.org/10.2139/ssrn.4283333> [Accessed 3 January 2025], p. 2

utility tokens allowing for almost arbitrary inflation of the exchange business entity valuation have led to business failures and accusations of fraud.³⁴

Recognizing the obstacles to adoption of tokenization within the existing regulatory framework the EU has devised the DLT Pilot Regime – a controlled environment for platforms experimenting with blockchain-based trading and settlement. This regulatory “sandbox” emphasizes the integration of DLT systems with traditional financial market infrastructures attempting to address interoperability challenges and by facilitating the use of smart contracts and tokenized settlement reducing the reliance on intermediaries.³⁵ This initiative allows for temporary exemptions from specific requirements under MiFID II and CSDR,³⁶ enabling platforms to innovate while still ensuring regulatory oversight. Additional safeguards to the stability of the financial system have also been provided, in particular limiting the issuers’ capitalization to 500 million EUR³⁷ and total aggregate market value of all tokenized financial instruments that are admitted to 6 billion EUR,³⁸ as well as embedding temporal limitations.³⁹ A promising development in the direction of establishing a fully-functional secondary market for equity tokens was the recent awarding of a DLT Trading and Settlement System (TSS) license under the Pilot Regime to 21X A.G.⁴⁰ in Germany, enabling it to

³⁴ See analysis by BDO Canada: “On Nov. 2, 2022, crypto news website CoinDesk reported that most of these loans were backed by the billions in FTT tokens held by Alameda, which constituted the majority of Alameda’s assets. According to the SEC, Alameda and FTX collectively held the majority of the issued FTT tokens and only a small portion were in circulation. The SEC stated that Bankman-Fried “misrepresented the risk profile of investing in FTX” for reasons including: 1) FTX valued the FTT tokens held by Alameda at prices greater than their market value. 2) Alameda pledged the overvalued FTT tokens as collateral against the funds it borrowed from FTX (i.e., the line of credit). 3) Bankman-Fried failed to disclose to investors FTX’s exposure to Alameda (i.e., the collateral was largely illiquid). If the value of the FTT tokens fell, Alameda’s collateral would also be worth less. As a result, FTX would be confronted with a solvency crisis if it could not recoup its loans from Alameda to cover impending customer withdrawals. This posed a risk to both FTX platform users and FTX investors. This is precisely what happened in the days that followed the revelation by CoinDesk.” (2023) *A complex scheme: The rise and demise of FTX*, [online] BDO Canada, Available from: <https://www.bdo.ca/insights/fraud-deconstructed-ftx-cryptocurrency> [Accessed 3 January 2025]

³⁵ Jiménez-Gómez, B. (2023). *Op. cit.* p. 671

³⁶ E.g. regarding direct retail participation in MTFs (Regulation 2022/858 - Pilot Regime, p. 26) and transaction reporting exemptions (Regulation 2022/858 - Pilot Regime, p. 27); several exemptions around transaction settlement and orders handling are provided as well (Regulation 2022/858 - Pilot Regime, p. 29-34)

³⁷ Regulation 2022/858 - Pilot Regime, *Op. cit.* Art. 3, p. 1

³⁸ Regulation 2022/858 - Pilot Regime, *Op. cit.* Art. 3, p. 2

³⁹ Regulation 2022/858 - Pilot Regime, *Op. cit.* Art. 14, p. 1

⁴⁰ Jünemann, M. Wirtz, J. (2024) *Finanzaufsichtsbehörden erteilen erste Lizenz für ein blockchainbasiertes Handels- und Abwicklungssystem*, [online] Bird & Bird, Available from: <https://www.twobirds.com/de/insights/2024/germany/financial-regulators-issue-first-license-for-a-blockchain-based-trading-and-settlement-system> [Accessed 3 January 2025]

start operating a blockchain-based trading and settlement system comparable to “conventional” stock exchanges in 2025.

Apart from licensing requirements equity token trading platforms are obliged to comply with a multitude of EU and national-level regulations; a selection of those particularly relevant for this type of DLT-based operations will be discussed below.

One of the primary obligations is ensuring the protection of personal data in a highly digitalized and decentralized trading environment in line with the provisions of the General Data Protection Regulation (GDPR).⁴¹ These requirements apply to any platform processing personal data of EU citizens⁴² regardless of whether the platform is centralized or decentralized, creating significant compliance challenges for blockchain-based trading systems. Key requirements include obtaining clear, informed, and specific consent⁴³ from users for data collection and processing, especially where sensitive personal data or profiling is involved. This includes implementing robust encryption protocols and ensuring data is pseudonymized where possible,⁴⁴ particularly given the immutable nature of blockchain records.⁴⁵ Moreover, platforms must comply with GDPR’s principle of data minimization and privacy-by-design collecting only data actually necessary to facilitate transactions and meet other regulatory obligations. Secondary market operators are particularly exposed because their activities entail not only user onboarding and Anti-Money Laundering (AML)/Counter-Terrorist

⁴¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). *Official Journal of the European Union* (OJ L 119) 4 May. Available from: <http://data.europa.eu/eli/reg/2016/679/oj>

⁴² GDPR. *Op. cit.* Art. 3, p. 2

⁴³ GDPR. *Op. cit.* Art. 6, p. 1a

⁴⁴ Innovative approaches such as “off-chain” storage of personal data linked to blockchain transactions or zero-knowledge proofs are increasingly being explored to balance GDPR compliance with the decentralized and transparent nature of token trading platforms.

⁴⁵ A dedicated study has been conducted on behalf of the European Parliament exploring the compatibility of blockchain-based DLT technologies and GDPR indicating that: “First, the GDPR is based on the underlying assumption that in relation to each personal data point there is at least one natural or legal person – the data controller – that data subjects can address to enforce their rights under EU data protection law. Blockchains, however, often seek to achieve decentralization in replacing a unitary actor with many different players. (...) Second, the GDPR is based on the assumption that data can be modified or erased where necessary to comply with legal requirements such as Articles 16 and 17 GDPR. Blockchains, however, render such modifications of data purposefully onerous in order to ensure data integrity and increase trust in the network. Determining whether distributed ledger technology may nonetheless be able to comply with Article 17 GDPR is burdened by the uncertain definition of ‘erasure’ in Article 17 GDPR.” See Finck, M. (2019) *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 634.445, p. 101

Financing (CFT) due diligence – both regarding natural persons being investors on the platform, as well as ultimate beneficiary owners of the entities issuing the tokens admitted to the trading venue – but also the ongoing monitoring of trading behavior, all of which require the collection, processing and, in many cases, long-term retention of personal data. This creates a structural tension: while GDPR requires minimization and the ability to rectify or delete data, secondary market compliance obligations mandate storage, auditability and in some cases disclosure of transaction histories to supervisory authorities.⁴⁶ Moreover, data localization obligations⁴⁷ may interact problematically with the inherently borderless character of distributed ledgers, complicating compliance for platforms offering cross-border services within the EU.

AML compliance is another critical requirement for equity token trading platforms operating within the EU. These trading venues, often dealing with high-value digital assets and international transactions, are considered high-risk entities under the EU's Anti-Money Laundering Directive (AMLD).⁴⁸ As such, they must implement robust measures to prevent their platforms from being used for illicit purposes such as money laundering or terrorist financing. Under AMLD, trading platforms are required to identify and verify the identity of their users – know-your-customer (KYC) – monitor transactions, and report suspicious activities to national Financial Intelligence Units (FIUs). This involves collecting and securely storing customer data including personal identification and proof of funds which, as indicated above, requires identifying a balance between AML and GDPR obligations.⁴⁹ For secondary market platforms, the challenge lies not only in onboarding investors and traders through stringent KYC checks but also in maintaining effective real-time monitoring of trading activity, which is technologically complex and costly, especially for smaller market entrants. The integration of blockchain technology introduces unique challenges, as transactions are often pseudonymous. To address these, platforms use advanced analytical tools for blockchain forensics, enabling the tracing of funds and identification of potential illicit activities. Moreover, platforms facilitating equity token trading must also comply with enhanced due diligence requirements for

⁴⁶ Ibáñez, L.D. O'Hara, K. and Simperl, E. (2018) On Blockchains and the General Data Protection Regulation, *EU Blockchain Forum and Observatory*, 79, p. 11

⁴⁷ GDPR. *Op. cit.* Art. 45

⁴⁸ Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. *Official Journal of the European Union* (PE/72/2017/REV/1) 19 June. Available from: <http://data.europa.eu/eli/dir/2018/843/oj>

⁴⁹ OECD. (2020) *Op.cit.* p. 20

high-risk transactions, particularly when dealing with politically exposed persons (PEPs) or transactions involving jurisdictions with inadequate AML standards; solutions combining on-chain transparency with off-chain identity verification are emerging as best practices.⁵⁰

Another key piece of legislation specifically relevant for MiFID II licensed trading venues is the Market Abuse Regulation (MAR),⁵¹ which aims to ensure market integrity and transparency in financial markets. As equity tokens qualify as financial instruments under MiFID II any secondary market operator for equity token trading under an MTF license would need to comply with its provisions. MAR specifically prohibits insider dealing, unlawful disclosure of inside information and market manipulation and imposes strict requirements on platforms to detect and prevent abusive practices.⁵² For compliance, equity token trading platforms must implement systems to monitor trading activities in real-time, identify suspicious transactions, and report them to the relevant National Competent Authority (NCA). These obligations have to be analyzed considering the unique characteristics of equity token trading, where blockchain's transparency offers opportunities for enhanced surveillance but also challenges due to pseudoanonymity.⁵³ Platforms are increasingly adopting blockchain analytics tools to trace token movements and detect patterns indicative of market manipulation.⁵⁴ MAR also requires platforms to ensure proper dissemination of inside information. This includes public disclosures via regulated information channels to ensure all market participants have equal access to material information about the tokens being traded and their characteristics. Another critical area of MAR compliance for tokenized equity markets is addressing wash trading, spoofing, and pump-and-dump

⁵⁰ (2024) Boerse Stuttgart Digital partners with Fenargo to scale regulatory compliant crypto solutions across Europe, [online] Fenargo, Available from: <https://resources.fenargo.com/newsroom/boerse-stuttgart-digital-partners-with-fenargo-to-scale-regulatory-compliant-crypto-solutions-across-europe> [Accessed 3 January 2025]

⁵¹ Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (MAR). *Official Journal of the European Union* (OJ L 173) 12 June

⁵² MAR. *Op. cit.* Art. 1, p. 1

⁵³ OECD. (2020) *Op.cit.* p. 21

⁵⁴ Rane, N. Choudhary, S. and Rane, J. (2023) Blockchain and Artificial Intelligence (AI) Integration for Revolutionizing Security and Transparency in Finance, SSRN Available from: <http://dx.doi.org/10.2139/ssrn.4644253> [Accessed 3 January 2025], p. 6

schemes⁵⁵ which could be particularly challenging in digital asset markets with high retail participation and global reach. Innovative measures, such as smart contracts programmed to prevent certain types of abusive trades are emerging as potential solutions to enhance compliance with MAR.⁵⁶

A separate operational model for secondary markets is the so-called decentralized exchange (DEX) operating without a central responsible entity in a peer-to-peer model involving buyers and sellers. The exchange of tokens or cryptocurrencies occurs directly between both parties without any intermediaries by use of dedicated software and protocols. The inherent immutability of the blockchain does provide a trusted platform simplifying clearing and settlement of the transaction and significantly reducing counterparty risk even in absence of a central trusted third party.⁵⁷ However, in case of the initial trading stage of the transaction, lack of a centralized solicitation venue and order book inhibits interaction between buyers and sellers and thereby obtaining liquidity and a significant trading volume.⁵⁸

Decentralized equity token trading platforms, which operate without a central intermediary, present unique challenges under the EU's legal and licensing frameworks; as fully decentralized platforms lack a clearly identifiable operator, attribution of compliance requirements might be challenging. On the other hand, in order to operate a viable secondary market it is highly problematic to avoid license-triggering activities such as e.g. solicitation of securities or custody of assets by at least some of the stakeholders. Actual regulatory classification whether the platform is fully decentralized and responsibility, in particular for compliance and risk management, can be attributed to a specific legal entity might depend on relatively complex technical details and, as ESMA highlights, depends on a case-by-case basis.⁵⁹

⁵⁵ du Toit, D. (2024) *Crypto Market Manipulation: Shedding Light on the Hidden Tactics*, [online] Coinpaper, Available from: <https://coinpaper.com/3631/crypto-market-manipulation-shedding-light-on-the-hidden-tactics> [Accessed 3 January 2025]

⁵⁶ Coelho, D. Figueiredo, A. J. (2024) The relationship between MiCAR and MAR: a brief introduction, SSRN, Available from: <http://dx.doi.org/10.2139/ssrn.4887363> [Accessed 3 January 2025]

⁵⁷ Although significant security and safety concerns are cited as one of the primary factors preventing wider adoption of DEXes, see Sonner, P. (2024) *Decentralized Exchanges Risks Review. What is a DEX in Crypto?* [online] Beinsure, Available from: <https://beinsure.com/decentralized-exchanges-risks-review-what-is-a-dex-cryptoexchange/> [Accessed 3 January 2025]

⁵⁸ Ibid

⁵⁹ According to ESMA: "Finally, regarding DEXs, ESMA acknowledges (...) where crypto-asset services are provided in a fully decentralised manner without any intermediary' should fall outside the scope of MiCA but also notes that the exact scope of this exemption remains uncertain. ESMA considers that an assessment of each system should be made on a case-by-case basis considering the

Although DEXes were seen as a promising path to rapid establishment of viable secondary markets for equity tokens, the inherent limitations of a purely decentralized approach have prevented widespread adoption so far. Combined centralized-decentralized (hybrid) models were found to be operationally more viable, however they do invoke licensing requirements that are not materially different from those described above for centralized platforms.⁶⁰

3. OBJECTIVES OF SECONDARY MARKETS

Liquidity, a fundamental attribute of well-functioning financial markets, is essential for the overall success of the tokenization value chain. Secondary markets provide a mechanism for investors to buy and sell equity tokens after the initial issuance, ensuring assets are not locked into illiquid positions. A key factor enabling liquidity is the trading volume of the venue, which in turn is dependent primarily on the number of traders and the funds involved. However, there are several factors related to the regulatory environment of equity token secondary markets that might pose challenges in achieving significant trading volumes.

One of the key characteristics of the European security token secondary market landscape is the relatively large number of small, domestically oriented trading platforms and simultaneously significant, in terms of volume, presence of global players; regulatory uncertainty as well as an incomplete capital markets and banking union within the EU might be amounts the factors inhibiting growth of pan-European trading venues.⁶¹

Another relevant factor adversely affecting growth of the investors base are onboarding and client acceptance challenges in KYC and AML-compliance related processes. This often translates into an inability to tap into existing users bases of cryptocurrency exchanges, which might constitute some of the most promising early adopters of equity token investing.⁶²

features of the system.” See ESMA. (2023) *Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper*, ESMA75-453128700-438, Available from: https://www.esma.europa.eu/sites/default/files/2023-10/ESMA75-453128700-438_MiCA_Consultation_Paper_2nd_package.pdf [Accessed 3 January 2025], p. 108

⁶⁰ Nägele, T. (2020) *Op.cit.* section 4.1

⁶¹ Cipollone, P. (2024) Towards a digital capital markets union, In: *Bundesbank Symposium on the Future of Payments*, Frankfurt am Main, 7. October. Available from: <https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp241007~cc903db51d.en.html> [Accessed 3 January 2025]

⁶² Benson, V. et al. (2024) Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions, *European Journal of Law and Economics*, 57. Available from: <https://doi.org/10.1007/s10657-024-09797-w> [Accessed 3 January 2025], sec. 5.2

Although not directly resulting from the trading venues' compliance requirements an overall issue in the equity tokenization value chain is the relatively limited offer of attractive investment options, especially available on secondary markets. While cryptocurrencies-related investment products and utility tokens have already achieved massive traction, larger-scale equity token trading remains elusive.⁶³

Licensing requirements and compliance obligations of secondary market operators have an indirect positive impact on the perception and confidence of potential investors regarding the equity tokenization concept. In fact, the element of licensing or supervision by an NCA is often specifically emphasized in marketing communication of platforms and intermediaries. However, as has already been indicated above regarding MTFs, the actual scope of regulation and supervision is often complex and difficult to determine by a non-professional investors. In addition, some claims can be regarded as clearly misleading, both in terms of the actual jurisdiction of supervision as well as the point in time.⁶⁴

The advent of secondary markets for equity tokens also expands market access allowing for continuous trading across geographies, removing barriers such as time zones and market. Moreover, tokenization reduces minimum investment thresholds, transaction fees and processing costs, making especially smaller scale investments financially more viable.⁶⁵ Ultimately, a mature equity token market could enable retail investors to access early-stage deals previously only available to professional investors or venture capital funds, yielding significantly higher profits⁶⁶ than available to them in "conventional" capital markets. However, corresponding investment risk exposure, without the mitigating impact of larger portfolios, could be

⁶³ (2024) *STM Market Report: April 2024*, [online] Medium, Available from: <https://medium.com/security-token-group/stm-market-report-april-2024-82b253d80626> [Accessed 3 January 2025]

⁶⁴ See e.g. Malta Financial Services Authority. (2021) *MFSA Warning to the Public regarding Binance and Other Unlicensed VFA Service Providers*, [press release] 14 July. Available from: <https://www.mfsa.mt/news-item/mfsa-warning-to-the-public-regarding-binance-and-other-unlicensed-vfa-service-providers/> [Accessed 3 January 2025]

⁶⁵ Schär, F. (2021) Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets, *FRB of St. Louis Review*, 103 (2). Available from: <https://doi.org/10.20955/r.103.153-74> [Accessed 3 January 2025], p. 5

⁶⁶ Neufund tokenization platform: "original mission to: make high-yield, innovative, & startup investment opportunities accessible to anyone." See Neufund. (2019) *Launching retail offerings, developing the platform and more. What's new at Neufund?* [blog entry] 22 May. Medium. Available from: <https://blog.neufund.org/launching-retail-offerings-developing-the-platform-and-more-whats-new-at-neufund-1599c851ef53> [Accessed 3 January 2025]

substantially underestimated – comprehensive application of MiFID II-based retail investor protection provisions seems to be of significant importance.⁶⁷

Secondary markets play also a pivotal role in the price discovery process, where the prices of securities are determined through the interactions of buyers and sellers rather than at levels set during issuance. This continuous pricing mechanism is closely linked to liquidity, which at a sufficient level enables trading without significant price disruptions by a single transaction. Pricing validation of tokens based on supply and demand dynamics contributes to investor confidence as well, enabling comparison of valuations between similar ventures. It also facilitates fair valuation of equity tokens from an accounting perspective, making them more attractive assets to investors with lower risk of potential impairment.⁶⁸

4. CROSS-BORDER OPERATIONS

Analyzing cross-border operations is essential for understanding how equity token secondary markets can evolve within the fragmented regulatory environment of the EU. The interaction between MiFID II passporting and divergent national interpretations of financial instruments reveals that regulatory fragmentation and supervisory inconsistencies remain major obstacles to scaling platforms across jurisdictions.⁶⁹ These barriers directly affect liquidity and investor participation, undermining the ability of tokenized markets to achieve the scale necessary for sustainable growth.

License passporting plays a pivotal role in the cross-border operations of secondary market platforms for equity tokens within the EU; as established under MiFID II, the passporting framework allows entities already licensed in one EU member state to provide financial services across the EU without requiring additional licensing in each jurisdiction.⁷⁰ However, despite the harmonization intent of MiFID II, national interpretations may vary, creating potential regulatory divergence. Platforms must navigate differing approaches by NCAs regarding licensing requirements and procedural nuances. For instance, some member states apply broader interpretations of financial instruments, potentially encompassing a wider range of tokenized assets.⁷¹ This divergence necessitates detailed jurisdiction-specific legal

⁶⁷ MiFID II. *Op. cit.* Art. 24, p. 4 (b)

⁶⁸ See e.g. *Security token offerings: The next phase of financial market evolution?*, [online] Deloitte, Available from: <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/audit/deloitte-cn-audit-security-token-offering-en-201009.pdf> [Accessed 3 January 2025], p. 17

⁶⁹ Nägele, T. (2020) *Op.cit.* section 4.2.1.2

⁷⁰ MiFID II. *Op. cit.* Art. 34, p. 1

⁷¹ This challenge has been identified by ESMA: “The different approaches to the national transposition of MiFID across Member States mean that there is no commonly adopted application

strategies for platforms operating across multiple EU countries, particularly given the on-going implementation of MiCA.

5. QUANTITATIVE ANALYSIS OF EQUITY TOKEN SECONDARY MARKETS

In an attempt to provide substantiation to the above review of key regulatory compliance requirements and constraints quantitative data regarding operators of equity token secondary markets has been collected.⁷² Information has been analyzed for 48 licensed security token secondary market entities, out of which 9 were incorporated within EU jurisdictions. An overview of the number of secondary market entities in jurisdictions for which data was available (with the EU summarized as one) and the respective shares in the global total have been visualized on the Figure 1 below:

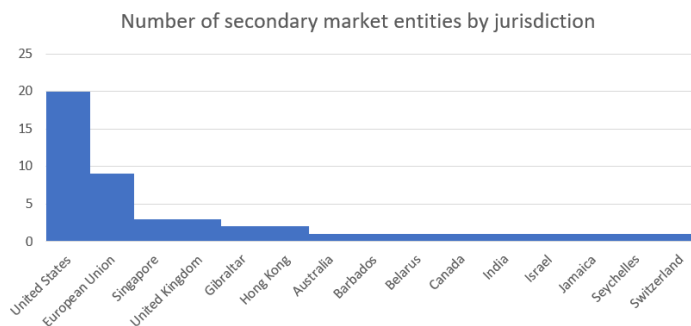


Figure 1: Number of secondary market entities by jurisdiction

of the definition of 'financial instrument' under MiFID in the EU. Whilst this issue has been noted as a concern since the implementation of MiFID/MiFID II, practical consequences may emerge with Regulation (EU) 2023/1114 (MiCA) regarding the classification of crypto-assets as financial instruments." See ESMA. (2024) *Final Report Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments*, ESMA75453128700-1323, 17 December. Available from: https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75453128700-1323_Final_Report_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs.pdf [Accessed 3 January 2025]

⁷² Data has been collected from multiple sources spanning different time periods and entities including databases of the International Token Standardization Association, STOWise – Token Asset Intelligence and STOcheck Report (update from 20 November 2019) supplemented by information from publicly available sources and press-releases of the secondary market operators. Available data does not cover all security and equity token projects (worldwide and in the EU). Analysis has been focused on relative factors only due limited completeness of data and difficulties in extraction of equity token data. *STO Services Directory*, [online] STOWise, Available from: <https://stowise.com/company-category/exchanges-at/> [Accessed 13 April 2025]

With the US demonstrating the highest number of secondary market platforms the EU follows at second place. Although it has to be taken under consideration that security token classification rules applied by the SEC in the United States⁷³ are different from those under MIFID II – a broader scope of financial instruments falls under the definition of securities than in the EU – this data could indicate a significant disadvantage in adoption of secondary market trading between the EU the US. In order to substantiate this assumption for EU-domiciled security token secondary market operators their current operational status has been confirmed with the results presented in Table 1 below:

Service Provider	Country	Incorporation Date	Status as of March 2025
Bitpanda	Austria	2014	Active
Blocktrade	Liechtenstein	2020	Active
Coinmetro	Estonia	2017	Active
Deutsche Börse Group	Germany	1993	Active
DXtech Exchange	Estonia	2018	Defunct
Extauri	Liechtenstein	2018	Defunct
LATOKEN	Estonia	2017	Active, but no security token listed
Malta Stock Exchange	Malta	1992	Active, but no security token listed
NXchange	Netherlands	2015	Active, but no security token listed

Table 1: Major secondary market equity token trading platforms within the EU – status as of March 2025

As can be seen from the data above the actual status of the secondary market operators in the EU is even less developed than could be anticipated from the number of entities alone, as a significant percentage is either defunct or failing to actively trade in security tokens. As of March 2025, the adoption of regulated secondary market infrastructures for equity tokens in the EU remains limited. According to ESMA, only three entities had been authorized under the DLT Pilot Regime:

- 21X AG (DLT-TSS, Germany);
- 360X AG (DLT-MTF, Germany, pre-operational); and

⁷³ Based on the so-called *Howey Test* identifying a security when all 4 criteria are met: money is invested, the investment is part of a "common enterprise", investors expect to make a profit from their investment and the expected profits depend on the efforts of others; it covers a broader scope of instruments compared to the definition applied by MIFID2; see *Securities and Exchange Commission v. W. J. Howey Co. et al.*, 328 U.S. 293 66 S. Ct. 1100; 90 L. Ed. 1244; 1946 U.S. LEXIS 3159; 163 A.L.R. 1043

- CSD Prague (DLT-SS, Czech Republic).

reflecting the significant barriers to entry created by licensing complexity and national divergences.⁷⁴ This slow pace of authorization contrasts with the regulatory ambition of MiFID II passporting and illustrates how compliance burdens have limited the creation of pan-European venues capable of supporting cross-border scale.

On the market side, global data suggest that as of April 2024 there were approximately 500–550 live security tokens traded across around a dozen platforms worldwide with monthly trading volume in tokenized securities reaching 8.55 million USD and Europe hosting only a minor fraction of total trading volume.⁷⁵

6. OBSERVATIONS AND CONCLUSIONS

Regarding the regulatory landscape and licensing requirements for secondary market operators of equity tokens, the analysis shows that MiFID II and related national laws continue to constitute the principal framework for authorization. While initiatives such as the German eWpG and Luxembourg's Blockchain II Law enable blockchain-native securities registration, the fragmented application of MiFID II across member states creates significant legal uncertainty for operators. The DLT Pilot Regime has provided a valuable experimental framework, but the limited number of licenses granted as of March 2025 indicates that regulatory complexity and divergent national interpretations still represent barriers to entry, limiting the development of robust pan-European infrastructures.

In relation to the impact of regulation on liquidity and market access, strict licensing and compliance obligations—particularly under AML/CTF, GDPR, and MAR—while essential for investor protection, tend to restrict onboarding, reduce investor bases, and fragment liquidity across small, domestically oriented platforms. The result is a “chicken and egg” problem: without sufficient scale, venues cannot generate liquidity attractive to issuers or investors, which in turn further discourages market participation. This undermines one of the core functions of secondary markets, namely to provide efficient price discovery and broad market access, with the EU still lagging behind the United States and Asia in terms of trading volumes and active platforms.

⁷⁴ ESMA. (2025) *Report on the Functioning and Review of the DLT Pilot Regime - Pursuant to Article 14 of Regulation (EU) 2022/858*, ESMA75-117376770-460, 25 June. Available from: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf [Accessed 20 August 2025], p. 4

⁷⁵ (2024) STM Market Report: April 2024. *Op.cit.*

Concerning cross-border operations, the MiFID II passporting framework was designed to support a single market for financial services, yet divergent national practices in defining financial instruments and licensing criteria remain obstacles to seamless expansion. Platforms operating across multiple jurisdictions must adapt to supervisory inconsistencies, which significantly increases compliance costs and discourages consolidation. As a result, cross-border scalability remains limited, hampering the EU's ambition to foster integrated and globally competitive markets for tokenized equity. Without greater regulatory convergence and a more uniform supervisory approach, security token exchanges in the EU risk remaining fragmented, undermining the potential for a pan-European marketplace.

As can be seen from the examples being discussed above and the still, despite many years of active endeavors, limited adoption of secondary market platforms for equity tokens, the topic in question is one of extraordinary regulatory complexity. One of the underlying root causes would be the clash of contradicting objectives and values: on one side ensuring stability and integrity of the financial system – preventing financial crises, speculation bubbles, fraudulent schemes and money laundering – and investor protection, in particular of retail investors, while on the other side supporting European innovation and competitiveness as well as boosting financial inclusion through increased capital market accessibility. It must however also be kept in mind that the cost of regulatory and supervisory inaction and delays is substantial for the whole EU in light of overwhelming global competition. Fragmentation of the European capital market might constitute another major root cause, inhibiting trading platforms in achieving enough volume and scale to compete effectively on the global market. Another related factor could be internal competition within the EU, in particular between smaller countries, more eager to embrace liberal regulatory and licensing approaches and focusing on significant cross-border activities, and larger countries, more concerned about protecting their domestic financial markets and investors. These differences, translating into diverse regulatory and supervisory approaches might encourage “jurisdiction shopping” and trigger additional intra-EU concerns.

Integration of equity token trading into the, often very substantial, trading volume of cryptocurrency exchanges clashed not only with licensing requirements, but also specific compliance provisions, in particular in the AML area. Despite early expectations of the cryptoindustry that even “retroactive” onboarding of the existing customer base for equity (and security tokens in general) trading would be possible in partnership with

existing stock exchanges,⁷⁶ financial market regulators were clear about strict application of KYC and due diligence checks prior to any trading taking place; several key players including e.g. market leader Binance, discontinued their applications for licensing.⁷⁷ At present, the entry into force of MiCA and tightening regulatory requirements regarding VASPs display a trend of regulatory convergence regarding requirements for trading in cryptoassets and equity tokens potentially reducing the concern mentioned above in future.

Several potential regulatory developments could be identified supporting the adoption of equity token secondary trading with the most specific being the extension of the DLT Pilot Regime both in volume – by increasing the value limitations – and time scale, enabling a longer and more favorable transition period. Establishing the DLT tokenization value chain as a viable financing and investment opportunity in the EU should become hereby an objective equal in importance to those of validation of the regulatory environment and protection of the stability of the financial system.

Further integration of the capital market union in the EU should be seen as another vital component of future development. Reduction of regulatory uncertainty resulting from national-level implementation differences of EU directives and NCA-level interpretation variances between jurisdictions is a vital component of successful cross-border operation and acquisition of sufficient scale for secondary market platforms. A potential solution to the problem of divergent MiFID II interpretations across jurisdictions could be the adoption of binding relevant Regulatory Technical Standards (RTS) developed by ESMA, clarifying the treatment of tokenized financial instruments and secondary trading venues. In parallel, a stronger role for the European Single Supervisory Mechanism in capital markets—akin to the banking SSM—could further ensure consistent supervisory practices, thereby fostering the creation of a genuinely pan-EU secondary market for equity tokens.

A final observation should be made regarding the role and involvement of existing European national-level “conventional” stock exchanges in the digital equity tokenization process. Realizing their relatively low

⁷⁶ See Malta Stock Exchange. (2018) *Malta Stock Exchange Signs MOU with Binance to Launch Security Tokens Trading Platform*, [press release] 11 September. Available from: <https://www.borzamalta.com.mt/news-and-articles/articles/mse-binance-mou> [Accessed 3 January 2025]

⁷⁷ Berwick, A. and Wilson, T. (2022) *Special report - crypto giant Binance kept weak money-laundering checks even as it promised tougher compliance documents show*, [online] Reuters, Available from: <https://www.reuters.com/article/business/media-telecom/special-report-crypto-giant-binance-kept-weak-money-laundering-checks-even-as-it-idUSL8N2U065F/> [Accessed 3 January 2025]

capitalization values, in particular in new technologies-oriented markets, effective cross-border cooperation in establishing a viable equity token trading venue could be seen as a possibility to retain relevance in a globalized financial landscape. On the other hand, their invaluable experience in market monitoring and abuse prevention would be of paramount value to issuers and investors alike, combining the future opportunities of tokenization with reliability and security built upon decades of past supervisory diligence.

LIST OF REFERENCES

- [1] Autorité des Marchés Financiers. (2020) *Review and analysis of the application of financial regulations to security tokens*. Available from: <https://www.amf-france.org/sites/institutionnel/files/private/2020-10/legal-analysis-security-tokens-amf-en.pdf> [Accessed 3 January 2025]
- [2] Bassana, F. and Rabittib, M. (2024) From smart legal contracts to contracts on blockchain: An empirical investigation. *Computer Law & Security Review*, 55
- [3] Benetti, Z. and Piazza, F. (2024) Decentralised Finance: A categorisation of smart contracts. *ESMA Working Papers*, No. 3, ESMA50-43599798-9913
- [4] Benson, V. et al. (2024) Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions, *European Journal of Law and Economics*, 57. Available from: <https://doi.org/10.1007/s10657-024-09797-w> [Accessed 3 January 2025]
- [5] Berwick, A. and Wilson, T. (2022) *Special report - crypto giant Binance kept weak money-laundering checks even as it promised tougher compliance documents show*, [online] Reuters, Available from: <https://www.reuters.com/article/business/media-telecom/special-report-crypto-giant-binance-kept-weak-money-laundering-checks-even-as-it-idUSL8N2U065F/> [Accessed 3 January 2025]
- [6] Bossi, P. (2020) *Nomisma's MiFID II License For A Blockchain-Based MTF*, [online] GLC, Available from: <https://globallegalchronicle.com/nomisma-s-mifid-ii-license-for-a-blockchain-based-mtf/> [Accessed 3 January 2025]
- [7] Cipollone, P. (2024) Towards a digital capital markets union, In: *Bundesbank Symposium on the Future of Payments*, Frankfurt am Main, 7. October. Available from: <https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp241007~cc903db51d.en.html> [Accessed 3 January 2025]
- [8] Coelho, D. Figueiredo, A. J. (2024) The relationship between MiCAR and MAR: a brief introduction, SSRN, Available from: <http://dx.doi.org/10.2139/ssrn.4887363> [Accessed 3 January 2025]

- [9] Commission Delegated Directive 2017/593 of 7 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to safeguarding of financial instruments and funds belonging to clients, product governance obligations and the rules applicable to the provision or reception of fees, commissions or any monetary or non-monetary benefits. *Official Journal of the European Union* (C/2016/2031) 31 March
- [10] Conlon, T. Corbet, S. and Hu, Y. (2022) The Collapse of FTX: The End of Cryptocurrency's Age of Innocence. [pre-print] Submitted to: *British Accounting Review*. Available from: <http://dx.doi.org/10.2139/ssrn.4283333> [Accessed 3 January 2025]
- [11] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. *Official Journal of the European Union* (PE/72/2017/REV/1) 19 June. Available from: <http://data.europa.eu/eli/dir/2018/843/oj>
- [12] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU. *Official Journal of the European Union* (OJ L 173, 12.6.2014) 12 June. Available from: <http://data.europa.eu/eli/dir/2014/65/oj>
- [13] du Toit, D. (2024) *Crypto Market Manipulation: Shedding Light on the Hidden Tactics*, [online] Coinpaper, Available from: <https://coinpaper.com/3631/crypto-market-manipulation-shedding-light-on-the-hidden-tactics> [Accessed 3 January 2025]
- [14] ESMA. (2022) *Report on the DLT Pilot Regime On the Call for Evidence on the DLT Pilot Regime and compensatory measures on supervisory data*, ESMA70-460-111
- [15] ESMA. (2023) *Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper*, ESMA75-453128700-438, Available from: https://www.esma.europa.eu/sites/default/files/2023-10/ESMA75-453128700-438_MiCA_Consultation_Paper_2nd_package.pdf [Accessed 3 January 2025]
- [16] ESMA. (2024) *Final Report Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments*, ESMA75453128700-1323, 17 December. Available from: https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75453128700-1323_Final_Report_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs.pdf [Accessed 3 January 2025]

- [17] ESMA. (2025) *Report on the Functioning and Review of the DLT Pilot Regime - Pursuant to Article 14 of Regulation (EU) 2022/858*, ESMA75-117376770-460, 25 June. Available from: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf [Accessed 20 August 2025]
- [18] Finck, M. (2019) *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 634.445
- [19] Garrido, J. M. (2023) *Digital Tokens: A Legal Perspective*. *IMF Working Papers*, 151
- [20] Ibáñez, L.D. O'Hara, K. and Simperl, E. (2018) *On Blockchains and the General Data Protection Regulation*, *EU Blockchain Forum and Observatory*, 79
- [21] Jiménez-Gómez, B. (2023) *Distributed Ledger Technology in Financial Markets. The European Union Experiment*, *Cuadernos de Derecho Transnacional*, 15 (2)
- [22] Jünemann, M. Wirtz, J. (2024) *Finanzaufsichtsbehörden erteilen erste Lizenz für ein blockchainbasiertes Handels- und Abwicklungssystem*, [online] Bird & Bird, Available from: <https://www.twobirds.com/de/insights/2024/germany/financial-regulators-issue-first-license-for-a-blockchain-based-trading-and-settlement-system> [Accessed 3 January 2025]
- [23] Kreppmeier, J. and Laschinger, R. (2023) *Signaling in the Market for Security Tokens*, *Journal of Business Economics*, 93. Available from: <https://doi.org/10.1007/s11573-023-01175-3> [Accessed 3 January 2025]
- [24] Kreppmeier, J. et al. (2023) *Real estate security token offerings and the secondary market: Driven by crypto hype or fundamentals?*, *Journal of Banking and Finance*, 154
- [25] Lambert, T. et al. (2021) *Security token offerings*, *Small Business Economics*, 59. Available from: <https://doi.org/10.1007/s11187-021-00539-9> [Accessed 3 January 2025]
- [26] Malta Financial Services Authority. (2021) *MFSA Warning to the Public regarding Binance and Other Unlicensed VFA Service Providers*, [press release] 14 July. Available from: <https://www.mfsa.mt/news-item/mfsa-warning-to-the-public-regarding-binance-and-other-unlicensed-vfa-service-providers/> [Accessed 3 January 2025]
- [27] Malta Stock Exchange. (2018) *Malta Stock Exchange Signs MOU with Binance to Launch Security Tokens Trading Platform*, [press release] 11 September. Available

- from: <https://www.borзамalta.com.mt/news-and-articles/articles/mse-binance-mou> [Accessed 3 January 2025]
- [28] Marjosola, H. (2022) Security Tokens and the Future of EU Securities Law: Rethinking the Harmonisation Project, *University of Helsinki Faculty of Law Legal Studies Research Paper Series*, 70 (2021). Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897849#
- [29] Mucklejohn, L. (2025) *EU regulator to intervene in row between market makers and German exchanges*, [online] Financial News, Available from: <https://www.fn.london.com/articles/eu-regulator-to-intervene-in-row-between-market-makers-and-german-exchanges-5087c7af> [Accessed: 20 June 2025]
- [30] Nägele, T. (2020) *Secondary Market for Security Tokens — The need for a new regulatory approach at the European Union level* [online] Medium. Available from: <https://tokencontainermodel.com/secondary-market-for-security-tokens-the-need-for-a-new-regulatory-approach-at-the-european-e922e4ca04> [Accessed 3 January 2025]
- [31] Nassr, I. (2021) Understanding the tokenization of assets in financial markets, *OECD Going Digital Toolkit Notes*, 19. Available from: <https://doi.org/10.1787/c033401a-en> [Accessed 3 January 2025]
- [32] Neufund. (2019) *Launching retail offerings, developing the platform and more. What's new at Neufund?* [blog entry] 22 May. Medium. Available from: <https://blog.neufund.org/launching-retail-offerings-developing-the-platform-and-more-whats-new-at-neufund-1599c851ef53> [Accessed 3 January 2025]
- [33] News Desk. (2021) *Nxchange securities token exchange acquires Bondex for tokenized shared issuance*, [online] Available from: <https://www.unlock-bc.com/news/2021-05-04/nxchange-securities-token-exchange-acquires-bondex-for-tokenized-shared-issuance/> [Accessed 3 January 2025]
- [34] OECD. (2020) The Tokenisation of Assets and Potential Implications for Financial Markets, *OECD Blockchain Policy Series*, 2020, Available from: www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm [Accessed 3 January 2025]
- [35] Rane, N. Choudhary, S. and Rane, J. (2023) Blockchain and Artificial Intelligence (AI) Integration for Revolutionizing Security and Transparency in Finance, SSRN Available from: <http://dx.doi.org/10.2139/ssrn.4644253> [Accessed 3 January 2025]

- [36] Raskin, M. and Yermack, D. (2016) Digital currencis, decentralized ledgers and the future of central banking, *National Bureau of Economic Research Working Papers*. Available from: <https://www.nber.org/papers/w22238>
- [37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). *Official Journal of the European Union* (OJ L 119) 4 May. Available from: <http://data.europa.eu/eli/reg/2016/679/oj>
- [38] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA), and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. *Official Journal of the European Union* (PE/54/2022/REV/1) 9 June. Available from: <http://data.europa.eu/eli/reg/2023/1114/oj>
- [39] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (MAR). *Official Journal of the European Union* (OJ L 173) 12 June
- [40] Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories (CSDR) and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012. *Official Journal of the European Union* (OJ L 257) 28 August. Available from: <http://data.europa.eu/eli/reg/2014/909/oj>
- [41] Regulation 2022/858 of the European Parliament and Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (Pilot Regime) and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU. *Official Journal of the European Union* (PE/88/2021/REV/2) 2 June. Available from: <http://data.europa.eu/eli/reg/2022/858/oj>
- [42] Schär, F. (2021) Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets, *FRB of St. Louis Review*, 103 (2). Available from: <https://doi.org/10.20955/r.103.153-74> [Accessed 3 January 2025]
- [43] Sonner, P. (2024) *Decentralized Exchanges Risks Review. What is a DEX in Crypto?* [online] Beinsure, Available from: <https://beinsure.com/decentraliz>

- ed-exchanges-risks-review-what-is-a-dex-cryptoexchange/
[Accessed 3 January 2025]
- [44] Zetzsche, D. A. Buckley, R. P. and Arner D. W. (2019) The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *University of Illinois Law Review*, 4
- [45] Zhang, Y. Gong, B. and Zhou, P. (2024) Centralized use of decentralized technology: Tokenization of currencies and assets. *Structural Change and Economic Dynamics*, Volume 71
- [46] (2023) *A complex scheme: The rise and demise of FTX*, [online] BDO Canada, Available from: <https://www.bdo.ca/insights/fraud-deconstructed-ftx-cryptocurrency> [Accessed 3 January 2025]
- [47] (2024) *Bitpanda Pioneers Security Token Access for European Retail Investors With Steelcoin Listing*, [online] Fintech Finance News, Available from: <https://ffnews.com/newsarticle/cryptocurrency/bitpanda-pioneers-security-token-access-for-european-retail-investors-with-steelcoin-listing/> [Accessed 3 January 2025]
- [48] (2024) *Boerse Stuttgart Digital partners with Fenargo to scale regulatory compliant crypto solutions across Europe*, [online] Fenargo, Available from: <https://resources.fenargo.com/newsroom/boerse-stuttgart-digital-partners-with-fenargo-to-scale-regulatory-compliant-crypto-solutions-across-europe> [Accessed 3 January 2025]
- [49] (2024) *STM Market Report: April 2024*, [online] Medium, Available from: <https://medium.com/security-token-group/stm-market-report-april-2024-82b253d80626> [Accessed 3 January 2025]
- [50] (2024) *Building the Digital Asset Securities Ecosystem Digital Asset Securities Control Principles: a framework for adoption, An Industry Paper from DTCC, Clearstream, and Euroclear with the collaboration of BCG*. [online] DTCC. Available from: <https://www.dtcc.com/-/media/DASCPWhitePaper.pdf> [Accessed 3 January 2025]
- [51] *Electronic Securities Act 2021*, Germany. Bundesgesetzblatt. In: German
- [52] *Law of 22 January 2021 amending the law of 5 April 1993 on the financial sector and the law of 6 April 2013 on dematerialised securities 2021*, Luxembourg. In: Luxembourgish
- [53] *Securities and Exchange Commission v. W. J. Howey Co. et al.*, 328 U.S. 293 66 S. Ct. 1100; 90 L. Ed. 1244; 1946 U.S. LEXIS 3159; 163 A.L.R. 1043
- [54] *Security token offerings: The next phase of financial market evolution?*, [online] Deloitte, Available from: <https://www2.deloitte.com/content/da>

m/Deloitte/cn/Documents/audit/deloitte-cn-audit-security-token-offering-en-201009.pdf [Accessed 3 January 2025]

DOI 10.5817/MUJLT2026-41367

ANOTHER VIEW ON ARTICLE 22 GDPR: THE FUTURE OF AUTOMATED DECISION-MAKING

by

NIMROD MIKE *

Artificial intelligence (AI) increasingly underpins automated decision-making (ADM) in high-stakes contexts such as credit scoring, workforce management, and public service allocation, raising acute concerns about transparency, accountability, and the limits of algorithmic secrecy. This paper examines how Article 22 GDPR should be understood following the Court of Justice of the European Union's SCHUFA ruling, which resolved the prior doctrinal debate by confirming that Article 22(1) operates as a prohibition in principle, qualified by exceptions under Article 22(2) and safeguards under Article 22(3). Through doctrinal analysis of SCHUFA alongside EU national court and data protection authority decisions spanning multiple sectors, including Uber/Ola, Deliveroo/Foodinho, Buona Scuola, AMAS, Caixabank, and Grindr, the paper delineates operational criteria for when ADM is solely automated, when it reaches the significant effects threshold, and what meaningful information must substantively provide. The analysis demonstrates that intermediate algorithmic outputs can constitute ADM where they materially shape subsequent outcomes, and that nominal human review fails to satisfy Article 22 where it amounts to rubber-stamping without interpretive criteria or authority to deviate. The paper further develops a cumulative ADM doctrine: sequential or continuous automated steps may collectively trigger Article 22 where they produce aggregate effects on livelihood, credit, services, or public benefits. A key doctrinal contribution is the distinction between transactional non-selection, which does not cross the significance threshold, and positional assessment, where algorithmic flagging, downranking, or sanctioning alters an individual's standing within a system and determines future access to opportunities. The paper concludes

* Nimród Mike, Ph.D., LL.M.; Corvinus University of Budapest, Institute of Data Analytics and Information Systems; Assistant professor; E-mail: nimrod.mike@uni-corvinus.hu

that explainable AI is a legally necessary instrument for making disclosures contestation-enabling under Article 22(3), but is insufficient without institutional safeguards, including genuine human oversight, rights to challenge, data protection impact assessments, and coordination with the AI Act's risk-based framework.

KEY WORDS

Automated decision-making (ADM), Article 22 GDPR, Explainable AI (xAI), SCHUFA ruling, Algorithmic transparency, Algorithmic accountability

1. INTRODUCTION

Artificial intelligence ("AI") underpins numerous automated decision-making ("ADM") processes. In credit scoring, these concerns are pronounced because AI-driven creditworthiness assessments affect financial opportunities.¹ The European Union ("EU") General Data Protection Regulation ("GDPR")² addresses ADM in Article 22. The debate has centered on whether Article 22 functions as a general prohibition or as a right requiring active exercise.³ The Court of Justice of the European Union ("Court" or "CJEU") in its SCHUFA ruling⁴ resolved this debate by stating that Article 22(1) is a prohibition in principle, with controllers needing to establish a lawful basis under Article 22(2). The prohibition is qualified, conditioning ADM on specific exceptions and safeguards.⁵ This paper elucidates this qualified character through the

¹ Addy, W. et al. (2024) AI in Credit Scoring: A Comprehensive Review of Models and Predictive Analytics. *Global Journal of Engineering and Technology Advances*, 18 (2), pp. 118-129. Available from: <https://doi.org/10.30574/gjeta.2024.18.2.0029>; Widagdo, P. et al. (2023) Artificial Intelligence in Credit Risk: A Literature Review. *Proceeding of The International Seminar on Business, Economics, Social Science and Technology (ISBEST)*, 3 (1). Available from: <https://doi.org/10.33830/isbest.v3i1.1472>

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. *Official Journal of the European Union* (L 119) 4 May. Available from: <http://data.europa.eu/eli/reg/2016/679/oj> [Accessed 28 March 2026]

³ Brkan, M. (2019) Do Algorithms Rule the World? Algorithmic Decision-making and Data Protection in the Framework of the GDPR and Beyond. *International Journal of Law and Information Technology*, 27 (2), pp. 91-121. Available from: <https://doi.org/10.1093/ijlit/eay017>; Bygrave, L. A. (2019) *Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making*. SSRN Electronic Journal. Available from: <https://doi.org/10.2139/ssrn.3329868>; Tosoni, L. (2021) The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation. *International Data Privacy Law*, 11 (2), pp. 145-162. Available from: <https://doi.org/10.1093/idpl/ipaa024>

⁴ Judgment of 7 December 2023, *OQ v Land Hessen (SCHUFA Holding)*, C-634/21, ECLI:EU:C:2023:957

⁵ Aza, A. (2024) Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context. *Industrial Law Journal*, 53 (4), pp. 840-858. Available from: <https://doi.org/10.1093/indlaw/dwae035>

SCHUFA ruling and EU national case law, demonstrating that explainable AI (“xAI”) is essential for satisfying the prohibition’s transparency obligations.

While focusing on credit scoring, the SCHUFA ruling raises broader issues of transparency, accountability, and algorithmic secrecy across various decision-making contexts.⁶ This paper argues that the qualified prohibition in Article 22 serves as a structural strength, enabling algorithmic systems to operate lawfully while meeting transparency requirements and the anti-rubber-stamping principle established in national case law.

The central research question examines how the SCHUFA ruling and EU national case law delineate the criteria for satisfying a qualified prohibition on ADM under the GDPR and Artificial Intelligence Act (“AI Act”).⁷ While xAI is crucial for fulfilling the transparency requirements of Article 22(3), this study argues that it alone is insufficient. The accountability framework of the GDPR and the risk-based structure of the AI Act underscore the necessity of human oversight, the right to challenge, and auditing.⁸

This study has the following structure: Section 2 reviews the scholarly debate on the right to explanation and the practical challenges of implementing transparency and xAI under Article 22. Section 3 analyzes the SCHUFA ruling and the accompanying national case law, elucidating the concrete doctrinal content of the qualified prohibition. Section 4 addresses cumulative automated decision-making across sectors. Section 5 examines the oversight framework under the GDPR and the AI Act. Section 6 concludes.

⁶ Biber, D. S. E. (2023) *Between Humans and Machines: Judicial Interpretation of the Automated Decision-Making Practices in the EU*. SSRN Electronic Journal., pp. 2-3. Available from: <https://doi.org/10.2139/ssrn.4662152>; Silveira, A. (2023) Automated Individual Decision-making and Profiling [on Case C-634/21 – SCHUFA (Scoring)]. *UNIO – EU Law Journal*, 8 (2), pp. 74-75. Available from: <https://doi.org/10.21814/unio.8.2.4842>

⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (AI Act). Official Journal of the European Union (OJ L 2024/1689) 12 July. Available from: <http://data.europa.eu/eli/reg/2024/1689/oj> [Accessed 28 March 2026]

⁸ Barredo Arrieta, A. et al. (2019) Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI. *Information Fusion*, 58, pp. 82-115. Available from: <https://doi.org/10.1016/j.inffus.2019.12.012>; Doshi-Velez, F. and Kim, B. (2017) *Towards A Rigorous Science of Interpretable Machine Learning*. Available from: <https://doi.org/10.48550/arxiv.1702.08608>; Kaminski, M. (2019) The Right to Explanation, Explained. *Berkeley Technology Law Journal*, 34 (1). Available from: <https://doi.org/10.15779/z38td9n83h>

2. LITERATURE REVIEW

2.1. RIGHT TO EXPLANATION

The right to explanation has emerged as a central theme in GDPR and AI governance discussions. Article 22 grants individuals the right to avoid being subjected to a decision based entirely on automated processing, which results in legal consequences or has a similarly significant impact on them. Legal scholars debate whether this establishes an explicit right to demand algorithmic explanations or merely suggests them through transparency provisions.⁹ Although the GDPR does not mandate detailed explanations for all AI decisions, its transparency obligations (Articles 13–15) and fairness requirements (Article 5) encourage controllers to provide information regarding automated decision logic.

Wachter, Mittelstadt and Floridi¹⁰ argue that the GDPR mandates certain disclosures but does not necessarily constitute a fully comprehensive right to explanation, whereas Selbst and Powles¹¹, and Kaminski¹² assert that the transparency obligations inherently require a degree of explainability that extends beyond mere procedural information. A further jurisprudential development is the position of the CJEU in *Dun and Bradstreet* (C-203/22)¹³, which clarifies that Article 15(1)(h) GDPR obliges controllers to provide relevant information and in a concise, transparent, intelligible form about the automated logic, even if a protected algorithmic trade secret is at stake.

A key interpretive question divided scholars before the CJEU's SCHUFA ruling: does Article 22(1) serve as a default prohibition, or is it a right that individuals must actively assert? The dominant perspective, supported by

⁹ Brkan, M. and Bonnet, G. (2020) Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas. *European Journal of Risk Regulation*, 11 (1), pp. 18-50. Available from: <https://doi.org/10.1017/err.2020.10>; Hamon, R. et al. (2022) Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making. *IEEE Computational Intelligence Magazine*, 17 (1), pp. 72-85. Available from: <https://doi.org/10.1109/mci.2021.3129960>; Wachter, S., Mittelstadt, B. and Floridi, L. (2017) Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7 (2), pp. 76-99. Available from: <https://doi.org/10.1093/idpl/ix005>

¹⁰ Wachter, S., Mittelstadt, B. and Floridi, L. (2017) *op. cit.*, pp. 76-77.

¹¹ Selbst, A. D. and Powles, J. (2017) Meaningful Information and the Right to Explanation. *International Data Privacy Law*, 7 (4), pp. 235-236. Available from: <https://doi.org/10.1093/idpl/ix022>

¹² Kaminski, M. (2019) *op. cit.*, pp. 209-213.

¹³ Judgment of 27 February 2025, *Dun & Bradstreet Austria GmbH v GL*, C-203/22, ECLI:EU:C:2025:117, paras. 55, 57–58, 66.

Brkan¹⁴, Mendoza and Bygrave¹⁵, and the Article 29 Working Party¹⁶, is that Article 22(1) establishes a prohibition in principle, placing the onus on controllers to justify automated decision-making rather than requiring data subjects to object¹⁷. The Article 29 Working Party guidelines are clear in that the provision establishes a general prohibition on solely automated decisions that produce legal or similarly significant effects, regardless of whether the data subject invokes it.

The minority perspective, as articulated by Tosoni¹⁸ and Thouvenin et al.¹⁹, interprets Article 22(1) as a right that necessitates active invocation by the data subject. However, as previously noted, the SCHUFA ruling has resolved this debate by establishing that Article 22(1) applies by default, requiring a lawful basis under Article 22(2) to justify any exception. This interpretation, which treats the provision as a restriction, offers enhanced protection. If individuals had to be informed of an automated decision and then object to trigger safeguards, the practical burden would fall disproportionately on those least equipped to handle it.

Metikoš and Ausloos²⁰ provide a systematic analysis of EU case law on the right to explanation, addressing three core interpretive questions concerning the scope of the right, the content of explanations required, and how explanation rights are balanced against competing interests. Regarding the scope, the authors identify a significant divergence among national courts regarding whether Article 15(1)(h), which requires controllers to provide meaningful information about the logic involved, applies only within the Article 22 framework or extends more broadly, a question that remains fragmented across member states. Regarding the content, the case law consistently holds that explanations must be decision-specific and contestation-enabling, a standard confirmed by the CJEU in *Dun*

¹⁴ Brkan, M. (2019) *op. cit.*, p. 99.

¹⁵ Mendoza, I. and Bygrave, L. A. (2017) *The Right Not to be Subject to Automated Decisions Based on Profiling*. Springer. Available from: https://doi.org/10.1007/978-3-319-64955-9_4

¹⁶ Article 29 Working Party. (2017) *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*. WP251rev.01. Article 29 Working Party. Available from: <https://ec.europa.eu/newsroom/article29/items/612053> [Accessed 28 March 2026]

¹⁷ Aza, A. (2024) *op. cit.*, p. 850; Bygrave, L. A. (2019) *op. cit.*, p. 6.

¹⁸ Tosoni, L. (2021) *op. cit.*, pp. 161-162.

¹⁹ Thouvenin, F, Früh, A. and Henseler, S. (2022) Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right. *European Data Protection Law Review*, 8 (2), p. 198. Available from: <https://doi.org/10.21552/edpl/2022/2/6>

²⁰ Metikoš, L. and Ausloos, J. (2024) The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act. Available from: <https://doi.org/10.31219/osf.io/ezgxf>

and *Bradstreet* (C-203/22)²¹, which established that the primary purpose of Article 15(1)(h) is to enable data subjects to effectively exercise their rights under Article 22(3). Regarding balancing, trade secret and business interest claims cannot justify a categorical refusal to explain, although the selective disclosure permitted to protect proprietary information may limit the practical utility of the right for individuals seeking to scrutinize algorithmic outputs for bias or error.

The stakes of getting explanation rights wrong extend beyond individual cases. Pasquale²² warned that without robust transparency mechanisms, AI-driven systems in domains like credit scoring risk entrenching a "black box society" in which consequential decisions are systematically insulated from scrutiny, reinforcing power imbalances at scale. Selbst and Powles²³ expressed this concern, contending that simply revealing the logic behind models is insufficient to tackle the societal impacts of automated decision-making. Instead, the broader effects on individuals and communities demand solutions that go beyond mere technical explanations. Clifford and Ausloos²⁴ add that fairness, as a core GDPR principle, demands not only transparent processes but a proportionate balance between individual rights and legitimate business interests, a balance that opaque algorithmic systems by definition cannot demonstrate. Edwards and Veale²⁵ distil these concerns into a pointed warning, noting that the search for a right to explanation in the GDPR risks producing a "transparency fallacy", which refers to the appearance of remedy without substantive protection. These critiques collectively reinforce the argument developed in this paper: formal compliance with disclosure obligations is insufficient unless the information provided is genuinely actionable, a standard that xAI methods must meet rather than merely approximate.

The regulatory interpretation of "meaningful information" has been concretely operationalized in enforcement proceedings against Klarna Bank AB. In March 2022, the Swedish Data Protection Authority (IMY) imposed a fine due to deficiencies in transparency concerning the bank's automated

²¹ Dun and Bradstreet. *op. cit.*, par. 57.

²² Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press

²³ Selbst, A. D. and Powles, J. (2017) *op. cit.*, pp. 235-237.

²⁴ Clifford, D. and Ausloos, J. (2018) Data Protection and the Role of Fairness. *Yearbook of European Law*, 37, p. 169. Available from: <https://doi.org/10.1093/yel/yey004>

²⁵ Edwards, L. and Veale, M. (2017) *Slave to the Algorithm. Why a "Right to an Explanation" is Probably Not the Remedy You Are Looking for* [preprint]. pp. 65-67. Available from: <https://doi.org/10.31228/osf.io/97upg>

credit-decision and fraud-detection processes.²⁶ The IMY established a two-pronged standard: data controllers are required to disclose not only the categories of data processed but also the specific circumstances that invariably result in a refusal decision. Klarna's privacy notice, which merely listed data types such as contact, identification, and financial information without elucidating which combinations of factors would definitively lead to rejection, was deemed inadequate to fulfill the requirements of Articles 13(2)(f) and 14(2)(g) of the GDPR. This enforcement action solidifies the doctrinal position affirmed in *Dun and Bradstreet (C-203/22)*²⁷, which stipulates that Article 15(1)(h) of the GDPR necessitates the provision of functionally actionable information regarding automated logic, rather than merely a catalogue of inputs. When applied to credit scoring under the AI Act's Annex III 5(b), this standard mandates that documentation for high-risk systems must be sufficiently detailed to inform a data subject not only that financial data are utilized but also which specific configurations will result in an adverse outcome.

2.2. TECHNICAL AND PRACTICAL CHALLENGES

While the legal framework establishes a clear trajectory toward "actionable" transparency, the practical implementation of these mandates within AI systems remains fraught with difficulty.²⁸ Contemporary AI models, particularly those utilizing machine learning and deep neural networks, frequently function as "black boxes" with decision-making processes that are not easily interpretable.²⁹ This complexity complicates the provision of clear explanations, a difficulty further compounded by the risk that detailed insights into algorithmic processing may reveal trade secrets or proprietary information.³⁰ In practice, many data controllers encounter a disparity

²⁶ Barros Vale, S. and Zanfir-Fortuna, G. (2022) Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities. *Future of Privacy Forum (FPF)*, p. 21. Available from: <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf> [Accessed 28 March 2026]

²⁷ C-203/22, ECLI:EU:C:2025:117, para. 65-66.

²⁸ Eiband, M. et al. (2018) *Bringing Transparency Design into Practice*. Available from: <https://doi.org/10.1145/3172944.3172961>

²⁹ Lipton, Z. C. (2018) The Mythos of Model Interpretability. *Communications of the ACM*, 61 (10), p. 36. Available from: <https://doi.org/10.1145/3233231>; Tamò-Larrieux, A. (2021) Decision-making by Machines: Is the "Law of Everything" Enough. *Computer Law & Security Review*, 41, 105541, p. 6. Available from: <https://doi.org/10.1016/j.clsr.2021.105541>; Wang, Y. (2024) Ethical Considerations of AI in Financial Decision. *Computing and Artificial Intelligence*, 2 (1), 1290. Available from: <https://doi.org/10.59400/cai.v2i1.1290>

³⁰ Edwards, L. and Veale, M. (2017) *op. cit.*, pp. 65-67; Wachter, S., Mittelstadt, B. and Russell, C. (2017) *Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR*. Cornell University, p. 46. Available from: <https://doi.org/10.48550/arxiv.1711.00399>

between regulatory ideals and technological realities when attempting to implement systems that are both high-performing and transparent. However, as determined in *Dun & Bradstreet*(C-203/22)³¹, data subjects must receive an intelligible explanation of how their data are scored, even when trade secrets are cited, requiring any refusal to disclose details to be justified through a balancing test conducted by a court or supervisory authority.

One strategy to address this gap involves employing model-agnostic explanation techniques, such as local interpretable model-agnostic explanations (LIME)³² or SHapley additive explanations (SHAP)³³, which approximate model behavior near specific inputs.³⁴ While these methods provide post-hoc insights without necessitating full parameter disclosure, Doshi-Velez and Kim³⁵ caution that such partial explanations may omit critical logic or remain too abstract for laypersons. Rudin³⁶ takes this critique further, arguing that post-hoc explanations of black-box models are fundamentally inadequate for high-stakes decisions and that interpretable models should be utilized from the outset. Felzmann et al.³⁷ echo this concern, suggesting that even advanced explainability methods struggle to balance accuracy and interpretability effectively, while Miller³⁸ observes that explanations must be user-centric and context-aware to be truly effective.

The legal implications of these technical limits become particularly significant under Article 22(3) GDPR. When a data controller invokes an exception under Article 22(2), the safeguards of Article 22(3) necessitate meaningful human oversight and the ability to challenge the decision. Crucially, this obligation pertains to the comprehensibility of the output for the data subject rather than solely the technical sophistication of the

³¹ C-203/22, ECLI:EU:C:2025:117, par. 75.

³² Ribeiro, M. T., Singh, S. and Guestrin, C. (2016) "Why Should I Trust You?". *ACM Digital Library*. Available from: <https://doi.org/10.1145/2939672.2939778>

³³ Lundberg, S. and Lee, S.-I. (2017) A Unified Approach to Interpreting Model Predictions. *ArXiv* Available from: <https://doi.org/10.48550/arxiv.1705.07874>

³⁴ Klosok, M. and Chlebus, M. M. (2020) *Towards Better Understanding of Complex Machine Learning Models Using Explainable Artificial Intelligence (XAI) – Case of Credit Scoring Modelling*. In: Working Papers. Available from: <https://ideas.repec.org/p/war/wpaper/2020-18.html> [Accessed 28 March 2026]

³⁵ Doshi-Velez, F. and Kim, B. (2017) *op. cit.*, p. 5.

³⁶ Rudin, C. (2018) *Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead*. Cornell University. Available from: <https://doi.org/10.48550/arxiv.1811.10154>

³⁷ Felzmann, H. et al. (2019) Transparency You Can Trust: Transparency Requirements for Artificial Intelligence Between Legal Norms and Contextual Concerns. *Big Data & Society*, 6 (1), 205395171986054. Available from: <https://doi.org/10.1177/2053951719860542>

³⁸ Miller, T. (2018) Explanation in Artificial Intelligence: Insights from the Social Sciences. *Artificial Intelligence*, 267, pp. 1-38. Available from: <https://doi.org/10.1016/j.artint.2018.07.007>

method. Tsakalakis et al.³⁹ operationalize this through a nine-dimensional typology of explanations mapped directly to Article 22(3) and the AI Act's data governance obligations for high-risk systems, such as credit scoring (Annex III 5(b)). This requirement for "actionable" information is further reinforced by sectoral standards, such as the EU Consumer Credit Directive (2023/2225),⁴⁰ which explicitly mandates explanations for creditworthiness assessments. These developments demonstrate that xAI solutions alone are inadequate without the support of human and institutional infrastructure.⁴¹

Furthermore, the implementation of fairness and non-discrimination principles remains a major obstacle. Bias in training data can systematically disadvantage protected groups, and the existence of competing fairness metrics complicates the establishment of a single definition⁴². Accountability becomes fractured when a non-transparent system produces damaging results, making it difficult to pinpoint responsibility among developers, suppliers, and implementers.⁴³ Consequently, genuine accountability necessitates organizational governance structures alongside algorithmic transparency.⁴⁴ This includes robust human oversight, which fails if it amounts to a "rubber stamp"; as Biber⁴⁵ notes, a reviewer lacking the interpretive framework, authority, or practical opportunity to arrive at a conclusion different from the automated output is effectively non-existent.

Finally, the compliance landscape is complicated by the structural distinction between the AI Act's transparency requirements and the GDPR's mandates. Nannini⁴⁶ delineates the tension between transparency as mere

³⁹ Tsakalakis, N. et al. (2024) *A Typology of Explanations for Explainability-by-Design* [preprint]. pp. 16-19, 29-30. Available from: <https://doi.org/10.31235/osf.io/d3awg>

⁴⁰ Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on Credit Agreements for Consumers and Repealing Directive 2008/48/EC. *Official Journal of the European Union* (OJ L 2023/2225) 30 October. Available from: <http://data.europa.eu/eli/dir/2023/2225/oj> and <http://data.europa.eu/eli/dir/2023/2225/oj> [Accessed 28 March 2026]

⁴¹ Ehsan, U. and Riedl, M. (2020) Human-centered Explainable AI: Towards a Reflective Sociotechnical Approach. *ArXiv*. Available from: <https://doi.org/10.48550/arxiv.2002.01092>

⁴² Biber, D. S. E. (2023) *op. cit.*, p. 32; Kaminski, M. E. and Malgieri, G. (2020) Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations. *International Data Privacy Law*, 11 (2), pp. 125-144. Available from: <https://doi.org/10.1093/idpl/11/2/ipaa020>

⁴³ Chopra, P. (2024) Ethical Implications of AI in Financial Services: Bias, Transparency, and Accountability. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10 (5), pp. 306-314. Available from: <https://doi.org/10.32628/cseit241051017>

⁴⁴ Kaminski, M. E. and Malgieri, G. (2020) *op. cit.*, p. 127.

⁴⁵ Biber, D. S. E. (2023) *op. cit.*, p. 32.

⁴⁶ Nannini, L. (2024) Habemus a Right to an Explanation: So What? – A Framework on Transparency-Explainability Functionality and Tensions in the EU AI Act. *Proceedings of*

information provision versus genuine comprehension, suggesting that the AI Act risks producing explanations that are formally provided but substantively inadequate. This creates a risk of regulatory arbitrage, in which systems might fulfill the AI Act's documentation requirements while failing to deliver the "meaningful information" mandated by Article 15(1)(h) GDPR and *Dun & Bradstreet* (C-203/22).⁴⁷ Ebers⁴⁸ identifies a similar weakness in the AI Act's risk categorisation, arguing that its pre-defined closed risk categories reduce risk management obligations largely to risk mitigation rather than genuine risk assessment. Collectively, these challenges highlight that interpretability and accountability must be integrated from the outset,⁴⁹ reinforcing the argument that data protection impact assessments remain an indispensable governance tool that the AI Act alone cannot replace.

These multifaceted challenges suggest that the legal adequacy of an AI system depends less on its technical complexity than on the institutional safeguards surrounding it. The precise boundaries of these safeguards and the criteria for justifying automated processing under the GDPR's restrictive regime have been further clarified by recent judicial interpretations, beginning with the landmark SCHUFA decision.

3. THE SCHUFA DECISION

3.1. THE OVERVIEW OF FACTS

In December 2023, the CJEU delivered a landmark ruling on ADM under the GDPR involving SCHUFA, Germany's major credit bureau. In *OQ v Land Hessen (SCHUFA Holding)*,⁵⁰ the Court held that the automated generation of an individual's credit score could constitute "automated decision-making" under Article 22 GDPR, especially where that score significantly influences third-party loan decisions. SCHUFA had refused to disclose detailed factors and weightings of its scoring process, citing trade secrets. The Court rejected this stance, emphasizing that individuals have a right to understand and challenge automated outputs that affect them.⁵¹

the AAAI/ACM Conference on AI, Ethics, and Society, 7, pp. 1023-1035. Available from: <https://doi.org/10.1609/aies.v7i1.31700>

⁴⁷ *Dun & Bradstreet*, *op. cit.* par. 61.

⁴⁸ Ebers, M. (2024) Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act. *European Journal of Risk Regulation*, 16 (2), pp. 692-693. Available from: <https://doi.org/10.1017/err.2024.78>

⁴⁹ Tamò-Larrieux, A. (2021) *op. cit.*, pp. 15-17.

⁵⁰ of 7 December 2023, *OQ v Land Hessen*, C-634/21, ECLI:EU:C:2023:957

⁵¹ Falletti, E. (2024) Credit Scoring Under Scrutiny by the Court of Justice of the European Union: Brief Remarks on the "SCHUFA Decision. *SSRN Electronic Journal*. Available from: <https://doi.org/10.2139/ssrn.4726282>; Silveira, A. (2023) *op. cit.* pp. 75-77.

The SCHUFA ruling brings crucial clarity to the scope of automated individual decision-making. The CJEU specified that any algorithmically generated assessment qualifies as an automated decision if it significantly shapes a later outcome, such as loan approval, even if nominal human intervention occurs afterward *OQ v Land Hessen (SCHUFA Holding)*.⁵² Consequently, such intermediate automated results cannot be used to circumvent the GDPR by segmenting decisions into separate phases. The Court noted that while profiling is not strictly required for Article 22 to apply, the central factor is whether an automated process substantially impacts an individual. Consistent with this broad interpretation, nominal “human-in-the-loop” arrangements do not exempt data controllers from the regulation’s safeguards if the final decision effectively relies on automated output.⁵³

Hubková⁵⁴ provides further doctrinal grounding for this conclusion in her analysis of EU administrative ADM. Through the concept of “cyber-delegation,” she argues that even when a human official nominally processes the output of an ADM tool, the output of the machine forms the functional core of the decision. Critically, she identifies an “epistemic asymmetry” between law and computation. Legal rules require interpretive flexibility and tolerance of discretion, whereas algorithms demand precise and unambiguous rules. This implies that the choices of the programmer effectively embed legal judgments that remain invisible to the human decision-maker using the tool. Hubková⁵⁵ further distinguishes technical explainability from legal justification, arguing that an explanation of the way a system works does not satisfy the legal obligation to give reasons for a decision. Rudolf & Kováč⁵⁶ reach a complementary conclusion. By analyzing the doctrinal impact of the *SCHUFA* ruling, they confirm that preparatory documents, such as AI-generated outputs used as inputs for formally human decisions, can qualify as autonomous decisions under Article 22(1) GDPR if

⁵² *OQ v Land Hessen, op. cit.*

⁵³ Biber, D. S. E. (2023) *op. cit.* pp. 28-31; Davis, P. and Schwemer, S. F. (2023) Rethinking Decisions Under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making. *SSRN Electronic Journal*, pp. 3-4, Available from: <https://doi.org/10.2139/ssrn.4478107>; Tosoni, L. (2021) *op. cit.* pp. 154-156.

⁵⁴ Hubková, P. (2024) EU Administrative Decision-Making Delegated to Machines – Legal Challenges and Issues. *AUC IURIDICA*, 70 (2), pp. 102-103. Available from: <https://doi.org/10.14712/23366478.2024.25>

⁵⁵ *Ibid*, pp. 117-118.

⁵⁶ Rudolf, G. and Kováč, P. (2024) The Role of Automated Decision-Making in Modern Administrative Law: Challenges and Data Protection Implications. *Central European Public Administration Review*, 22 (2), p. 95. Available from: <https://doi.org/10.17573/cepar.2024.2.04>

they effectively predetermine the outcome. This reinforces the argument that a nominally hybrid process often functions solely as an automated one.

Article 22's reach extends beyond sophisticated machine-learning models to include simple rule-based exclusions. The Finnish Data Protection Ombudsman's 2019 decision against Svea Ekonomi illustrates this point: the DPA found that automatically excluding credit applicants based solely on an age threshold fell within Article 22(1) GDPR. The Ombudsman noted that age alone does not describe solvency or willingness to pay and therefore cannot serve as a decisive factor.⁵⁷ The controller was ordered to provide data subjects with information on the decision's logic, its role in the assessment, and its consequences. This confirms, following Hubková,⁵⁸ that the Article 22 threshold is triggered by the significant effect on the individual rather than the technical architecture of the system.

Additionally, the Court addressed the tension between trade secrecy and transparency. While businesses may protect proprietary methodologies, the CJEU has reiterated that individuals deserve sufficient information to understand and challenge significant automated decisions, thereby rejecting SCHUFA's argument that algorithmic secrecy overrode GDPR obligations.⁵⁹ This doctrine strengthens Article 22 as a practical tool for ensuring meaningful human oversight, reinforcing the need for xAI to make automated processes contestable. Although arising from credit scoring, the Court's reasoning applies to a broad range of high-stakes AI contexts, from employment screening to social-benefits determination.⁶⁰

3.2. THE LESSONS LEARNED FROM THE DECISION

The recent *SCHUFA* ruling reaffirms that organizations utilizing AI-driven credit scoring, or any high-stakes ADM, must prioritize transparency and fairness as fundamental principles of the GDPR *OQ v Land Hessen (SCHUFA Holding)*.⁶¹ Furthermore, the ruling foreshadows the way the AI Act intensifies these obligations. The Court clarified that individuals are entitled to "meaningful information" regarding the logic and implications of automated decisions that affect them *OQ v Land Hessen (SCHUFA Holding)*.⁶² Although credit bureaus may seek to protect trade secrets, the CJEU determined that commercial confidentiality does not supersede the data protection rights of individuals. This decision underscores the imperative

⁵⁷ Barros Vale, S. and Zafir-Fortuna, G. (2022) *op. cit.* p. 46.

⁵⁸ Hubková, P. (2024) *op. cit.* p. 105.

⁵⁹ Falletti, E. (2024) *op. cit.*; Silveira, A. (2023) *op. cit.* pp. 80-81.

⁶⁰ Aza, A. (2024) *op. cit.* p. 855-856; Biber, D. S. E. (2023) *op. cit.*

⁶¹ *OQ v Land Hessen, op. cit.* paras 56-57, 63-66.

⁶² *Ibid.* paras. 56, 63.

of procedural fairness, as highlighted by Clifford & Ausloos⁶³, ensuring that data subjects can comprehend and contest decisions with significant impact.

Significantly, the *SCHUFA* decision highlights the necessity for substantive human intervention. Article 22 of the GDPR mandates that any "human in the loop" must genuinely evaluate automated outcomes rather than merely approve them without scrutiny.⁶⁴ In practice, organizations must strike a balance between avoiding information overload and providing sufficient detail to empower individuals.⁶⁵ The European Data Protection Board ("EDPB") has endorsed the guidelines of the Article 29 Working Party on automated decision-making, confirming the continued authority of those guidelines under the GDPR.⁶⁶ Whittlestone et al.⁶⁷ similarly emphasize that explanations must be intelligible, actionable, and tailored to the intended audience.

An instructive decision by the Portuguese Data Protection Authority (CNPd) in May 2021 anticipated the anti-rubber-stamping doctrine confirmed in *SCHUFA*. This decision involved the assessment of a university regarding the proposed implementation of examination-proctoring software.⁶⁸ The software analyzed the biometric patterns of students via webcam footage to generate a fraud-likelihood score, which professors would use to determine whether to investigate potential irregularities. The university contended that no qualifying ADM existed because professors retained the final authority for decisions. However, the CNPD dismissed this argument, noting that the absence of specific guidelines on the interpretation of scores and the lack of guiding criteria for teachers could lead teachers to validate the decisions of the systems as a rule.⁶⁹

This formulation is particularly significant. What disqualifies a nominally human decision-maker from preventing a "solely automated" classification is precisely the absence of criteria that would enable coherent deviation from the automated output. A human lacking both an interpretive framework and the authority to reach an independent conclusion is functionally equivalent to no human at all, a conclusion subsequently confirmed by the CJEU in

⁶³ Clifford, D. and Ausloos, J. (2018) *op. cit.* pp. 26-28.

⁶⁴ *OQ v Land Hessen, op. cit.* paras. 54, 66.

⁶⁵ Felzmann, H. et al. (2019) *op. cit.*

⁶⁶ Article 29 Working Party. (2017) *op. cit.*

⁶⁷ Whittlestone, J. et al. (2019) The Role and Limits of Principles in AI Ethics. *ACM Digital Library*. Available from: <https://doi.org/10.1145/3306618.3314289>

⁶⁸ Barros Vale, S. and Zafir-Fortuna, G. (2022) *op. cit.* p. 34.

⁶⁹ *Ibid.*

SCHUFA and operationalized in the 2023 Uber appellate decision.⁷⁰ Sarra⁷¹ generalizes this principle doctrinally: the "solely automated" threshold is satisfied unless the controller can demonstrate that a human has specifically and materially intervened in the individual decision in a manner that would have altered the outcome. General monitoring is insufficient, and the burden of proof rests with the controller. This standard aligns directly with case law. What was absent in the CNPD and the 2023 Uber appellate decision, and present in *Caixabank* as explained below, is precisely a demonstrable and outcome-determinative human contribution to the specific decision under review.

These developments must be contextualized within the existing framework of cases in which genuine human judgment was deemed sufficient to exclude a process from Article 22. In January 2021, the Spanish Data Protection Authority (AEPD) determined that Caixabank's client-profiling practices did not constitute ADM under Article 22(1) because the bank's employees exercised independent judgment in making individual credit and pricing decisions based on profiled data.⁷² Notably, the AEPD imposed a combined fine of €6 million for transparency violations, as Caixabank failed to adequately inform data subjects about the profiles being constructed and relied on invalidly bundled consent. This outcome exemplifies a recurring structural pattern in case law: avoiding Article 22 qualification does not exempt controllers from compliance obligations under Articles 5, 6, 13, and 14 of the GDPR.

Furthermore, in a 2022 decision regarding Grindr's content-moderation algorithm, the AEPD found no Article 22 violation because employees analyzed automated signals before deciding whether to remove content or block accounts.⁷³ While this outcome initially appeared straightforward, *post-SCHUFA*, the question is no longer whether a human reviews the output, but whether that human possesses the substantive capacity and procedural opportunity to reach a different conclusion from the indication of the automated system. In scenarios where content moderation scales to millions of items per day, the factual basis for genuine independent human review, rather than the systematic validation of algorithmic signals, must

⁷⁰ Gerechtshof Amsterdam (No. 200.295.747/01). (2023). Available from: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:796> [Accessed 28 March 2026]

⁷¹ Sarra, C. (2025) Artificial Intelligence in Decision-making: A Test of Consistency Between the "EU AI Act" and the "General Data Protection Regulation." *Athens Journal of Law*, 11 (1). pp. 57-58. Available from: <https://doi.org/10.30958/ajl.11-1-3>

⁷² Barros Vale, S. and Zanfir-Fortuna, G. (2022) *op. cit.* p. 32.

⁷³ *Ibid.*

be scrutinized against the CNPD proctoring standard: are there interpretive guidelines, independent criteria, and a genuine opportunity to deviate?

Transparency requirements are essential components of xAI strategies,⁷⁴ however, they create tensions between regulatory compliance and proprietary interests. As noted by the Court, the refusal to disclose algorithmic factors or weightings obstructs data subjects' rights under the GDPR.⁷⁵ Kaminski⁷⁶ cautioned that inadequate explanations could render organizations vulnerable to legal liability and penalties. The AI Act similarly mandates interpretable and accountable AI systems, compelling credit-scoring providers to balance disclosure obligations with the protection of intellectual property.⁷⁷ A concurrent obligation of fairness arises from both the GDPR and the AI Act. Fairness involves preventing discriminatory outcomes through the use of high-quality, representative training data and implementing robust oversight procedures.⁷⁸ In the context of credit scoring, fairness also depends on continuous bias audits and accessible mechanisms for individuals to contest unjust outcomes. This aligns with Clifford and Ausloos⁷⁹ dual framework, wherein procedural fairness necessitates transparent decision-making, while fair balancing seeks to harmonize data subjects' rights with legitimate business interests.

⁷⁴ Binns, R. and Veale, M. (2021) Is That Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR. *International Data Privacy Law*, 11 (4), pp. 319-332. Available from: <https://doi.org/10.1093/idpl/ipab020>

⁷⁵ OQ v Land Hessen, *op. cit.* paras. 63–66.

⁷⁶ Kaminski, M. (2019) *op. cit.*

⁷⁷ Smuha, N. A. (2021) From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence. *Law, Innovation and Technology*, 13 (1), pp. 63-65. Available from: <https://doi.org/10.1080/17579961.2021.1898300>; Veale, M. and Borgesius, F. (2021) Demystifying the Draft EU Artificial Intelligence Act. *ArXiv* Available from: <https://doi.org/10.48550/arxiv.2107.03721>

⁷⁸ Karsai, K. (2021) Algorithmic Decisions within the Criminal Justice Ecosystem and Their Problem Matrix. *International Review of Penal Law / Revue Internationale de Droit Pénal*, 92 (1), pp. 13-30; Karsai, K. (2024) The Use of Algorithms to Support Judicial Decision-Making in Criminal Matters with a Special Focus on Trial Decisions. *Studia Iuridica Lublinensia*, 33 (5), pp. 103-124. Available from: <https://doi.org/10.17951/sil.2024.33.5.103-124>

⁷⁹ Clifford, D. and Ausloos, J. (2018) *op. cit.* pp. 38-39.

4. CUMULATIVE ADM AND ARTICLE 22 GDPR

4.1. THE CUMULATIVE ADM DOCTRINE

Article 22 of the GDPR is typically applied in contexts involving a single, high-stakes automated decision. However, recent scholarly work and the case law examined in this section reveal that continuous or sequential automated processing can collectively exert an impact on individuals that is equally significant to any isolated determination.⁸⁰ Indeed, in some instances, this cumulative effect is more pervasive. The qualified prohibition framework affirmed in the *SCHUFA* is particularly well suited to addressing this phenomenon. Once an automated process generates effects that substantially influence an individual's access to employment, credit, services, or public benefits, Article 22(1) is activated. This requires the controller to establish a lawful basis under Article 22(2), alongside the safeguards of Article 22(3).

A brief methodological note is warranted regarding the utilization of national court and DPA decisions to substantiate an EU-wide doctrinal argument. Article 22 is a directly applicable provision of EU law, characterized by a uniform text, structure, and purpose across all member states; the guidance of the CJEU interpretively governs its national adjudication. The harmonization role of the EDPB under Article 70 GDPR, along with the endorsement of a consistent "significant effects" standard, ensures that enforcement practices converge across member states, even in the absence of a ruling by the CJEU on every factual scenario. The decisions examined in the subsequent section encompass multiple sectors, including gig-economy platform management, public employment services, food delivery, and financial and insurance products, and originate from several member states. Their breadth is analytically significant. It demonstrates that the cumulative ADM scope and significance threshold are not artifacts of any particular national legal culture or economic sector. Instead, they represent a consistent and uniform doctrinal response to the structural characteristics of automated processing, where individual steps may be unremarkable while the aggregate effect is substantial.

Binns and Veale⁸¹ underscore the doctrinal complexities that arise in multistage profiling contexts, emphasizing the ambiguity in determining the location of the decision and whether significance should be assessed based on each individual outcome or the cumulative effect. Concentrating solely on a final and singular output may obscure the impact of preceding automated processes that effectively predetermined results. This perspective transitions the Article 22 inquiry from a binary evaluation of a single decision to a more

⁸⁰ Brkan, M. (2019) *op. cit.*

⁸¹ Binns, R. and Veale, M. (2021) *op. cit.*

nuanced analysis of decision systems as they evolve over time. Importantly, when a controller structures an automated process as a sequence of minor steps to avoid the appearance of a singular decisive moment, regulators and courts may prioritize substance over form. Davis and Schwemer⁸² contend that the term "decision" in Article 22 should be interpreted broadly to encompass algorithmic recommendations and intermediate outputs that effectively shape the fate of an individual. This approach is consistent with the protective purpose of the GDPR: to prevent individuals from being subjected to unchecked algorithmic power, whether exerted in a single instance or through a series of individually minor steps.

4.2.THE QUALIFIED PROHIBITION IN PRACTICE: SECTORAL EVIDENCE

The doctrinal framework has been evaluated across various sectors. The case law analyzed in this section illustrates the consistent application of the qualified prohibition of Article 22. In contexts such as gig-economy platforms, public-sector employment services, and financial and insurance products, national courts and data protection authorities (DPAs) have consistently determined that continuous automated processing meets the significance threshold when it determines or materially influences individuals' access to income, employment, credit, or public benefits.

Gig-economy platform management provides the most extensively litigated illustration. The ride-hailing platform of Uber continuously processes the data of drivers to carry out a series of consequential automated operations: matching drivers with ride requests, setting dynamic prices, detecting fraud signals, and deactivating accounts for alleged violations. Dutch litigation against Uber and its competitor Ola, spanning first-instance judgments in 2021 and an appellate ruling in 2023, charted the significance threshold with precision.⁸³ The Amsterdam District Court declined to find Article 22 violations in relation to temporary fraud-flag suspensions and ride-allocation decisions, treating the former as reversible and the latter as producing only short-term economic effects insufficient to meet the "impactful, long-term or lasting" standard.⁸⁴ By contrast, the same court held that Ola's automated performance-based fines crossed the threshold. Such

⁸² Davis, P. and Schwemer, S. F. (2023) *op. cit.* pp. 3-4.

⁸³ Gerechtshof Amsterdam (2023). *op. cit.*; Rechtbank Amsterdam (No. C/13/692003 / HA RK 20-302) (2021). para. 4.19, 4.24. Available from: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1018> [Accessed 28 March 2026]; Rechtbank Amsterdam (No. C/13/689705 / HA RK 20-258) (2021). paras. 3.1, 4.25, 4.45, 4.47, 4.49, 4.52. Available from: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1019> [Accessed 28 March 2026]

⁸⁴ Barros Vale, S. and Zafir-Fortuna, G. (2022) *op. cit.* p. 36.

penalties have effects that are important enough to deserve attention and significantly affect the conduct or choices of the person concerned, amounting to sanctions that alter the contractual rights of drivers. The court prohibited Ola from continuing this practice, recognizing that even individually modest fines produced a profound cumulative effect on livelihood and behavior.

The procedural sequencing of first-instance cases is instructive for the cumulative ADM argument. Barros Vale & Zanfira-Fortuna⁸⁵ note that the court considered the substantive impact of automated practices on the basis of the available facts before turning to the evidentiary burden of the claimants. The implication is consequential: where longitudinal evidence establishes demonstrable aggregate harm, such as income suppression, systematic access restriction, or behavioral modification over time, a court may apply Article 22 even to individually innocuous automated allocations. The doctrinal challenge for claimants is evidence rather than legal principles.

The 2023 Uber appellate decision resolved a more difficult question: whether account termination through automated fraud detection, nominally reviewed by human staff in Kraków, constituted solely automated processing. The Amsterdam Court of Appeal found that four drivers had been deprived of their livelihoods through algorithmic termination without any genuine opportunity to be heard and that Uber could not substantiate the nature of the alleged human involvement. Accordingly, the court rejected the thin veneer of human oversight and applied Article 22, invoking Article 15(1)(h) GDPR to compel Uber to disclose the algorithms and criteria used in firing decisions.⁸⁶ The case confirmed what Biber⁸⁷ identified as an emerging judicial consensus: the determinative factor is the effect on the individual, not the form in which the decision is structured. Metikoš and Ausloos⁸⁸ synthesize this jurisprudential trajectory, observing that the standard for meaningful human oversight has crystallized around a demanding substantive test. The reviewer must be technically capable of understanding the automated output, procedurally empowered to hear the data subject, and institutionally positioned to reach different conclusions. The remote reviewers of Uber plainly did not meet this test.

The same doctrinal logic was applied by the Italian Data Protection Authority (Garante) to food delivery platforms. In its investigation of Deliveroo, Garante found that an automated rider-ranking system determining access to peak-hour delivery slots constituted a qualifying

⁸⁵ Barros Vale, S. and Zanfira-Fortuna, G. (2022) *op. cit.* p. 37.

⁸⁶ Gerechtshof Amsterdam (2023). *op. cit.*

⁸⁷ Biber, D. S. E. (2023) *op. cit.* pp. 35-36.

⁸⁸ Metikoš, L. and Ausloos, J. (2024) *op. cit.* pp. 13-15.

ADM under Article 22(1). Even if no single shift assignment was decisive in isolation, the pattern of automated allocation materially shaped riders' earnings and career prospects.⁸⁹ In the parallel June 2021 decision concerning Foodinho, Garante specifically rejected the argument that the system escaped Article 22 classification because its parameters had been manually configured by employees. The design-stage involvement of humans does not prevent the runtime application of algorithmic rules from constituting "solely automated" processing. Once deployed, the algorithm operates without case-by-case human input, and Article 22 governs the deployment stage decision.⁹⁰ Together, Deliveroo and Foodinho establish that the algorithmic management of gig workers systematically meets Article 22(1) significance threshold wherever access to income-generating opportunities is at stake.

This qualified prohibition applies with equal force in the public sector, where algorithmic classification systems can determine individuals' access to services and administrative support over extended timeframes. The Italian *Buona Scuola* litigation and the Austrian AMAS case illustrate this with complementary force. In *Buona Scuola*, the Italian Council of State (*Consiglio di Stato*) delivered a landmark 2019 judgment treating the rule-based algorithm of the Ministry of Education for assigning teachers to schools as equivalent to any other administrative act for purposes of legal oversight.⁹¹ The court acknowledged that serial or standardized mass-decision processes can be efficient but warned that public authorities cannot use automation to circumvent the principles governing administrative activity. Full disclosure of the existence of automated decision processes and the algorithms employed was required by the transparency principle, together with adequate opportunities for human intervention and redress. Although argued in administrative-law terms rather than under the GDPR directly, the insistence of the court on transparency and contestability precisely echoes the safeguards of Article 22(3), namely, the right to obtain an explanation, to express one's view, and to contest the outcome.

The Austrian AMAS case confirms that the cumulative significance argument applies to public sector classification systems, irrespective of whether any single output directly terminates an entitlement. The Austrian Public Employment Service deployed the AMAS to classify jobseekers into three tiers based on predicted employment probability, taking into account age, gender, education, caring duties, and health status. Counselors used this

⁸⁹ Barros Vale, S. and Zanfiri-Fortuna, G. (2022) *op. cit.* pp. 38-39.

⁹⁰ Barros Vale, S. and Zanfiri-Fortuna, G. (2022) *op. cit.* p. 13.

⁹¹ Galetta, D.-U. and Pinotti, G. (2023) Automation and Algorithmic Decision-Making Systems in the Italian Public Administration. *CERIDAP*, 2023 (1), pp. 13-23. Available from: <https://doi.org/10.13130/2723-9195/2023-1-7>

classification to allocate support resources, channeling intensive assistance to the middle tier and reducing support to those in the low-opportunity group.⁹² The Austrian Data Protection Authority (Datenschutzbehörde) found the processing unlawful; on appeal, the Federal Administrative Court (BVwG) overturned that finding on the basis of statutory public interest justification. Notwithstanding the outcome on lawfulness, the case confirms the cumulative significance point: assignment to the low-opportunity tier systematically determines access to support, generates a lasting record within public administration, and may influence future interactions across connected systems. Therefore, Article 22 of the analysis in the public sector must engage with the long-run administrative consequences of algorithmic classification, not merely its immediate and discrete output.

Beyond gig-economy and public-sector contexts, the cumulative ADM doctrine operates wherever automated systems generate sequences of consequential processing whose aggregate effect crosses the Article 22(1) significance threshold. During recruitment, algorithmic filtering that systematically prevents categories of applicants from reaching a human reviewer significantly affects employment prospects, even if no individual rejection appears material in isolation.⁹³ In fintech, continuous machine-learning recalibrations of credit limits, suspension scores, and dynamic pricing constitute an ongoing automated assessment whose cumulative financial effect may be substantial, even when no single adjustment is dramatic. The personalized rates decision regarding car-sharing by Garante,⁹⁴ confirmed by the Italian Supreme Court in November 2021, established that continuous behavioral scoring constitutes profiling under Article 4(4) GDPR. The aggregate financial effect of daily recalibration can be substantial, even if no single adjustment is trivial. The *Creditinfo* decision of the Icelandic DPA⁹⁵ adds a cross-sectoral clarification: satisfying Article 15 access obligations by disclosing score factors does not displace Article 22 analysis, which runs in parallel. In healthcare, AI-driven triage and deterioration-risk systems engage Article 22 wherever clinicians lack the interpretive criteria or practical opportunity to deviate from algorithmic outputs, a gap Van Kolfshooten⁹⁶ identified as critical in EU health data law. Across credit, insurance, employment, healthcare, and public

⁹² Barros Vale, S. and Zanfir-Fortuna, G. (2022) *op. cit.* p. 16.

⁹³ Binns, R. and Veale, M. (2021) *op. cit.*

⁹⁴ Barros Vale, S. and Zanfir-Fortuna, G. (2022) *op. cit.* p. 7.

⁹⁵ Barros Vale, S. and Zanfir-Fortuna, G. (2022) *op. cit.* p. 46.

⁹⁶ Van Kolfshooten, H. B. (2024) A Health-conformant Reading of the GDPR's Right Not to be Subject to Automated Decision-making. *Medical Law Review*, 32 (3), pp. 373-391. Available from: <https://doi.org/10.1093/medlaw/fwae029>

benefits, Article 22 is engaged wherever algorithmic classification produces meaningful downstream effects on access to services or opportunities, whether these effects materialize immediately or accumulate over time.

Content moderation represents a domain where Article 22 analysis is complicated by the entry into force of the Digital Services Act (“DSA”)⁹⁷, which now provides the primary EU framework governing automated content-removal and account-suspension decisions for very large online platforms. Whether Article 22 of the GDPR applies in parallel to content moderation decisions that also involve user data profiling remains an open question.⁹⁸ This study does not purport to resolve this issue; the gig-economy and public-sector case law surveyed above provides a more analytically settled illustration of how cumulative automated processing engages in the qualified prohibition of Article 22.

5. BALANCING ACCOUNTABILITY AND INNOVATION: OVERSIGHT OF CUMULATIVE ADM

Robust oversight of cumulative ADM requires a calibrated approach. It is imperative to implement robust oversight mechanisms to prevent the subtle erosion of individual rights through the aggregate functioning of opaque algorithms. However, regulators must avoid adopting an excessively rigid stance that could impede beneficial innovations and the efficient utilization of AI. Data protection law, particularly when interpreted in conjunction with sector-specific regulations, provides mechanisms to achieve this balance by prioritizing accountability and transparency over outright prohibiting automation.

A fundamental aspect of the approach of the GDPR to algorithmic accountability is the mandate for data protection impact assessments (DPIAs) for high-risk processing under Article 35 GDPR. Kaminski and Malgieri⁹⁹ note that DPIAs serve as a form of systemic oversight that complements individual rights, effectively functioning as a “suitable safeguard” when organizations deploy automated decision systems. In the context of cumulative decision-making, a DPIA compels controllers to assess not only each decision in isolation but also the cumulative impact of an AI system on data subjects over time. For instance, a gig platform implementing an algorithmic management tool should evaluate whether its continuous

⁹⁷ Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union* (L 277) 19 October. Available from: <http://data.europa.eu/eli/reg/2022/2065/oj> [Accessed 28 March 2026]

⁹⁸ Davis, P. and Schwemer, S. F. (2023) *op. cit.* pp. 6-7.

⁹⁹ Kaminski, M. E. and Malgieri, G. (2020) *op. cit.* pp. 129, 132.

automated processing and algorithmic management of workers could collectively have a significant effect on the rights and freedoms of those workers. By documenting risks and measures to mitigate them, such as periodic human review of outcomes, bias testing, or setting impact thresholds that trigger human intervention, the controller both complies with the GDPR and potentially prevents harm before it materializes.

Regulators can promote industry-specific algorithmic impact assessments that extend the DPIA concept, ensuring multi-layered explanations and accountability at design stages.¹⁰⁰ Importantly, this ex-ante oversight does not prohibit automated decisions; rather, it requires foresight and responsibility from those who develop and deploy such systems. Kaminski and Malgieri describe this as a shift from mere compliance to an ethic of collaborative governance, where organizations, experts, and regulators collaborate to align AI innovation with data protection values.¹⁰¹ By mandating internal checks like DPIAs and auditing without dictating the precise design of algorithms, the risk-based framework of the GDPR aims to protect individuals while allowing beneficial data-driven practices to evolve under vigilant oversight.

The relationship between the DPIA framework of the GDPR and the Fundamental Rights Impact Assessment (FRIA) under Article 27 of the AI Act is characterized by considerable complexity. Rintamäki et al.¹⁰² conduct an empirical analysis mapping DPIA obligations across all 27 EU Member States against the high-risk classifications of the AI Act, revealing significant regulatory divergence and fragmentation. Their study indicates that sectors with substantial overlap between GDPR high-risk processing and AI Act Annex III categories, such as credit scoring under Annex III 5(b) and employment under Annex III 4, are precisely where coordination failures between national DPAs and the supervisory framework of the AI Act are most pronounced.

Rintamäki et al.¹⁰³ demonstrate that no current DPIA guidance of any member state fully aligns with the requirements of the FRIA, resulting in compliance uncertainty for organizations deploying high-risk AI systems that also process personal data. In the context of Article 22 of the GDPR, this suggests that a DPIA conducted without reference to the FRIA requirements of the AI Act may fail to encompass the full range of systemic risks

¹⁰⁰ Kaminski, M. E. and Malgieri, G. (2020) *op. cit.* pp. 139-140.

¹⁰¹ Kaminski, M. E. and Malgieri, G. (2020) *op. cit.* p. 131.

¹⁰² Rintamäki, T. et al. (2024) *Impact Assessment Requirements in the GDPR vs the AI Act: Overlaps, Divergence, and Implications* [preprint]. Available from: <https://doi.org/10.31219/osf.io/6ghzj>

¹⁰³ Rintamäki, T. et al. (2024) *op. cit.* pp. 25-26.

posed by credit scoring or algorithmic management systems to the rights of data subjects, thereby reinforcing the need for formally coordinated impact assessments. Sarra¹⁰⁴ identifies a more fundamental tension: the human oversight principle under Article 14 of the AI Act mandates competent human monitoring of high-risk AI systems, yet meaningful human involvement is precisely what excludes a decision from the scope of Article 22 GDPR. Consequently, a controller complying with the AI Act may inadvertently negate the stronger protections of Article 22, replacing them with the narrower and residual explanation right of Article 86 of the AI Act instead of the rights to contestation and human intervention found in the GDPR. The proposed solution of Sarra, that only a specific, traceable, and outcome-determinative human intervention suffices to displace Article 22, is further examined in Section 3.2.

The structure of Article 22, which permits ADM when the conditions of Article 22(2) are satisfied and the safeguards of Article 22(3) are operational, inherently reflects an appropriate balance. This provision conditions automation on genuine accountability rather than prohibiting it outright. Regulators can enhance this balance by clarifying that the information obligations under Articles 13–15 of the GDPR apply continuously for cumulative processing, rather than solely at the point of an initial decision. Furthermore, they should confirm that the human oversight mandated by Article 22(3) necessitates real interpretive capacity and the authority to deviate. Standards-based guidance that articulates criteria for when sequential automated processing crosses the significance threshold, similar to the criteria identified in Section 4.1, would enable organizations to design compliant systems proportionately. At the EU level, the DPIA framework of the GDPR and the conformity assessments of the AI Act serve as natural complements. When used together, they can ensure that high-risk automated systems are evaluated both technically and for their impact on individual rights prior to deployment.

Almada¹⁰⁵ offers a sector-specific examination of the implications of the AI Act for financial services, with particular pertinence to the credit-scoring context central to the *SCHUEA* litigation. By analyzing the risk-based architecture of the AI Act within the framework of financial regulation, Almada affirms that credit scoring under Annex III 5(b) exemplifies a scenario where the high-risk classification of the AI Act directly intersects with the procedural safeguards of Article 22 GDPR. He highlights the concern

¹⁰⁴ Sarra, C. (2025) *op. cit.* pp. 52-55.

¹⁰⁵ Almada, M. (2025) *The EU AI Act: Logic, Content, and Implications for Finance*. SSRN *Electronic Journal*. Available from: <https://doi.org/10.2139/ssrn.5125735>

that the AI Act may pose a barrier to AI innovation in European financial markets.¹⁰⁶ This paper contends that this concern is best addressed not by relaxing transparency and oversight standards, but by ensuring that the qualified prohibition framework of Article 22 GDPR provides the doctrinal flexibility necessary to accommodate beneficial ADM while requiring genuine accountability mechanisms that are operationally proportionate to the scale and nature of the automated process involved.

6. CONCLUSION

The case law surveyed in this paper demonstrates that Article 22 GDPR functions as a qualified prohibition. It is a conditional framework that permits ADM where a lawful basis under Article 22(2) is established and the safeguards of Article 22(3) are genuinely operative, carrying real substantive weight in each of those conditions. The ruling of the CJEU in *SCHUFA* confirmed the default applicability of the prohibition and its resistance to circumvention through trade secrecy. Meanwhile, national case law, spanning *Buona Scuola*, *Uber/Ola*, *Deliveroo*, *Foodinho*, the Austrian *AMAS* litigation, and the *Grindr* decision of the Spanish AEPD, has given the qualified character of that prohibition its concrete operational content. Article 22 is engaged wherever automated processing produces effects that meaningfully shape the access of an individual to employment, credit, services, or public benefits, whether through a single high-stakes decision or the accumulation of sequential automated processing steps whose aggregate impact crosses the significance threshold.

What that threshold requires can now be stated with doctrinal precision. The determinative distinction is between transactional non-selection and positional assessment. Transactional non-selection occurs when an automated process fails to connect a data subject with a particular opportunity on a given instance; examples include a ride that is not assigned, a delivery slot that is not offered, or a job posting that is not surfaced. Such outcomes are reversible, leave the data subject's standing within the platform intact, and produce no record that shapes future interactions. In contrast, a positional assessment occurs when the algorithm renders a judgment about the individual, such as flagging, penalizing, downranking, or reclassifying them on the basis of a behavioral evaluation that alters their position within the system and thereby shapes the universe of opportunities available to them going forward.

An automated output crosses the significance threshold of Article 22(1) when it constitutes a positional assessment of this kind: one that is not

¹⁰⁶ Almada, M. (2025) *op. cit.* p. 111.

readily reversible by the action of the data subject and is determinative of access to a substantial interest, whether livelihood, income-generating opportunity, credit, employment, or public benefit. The *Ola/Uber* contrast operationalizes this directly: a single non-assigned ride is a transactional non-selection and does not meet the test, whereas an automated fine altering contractual rights is a positional sanction that does. The peak-hour ranking system of *Deliveroo* falls on the positional side because it does not merely allocate individual slots but recalibrates the standing of the courier within the allocation hierarchy of the platform across all future interactions. This distinction has broad application to two-sided marketplace platforms, including ride-hailing, food delivery, freelance labor markets, and dynamic pricing systems, and provides a workable doctrinal criterion for controllers and DPAs assessing the applicability of Article 22 in algorithmic brokerage contexts.

Within the perimeter so defined, the Article 22(2) exceptions do not dissolve the obligation. They are the conditions on which ADM is permitted, and Article 22(3) safeguards are the substantive price of that permission: human reviewers must be genuinely capable of deviating from algorithmic outputs, and meaningful information about automated logic must be provided in a form that enables actual contestation rather than merely formal acknowledgement. xAI methods are the technical infrastructure through which the latter obligation is dischargeable in complex machine-learning environments. Risk-based regulatory strategies, including data protection impact assessments, regular audits, and clarity around decision logic, complement this framework by bridging the gap between legal mandates and the operational complexity of modern machine-learning systems, and xAI must be accompanied by the institutional infrastructure that makes its outputs genuinely actionable for data subjects rather than formally adequate for controllers.

Constraining purely automated decision-making under Article 22 does not ban innovation. It reaffirms that the autonomy and dignity of an individual, which are central themes of the GDPR, must be upheld even amid the large-scale deployment of AI. The analysis of cumulative automated decisions in this study reveals how incremental steps, each seemingly trivial, can aggregate into serious risks to rights and freedoms. Recognizing these potential harms ensures that controllers cannot sidestep accountability by fragmenting decision-making processes into smaller parts.

Several limitations mark the boundaries of this analysis and point toward future research. The paper does not resolve whether Article 22 GDPR applies in parallel with the DSA to content moderation decisions that also involve

the profiling of personal data, an open doctrinal question whose resolution requires dedicated treatment. The coordination gaps between the DPIA framework of the GDPR and the FRIA of the AI Act, mapped by Rintamäki et al.¹⁰⁷, call for further empirical and normative work on how supervisory authorities should manage overlapping impact assessment obligations. More fundamentally, the individual-focused architecture of Article 22 inadequately addresses collective and group-level harms from systematic algorithmic disadvantage. Future legislative development may need to directly engage this dimension.

LIST OF REFERENCES

- [1] Addy, W. et al. (2024) AI in Credit Scoring: A Comprehensive Review of Models and Predictive Analytics. *Global Journal of Engineering and Technology Advances*, 18 (2), pp. 118-129. Available from: <https://doi.org/10.30574/gjeta.2024.18.2.0029>
- [2] Almada, M. (2025) The EU AI Act: Logic, Content, and Implications for Finance. *SSRN Electronic Journal*. Available from: <https://doi.org/10.2139/ssrn.5125735>
- [3] Article 29 Working Party. (2017) *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*. WP251rev.01. Article 29 Working Party. Available from: <https://ec.europa.eu/newsroom/article29/items/612053>
- [4] Aza, A. (2024) Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in *SCHUFA Holding (Scoring)* in the Labour Context. *Industrial Law Journal*, 53 (4), pp. 840-858. Available from: <https://doi.org/10.1093/indlaw/dwae035>
- [5] Barredo Arrieta, A. et al. (2019) Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI. *Information Fusion*, 58, pp. 82-115. Available from: <https://doi.org/10.1016/j.inffus.2019.12.012>
- [6] Barros Vale, S. and Zafir-Fortuna, G. (2022) Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities. *Future of Privacy Forum (FPF)*. Available from: <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf>
- [7] Biber, D. S. E. (2023) Between Humans and Machines: Judicial Interpretation of the Automated Decision-Making Practices in the EU. *SSRN Electronic Journal*. Available from: <https://doi.org/10.2139/ssrn.4662152>

¹⁰⁷ Rintamäki, T. et al. (2024) *op. cit.* pp. 25-26.

- [8] Binns, R. and Veale, M. (2021) Is That Your Final Decision? Multi-stage Profiling, Selective Effects, and Article 22 of the GDPR. *International Data Privacy Law*, 11 (4), pp. 319-332. Available from: <https://doi.org/10.1093/idpl/ipab020>
- [9] Brkan, M. (2019) Do Algorithms Rule the World? Algorithmic Decision-making and Data Protection in the Framework of the GDPR and Beyond. *International Journal of Law and Information Technology*, 27 (2), pp. 91-121. Available from: <https://doi.org/10.1093/ijlit/eay017>
- [10] Brkan, M. and Bonnet, G. (2020) Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas. *European Journal of Risk Regulation*, 11 (1), pp. 18-50. Available from: <https://doi.org/10.1017/err.2020.10>
- [11] Bygrave, L. A. (2019) Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making. *SSRN Electronic Journal*. Available from: <https://doi.org/10.2139/ssrn.3329868>
- [12] Chopra, P. (2024) Ethical Implications of AI in Financial Services: Bias, Transparency, and Accountability. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10 (5), pp. 306-314. Available from: <https://doi.org/10.32628/cseit241051017>
- [13] Clifford, D. and Ausloos, J. (2018) Data Protection and the Role of Fairness. *Yearbook of European Law*, 37, pp. 130-187. Available from: <https://doi.org/10.1093/yel/yey004>
- [14] Davis, P. and Schwemer, S. F. (2023) Rethinking Decisions Under Article 22 of the GDPR: Implications for Semi-Automated Legal Decision-Making. *SSRN Electronic Journal*. Available from: <https://doi.org/10.2139/ssrn.4478107>
- [15] Doshi-Velez, F. and Kim, B. (2017) Towards A Rigorous Science of Interpretable Machine Learning. *ArXiv*. Available from: <https://doi.org/10.48550/arxiv.1702.08608>
- [16] Judgment of 7 December 2023, *OQ v Land Hessen (SCHUFA Holding)*, C-634/21, ECLI:EU:C:2023:957.
- [17] Judgment of 27 February 2025, *Dun & Bradstreet Austria GmbH v GL*, C-203/22, ECLI:EU:C:2025:117.
- [18] Ebers, M. (2024) Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act. *European Journal of Risk Regulation*, 16 (2), pp. 684-703. Available from: <https://doi.org/10.1017/err.2024.78>

- [19] Edwards, L. and Veale, M. (2017) *Slave to the Algorithm? Why a "Right to an Explanation" is Probably Not the Remedy You Are Looking for* [preprint]. Available from: <https://doi.org/10.31228/osf.io/97upg>
- [20] Ehsan, U. and Riedl, M. (2020) Human-centered Explainable AI: Towards a Reflective Sociotechnical Approach. *ArXiv*. Available from: <https://doi.org/10.48550/arxiv.2002.01092>
- [21] Eiband, M. et al. (2018) Bringing Transparency Design into Practice. *ACM Digital Library*. pp. 211-223. Available from: <https://doi.org/10.1145/3172944.3172961>
- [22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. *Official Journal of the European Union* (L 119) 4 May. Available from: <http://data.europa.eu/eli/reg/2016/679/oj>
- [23] Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union* (L 277) 19 October. Available from: <http://data.europa.eu/eli/reg/2022/2065/oj>
- [24] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (AI Act). *Official Journal of the European Union* (OJ L 2024/1689) 12 July. Available from: <http://data.europa.eu/eli/reg/2024/1689/oj>
- [25] Falletti, E. (2024) Credit Scoring Under Scrutiny by the Court of Justice of the European Union: Brief Remarks on the "SCHUFA Decision". *SSRN Electronic Journal*. Available from: <https://doi.org/10.2139/ssrn.4726282>
- [26] Felzmann, H. et al. (2019) Transparency You Can Trust: Transparency Requirements for Artificial Intelligence Between Legal Norms and Contextual Concerns. *Big Data & Society*, 6 (1), 205395171986054. Available from: <https://doi.org/10.1177/2053951719860542>
- [27] Galetta, D.-U. and Pinotti, G. (2023) Automation and Algorithmic Decision-Making Systems in the Italian Public Administration. *CERIDAP*, 2023 (1), pp. 13-23. Available from: <https://doi.org/10.13130/2723-9195/2023-1-7>
- [28] Gerechtshof Amsterdam (No. 200.295.747/01) (2023). Available from: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:796>
- [29] Hamon, R. et al. (2022) Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making.

- IEEE Computational Intelligence Magazine*, 17 (1), pp. 72-85. Available from: <https://doi.org/10.1109/mci.2021.3129960>
- [30] Hubková, P. (2024) EU Administrative Decision-Making Delegated to Machines – Legal Challenges and Issues. *AUC IURIDICA*, 70 (2), pp. 101-119. Available from: <https://doi.org/10.14712/23366478.2024.25>
 - [31] Kaminski, M. (2019) The Right to Explanation, Explained. *Berkeley Technology Law Journal*, 34 (1). Available from: <https://doi.org/10.15779/z38td9n83h>
 - [32] Kaminski, M. E. and Malgieri, G. (2020) Algorithmic Impact Assessments Under the GDPR: Producing Multi-layered Explanations. *International Data Privacy Law*, 11 (2), pp. 125-144. Available from: <https://doi.org/10.1093/idpl/ipaa020>
 - [33] Karsai, K. (2021) Algorithmic Decisions within the Criminal Justice Ecosystem and Their Problem Matrix. *International Review of Penal Law / Revue Internationale de Droit Pénal*, 92 (1), pp. 13-30.
 - [34] Karsai, K. (2024) The Use of Algorithms to Support Judicial Decision-Making in Criminal Matters with a Special Focus on Trial Decisions. *Studia Iuridica Lublinensia*, 33 (5), pp. 103-124. Available from: <https://doi.org/10.17951/sil.2024.33.5.103-124>
 - [35] Kłosok, M. and Chlebus, M. M. (2020) Towards Better Understanding of Complex Machine Learning Models Using Explainable Artificial Intelligence (XAI) – Case of Credit Scoring Modelling. In: *Working Papers*. Available from: <https://ideas.repec.org/p/war/wpaper/2020-18.html> [Accessed 28 March 2026]
 - [36] Lipton, Z. C. (2018) The Mythos of Model Interpretability. *Communications of the ACM*, 61 (10), pp. 36-43. Available from: <https://doi.org/10.1145/3233231>
 - [37] Lundberg, S. and Lee, S.-I. (2017) A Unified Approach to Interpreting Model Predictions. *ArXiv*. Available from: <https://doi.org/10.48550/arxiv.1705.07874>
 - [38] Mendoza, I. and Bygrave, L. A. (2017) *The Right Not to be Subject to Automated Decisions Based on Profiling*. Springer. pp. 77-98. Available from: https://doi.org/10.1007/978-3-319-64955-9_4
 - [39] Metikoš, L. and Ausloos, J. (2024) *The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act* [preprint]. Available from: <https://doi.org/10.31219/osf.io/ezgxf>

- [40] Miller, T. (2018) Explanation in Artificial Intelligence: Insights from the Social Sciences. *Artificial Intelligence*, 267, pp. 1-38. Available from: <https://doi.org/10.1016/j.artint.2018.07.007>
- [41] Nannini, L. (2024) Habemus a Right to an Explanation: So What? – A Framework on Transparency-Explainability Functionality and Tensions in the EU AI Act. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 7, pp. 1023-1035. Available from: <https://doi.org/10.1609/aies.v7i1.31700>
- [42] Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.
- [43] Rechtbank Amsterdam (No. C/13/692003 / HA RK 20-302) (2021). Available from: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1018> [Accessed 28 March 2026]
- [44] Rechtbank Amsterdam (No. C/13/689705 / HA RK 20-258) (2021). Available from: <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1019> [Accessed 28 March 2026]
- [45] Ribeiro, M. T., Singh, S. and Guestrin, C. (2016) Why Should I Trust You?. *KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. pp. 1135-1144. Available from: <https://doi.org/10.1145/2939672.2939778>
- [46] Rintamäki, T. et al. (2024) *Impact Assessment Requirements in the GDPR vs the AI Act: Overlaps, Divergence, and Implications* [preprint]. Available from: <https://doi.org/10.31219/osf.io/6qhzj>
- [47] Rudin, C. (2018) Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. *ArXiv*. Available from: <https://doi.org/10.48550/arxiv.1811.10154>
- [48] Rudolf, G. and Kováč, P. (2024) The Role of Automated Decision-Making in Modern Administrative Law: Challenges and Data Protection Implications. *Central European Public Administration Review*, 22 (2), pp. 83-108. Available from: <https://doi.org/10.17573/cepar.2024.2.04>
- [49] Sarra, C. (2025) Artificial Intelligence in Decision-making: A Test of Consistency Between the “EU AI Act” and the “General Data Protection Regulation”. *Athens Journal of Law*, 11 (1), pp. 45-62. Available from: <https://doi.org/10.30958/ajl.11-1-3>
- [50] Selbst, A. D. and Powles, J. (2017) Meaningful Information and the Right to Explanation. *International Data Privacy Law*, 7 (4), pp. 233-242. Available from: <https://doi.org/10.1093/idpl/ix022>

- [51] Silveira, A. (2023) Automated Individual Decision-making and Profiling [on Case C-634/21 – SCHUFA (Scoring)]. *UNIO – EU Law Journal*, 8 (2), pp. 74-85. Available from: <https://doi.org/10.21814/unio.8.2.4842>
- [52] Smuha, N. A. (2021) From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence. *Law, Innovation and Technology*, 13 (1), pp. 57-84. Available from: <https://doi.org/10.1080/17579961.2021.1898300>
- [53] Tamò-Larrieux, A. (2021) Decision-making by Machines: Is the “Law of Everything” Enough? *Computer Law & Security Review*, 41, 105541. Available from: <https://doi.org/10.1016/j.clsr.2021.105541>
- [54] Thouvenin, F., Früh, A. and Henseler, S. (2022) Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right? *European Data Protection Law Review*, 8 (2), pp. 183-198. Available from: <https://doi.org/10.21552/edpl/2022/2/6>
- [55] Tosoni, L. (2021) The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation. *International Data Privacy Law*, 11 (2), pp. 145-162. Available from: <https://doi.org/10.1093/idpl/ipaa024>
- [56] Tsakalakis, N. et al. (2024) *A Typology of Explanations for Explainability-by-Design* [preprint]. Available from: <https://doi.org/10.31235/osf.io/d3awg>
- [57] Van Kolschooten, H. B. (2024) A Health-conformant Reading of the GDPR’s Right Not to be Subject to Automated Decision-making. *Medical Law Review*, 32 (3), pp. 373-391. Available from: <https://doi.org/10.1093/medlaw/fwa029>
- [58] Veale, M. and Borgesius, F. (2021) Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International* (2021) 22(4) 97-112 Available from: <https://doi.org/10.48550/arxiv.2107.03721>
- [59] Wachter, S., Mittelstadt, B. and Floridi, L. (2017) Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7 (2), pp. 76-99. Available from: <https://doi.org/10.1093/idpl/ipx005>
- [60] Wachter, S., Mittelstadt, B. and Russell, C. (2017) Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *ArXiv*. Available from: <https://doi.org/10.48550/arxiv.1711.00399>
- [61] Wang, Y. (2024) Ethical Considerations of AI in Financial Decision. *Computing and Artificial Intelligence*, 2 (1), 1290. Available from: <https://doi.org/10.59400/cai.v2i1.1290>

- [62] Whittlestone, J. et al. (2019) The Role and Limits of Principles in AI Ethics: Towards a Focus on Tensions, *AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*. pp. 195-200. Available from: <https://doi.org/10.1145/3306618.3314289>
- [63] Widagdo, P. et al. (2023) Artificial Intelligence in Credit Risk: A Literature Review. *Proceeding of The International Seminar on Business, Economics, Social Science and Technology (ISBEST)*, 3 (1). Available from: <https://doi.org/10.33830/isbest.v3i1.1472>

DOI 10.5817/MUJLT2026-42766

EMBEDDING A HARMONISED EU IDENTITY SYSTEM INTO A MATURE NATIONAL E-STATE: AN ESTONIAN CASE STUDY

by

YULIIA KRAVCHENKO * THOMAS HOFFMANN [†]
ERIC BLAKE JACKSON [‡]

The implementation of the European Digital Identity (EUDI) Wallet is among the EU's most ambitious cross-border digital identity initiatives undertaken within the EU. Estonia, a country often regarded as a digital frontrunner, received an EUDI Wallet Minimum Viable Product (MVP) from the private Estonian company, Cybernetica, in June 2024, enabling credential issuance independent of physical ID cards, selective disclosure supported by privacy-preserving cryptography, and a modular design aligned with the EU Architecture and Reference Framework (ARF). While Estonia's existing identity and interoperability infrastructure provides strong continuity in trust, assurance, and security, the transition produces frictions centred on the redistribution of control, data minimisation and presentation, portability, and cross-border interoperability. The analysis therefore indicates that the principal challenge is not establishing baseline legal compliance, but aligning governance, supervision, liability, and recovery support with a wallet-mediated transaction chain during a period of channel coexistence.

KEY WORDS

EUDI Wallet, Digital Identity, Trust Services, Interoperability

* Yuliia Kravchenko; Department of Software Science, TalTech – Tallinn University of Technology, Estonia; Early Stage Researcher; E-mail: yuliia.kravchenko@taltech.ee

[†] Dr. Thomas Hoffmann; Department of Law, TalTech – Tallinn University of Technology, Estonia; Tenured Associate Professor; Faculty of Law, Palacký University, Olomouc, Czechia; Research Fellow; E-mail: thomas.hoffmann@taltech.ee

[‡] Dr. Eric Blake Jackson; Department of Software Science, TalTech – Tallinn University of Technology, Estonia; Researcher and Programme Director; E-mail: eric.jackson@taltech.ee

1. INTRODUCTION

Digital identity infrastructure is a fundamental enabling layer for public and private digital services, supporting authentication, access to e-services, identity proofing and the broader trust environment in which electronic signatures and certificates are issued and used. Within the European Union, the original eIDAS framework¹ provided mutual recognition of notified national electronic identification schemes, but cross-border uptake has remained uneven, and many services continue to rely on fragmented, country-specific identity solutions.² The European Digital Identity (EUDI) Wallet initiative raised the ambition by offering a wallet-centric ecosystem, enabling individuals to store credentials and present them across borders.³

Estonia, a country widely recognised as a mature e-state, already operates high-assurance identity, signature, and interoperability infrastructure at national scale.⁴ Consequently, embedding a harmonised EU identity layer into a highly institutionalised ecosystem may produce transition frictions that differ in kind and intensity from those faced in less digitally mature or less widely adopted national contexts. Hence, the research gap addressed in this paper concerns the harmonisation of a new wallet-centric trust model⁵ with the existing eID regime in Estonia.

¹ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. Official Journal of the European Union L 257, 28 August 2014, pp. 73-114. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910> [Accessed 3 June 2026]

² Dumortier, J. (2016) Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation). [online] Available from: <https://ssrn.com/abstract=2855484> [Accessed 3 June 2026]; Lips, S., Bhargava, N. and Draheim, D. (2020) eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. In: Chugunov, A. et al. (eds.) *Electronic Governance and Open Society: Challenges in Eurasia (EGOSE 2020)*. Communications in Computer and Information Science, vol. 1349. Cham: Springer, pp. 75-89. Available from: https://doi.org/10.1007/978-3-030-67238-6_6 [Accessed 3 June 2026]; Aavik, G. and Krimmer, R. (2016) Integrating Digital Migrants: Solutions for Cross-Border Identification from E-Residency to eIDAS. A Case Study from Estonia. In: Scholl, H. J. et al. (eds.) *Electronic Government (EGOV 2016)*. Lecture Notes in Computer Science, vol. 9820. Cham: Springer, pp. 151-163. Available from: https://doi.org/10.1007/978-3-319-44421-5_12 [Accessed 3 June 2026]

³ Babel, M. et al. (2025) Self-Sovereign Identity and Digital Wallets. *Electronic Markets*, 35, art. 28. Available from: <https://doi.org/10.1007/s12525-025-00772-0> [Accessed 3 June 2026]

⁴ Gakh, V. et al. (2024) Enhancing Privacy Risk Modeling in Practice: A Case Study of an E-Justice System. *IEEE Access*, 12, pp. 183851-183874. Available from: <https://doi.org/10.1109/ACCESS.2024.3509332> [Accessed 3 June 2026]

⁵ Degen, K. and Teubner, T. (2024) Wallet Wars or Digital Public Infrastructure? Orchestrating a Digital Identity Data Ecosystem from a Government Perspective. *Electronic Markets*, 34, art. 50. Available from: <https://doi.org/10.1007/s12525-024-00731-1> [Accessed 3 June 2026]

The Estonian case is therefore analytically valuable because the implementation question is not whether an identity infrastructure can be upgraded, but how a mature and highly institutionalised public-service model can absorb a holder-controlled, attribute-centric and cross-border wallet regime without losing existing assurance, usability and institutional clarity.

To address the presented research gap, this study answers the following research questions:

- How does Estonia's eID ecosystem compare to the new EUDI Wallet ecosystem?
- What frictions arise during the implementation of the EUDI Wallet in Estonia?

The paper is organised as follows: Section 2 reviews Estonia's existing digital identity ecosystem, emphasizing the distribution of identity functions across credentials, authentication mediation, and interoperability infrastructure. Section 3 introduces the EUDI Wallet initiative, focusing on eIDAS 2.0, the EU Architecture and Reference Framework (ARF), and Estonia's early implementation developments. Section 4 outlines the research design and methodology. Section 5 presents the theoretical frameworks employed in the analysis, including institutional theory and an identity-management taxonomy. Section 6 reports the comparative results. Section 7 discusses the legal risk and principal ambiguities arising under eIDAS 2.0 and outlines the implications for Estonia's implementation strategy. Section 8 sets out concrete recommendations and policy/design implications. Section 9 concludes with an outlook on embedding the wallet model within a mature e-state.

2. ESTONIAN ECOSYSTEM OVERVIEW

Estonia's current digital identity ecosystem is built around state-issued electronic identity credentials (ID-card and Mobile-ID) and a widely adopted private solution (Smart-ID). Most public e-services consume authentication through the state gateway TARA, which brokers multiple credential types, while backend systems exchange data through X-Road, a secure interoperability layer that enables controlled access to authoritative registries without centralising data. This section provides the institutional and operational context for the comparison. The legal basis for state-issued credentials is the Identity Documents Act (*Isikut tõendavate dokumentide*

seadus, ITDS),⁶ while authoritative identity attributes are maintained under the Population Register Act (*Rahvastikuregistri seadus*, RRS).⁷ The Estonian Information System Authority (RIA) acts as the supervisory body for trust services under Article 17 eIDAS.⁸

2.1.ID CARD

The Estonian electronic identity card (ID-card) is the core state-issued credential enabling strong authentication and qualified electronic signatures for e-services. It is backed by national legislation governing issuance and use of identity documents and is widely integrated across public and private services. The card's cryptographic functions and unique personal identifier support high-assurance identification and interoperability across administrative systems.⁹

2.2.MOBILE ID

Mobile-ID is a SIM-based authentication and signature solution that enables the same core eID functions as the ID-card through mobile devices¹⁰. It is widely used for accessing e-services and signing¹¹ and is typically consumed via the TARA gateway alongside other credential types. Similarly to the ID-card, Mobile-ID is treated as a notified electronic identification means within the EU eIDAS framework (notification under Article 9 Regulation 910/2014), while its signature functionality remains part of the trust-services environment rather than an electronic-identification function as such.¹²

⁶ Isikut Tõendavate Dokumentide Seadus [Identity Documents Act]. Republic of Estonia. Tallinn: Riigi Teataja. In Estonian. Available from: <https://www.riigiteataja.ee/akt/102072013047?leiaKehtiv=> [Accessed 3 June 2026]

⁷ Rahvastikuregistri Seadus [Population Register Act]. Republic of Estonia. Tallinn: Riigi Teataja. In Estonian/English. Available from: <https://www.riigiteataja.ee/en/eli/ee/511012023005/consolide/current> [Accessed 3 June 2026]

⁸ Regulation (EU) No 910/2014, Art. 17.

⁹ European Commission. (n.d.) Estonia. [online] eIDAS Community. Available from: <https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/62885749/Estonia> [Accessed 3 June 2026]

¹⁰ Laud, P. and Roos, M. (2009) Formal Analysis of the Estonian Mobile-ID Protocol. In: Jøsang, A., Maseng, T. and Knapskog, S. J. (eds.) Identity and Privacy in the Internet Age (NordSec 2009). Lecture Notes in Computer Science, vol. 5838. Berlin, Heidelberg: Springer, pp. 271-286. Available from: https://doi.org/10.1007/978-3-642-04766-4_19 [Accessed 3 June 2026]

¹¹ Tsap, V., Lips, S. and Draheim, D. (2020) Analysing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. In: Kõ, A. et al. (eds.) Electronic Government and the Information Systems Perspective (EGOVIS 2020). Lecture Notes in Computer Science, vol. 12394. Cham: Springer, pp. 159-173. Available from: https://doi.org/10.1007/978-3-030-58957-8_12 [Accessed 3 June 2026]

¹² European Commission. (n.d.) Estonia. [online] eIDAS Community. Available from: <https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/62885749/Estonia> [Accessed 3 June 2026]

2.3.SMART ID

Smart-ID is a private authentication and signing solution that is widely adopted in Estonia, especially in the private sector. It complements the state-issued credentials and is commonly offered as an additional authentication channel for services via TARA and other integrations.¹³

From a service-provider perspective, Smart-ID has become an important authentication channel because it offers a relatively low-friction user experience while still operating within the regulated national trust framework. Its use alongside state-issued credentials illustrates the public-private partnership model that characterises Estonia's digital identity infrastructure.¹⁴

For the purposes of the comparison, ID-card and Mobile-ID are analysed primarily as state-issued electronic identification and signature-capable credentials, whereas Smart-ID is analysed as a widely used private authentication and signing channel operating within Estonia's regulated national trust and service-delivery environment.

2.4.X-ROAD AND TARA

Although X-Road and TARA are not electronic identification means, they are critical to the legal and practical operation of Estonia's e-state. X-Road is Estonia's nationwide interoperability infrastructure for secure data exchange between information systems.¹⁵ In practice, X-Road acts as the 'backbone' that allows digital services to assemble required information from multiple registries without building point-to-point integrations.

TARA is Estonia's state authentication service that brokers user authentication for public-sector e-services.¹⁶ Instead of each service integrating separately with ID-card, Mobile-ID and Smart-ID, service providers can integrate once with TARA and rely on it to manage the

¹³ Kattel, R. and Mergel, I. (2019) Estonia's Digital Transformation: Mission Mystique and the Hiding Hand. In: Compton, M. E. and 't Hart, P. (eds.) *Great Policy Successes*. Oxford: Oxford University Press, pp. 143-160. Available from: <https://doi.org/10.1093/oso/9780198843719.003.0008> [Accessed 3 June 2026]

¹⁴ Lips, S. et al. (2023) Management of National eID Infrastructure as a State-Critical Asset and Public-Private Partnership: Learning from the Case of Estonia. *Information Systems Frontiers*, 25, pp. 2439-2456. Available from: <https://doi.org/10.1007/s10796-022-10363-5> [Accessed 3 June 2026]

¹⁵ Riigi Infosüsteemi Amet. (n.d.) Data Exchange Layer X-tee. [online] Tallinn: RIA. Available from: <https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee> [Accessed 3 June 2026]

¹⁶ id.ee. (2024) Trust Services: Authentication Services. [online] Tallinn: id.ee. Available from: <https://www.id.ee/en/article/trust-services-authentication-services/> [Accessed 3 June 2026]

authentication protocol flow and return verified identity attributes.¹⁷ This design has supported rapid service onboarding and consistent authentication assurance across the public sector.

This matters for the EUDIW because the wallet may displace part of the interaction pattern that TARA currently mediates. Instead of merely returning identity attributes after authentication, relying parties may request wallet-presented PID or attestations and may need to perform validation, status checking and relying-party authentication under the EUDI framework.

2.5.EESTI.EE-APPLICATION

Developed by the Estonian Information System Authority (RIA), the Eesti.ee mobile application was launched in December 2024 as a mobile interface to the state portal and common services. Data exchange between underlying government systems is carried out through X-Road. Although it is not an electronic identification means, since July 2025 the app has also allowed users to display selected data from previously issued identity documents, including the ID-card and passport, for proof of identity where both the user and the service provider accept that presentation.¹⁸ Authentication to the application relies on recognised e-identification methods. By early 2026 the app had exceeded 200,000 downloads, indicating that Estonia's future EUDI Wallet will develop alongside an already established national mobile channel. The application is therefore relevant as a comparator and possible adoption channel, but it should not be conflated with the EUDI Wallet. The former is a national service-access interface, whereas the latter is an EU-regulated electronic-identification means and credential-presentation ecosystem.

¹⁷ Riigi Infosüsteemi Amet. (n.d.) Central Authentication Services. [online] Tallinn: RIA. Available from: <https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/central-authentication-services> [Accessed 3 June 2026]

¹⁸ Riigi Infosüsteemi Amet. (n.d.) Eesti App. [online] Tallinn: RIA. Available from: <https://www.ria.ee/en/state-information-system/personal-services/eesti-app> [Accessed 3 June 2026]

3. EIDAS 2.0 AND EUROPEAN DIGITAL IDENTITY WALLET (EUDI WALLET)

3.1.EIDAS 2.0

The eIDAS Regulation (Regulation (EU) No 910/2014)¹⁹ established the legal framework for electronic identification and trust services across the European Union. 10 years later, in 2024, the EU adopted an updated framework, often referred to (and here further) as eIDAS 2.0 (Regulation (EU) 2024/1183)²⁰, which developed and expanded the original eIDAS framework by moving from cross-border recognition of national eIDs toward a common European digital identity ecosystem.

3.2.EUDI WALLET

A central element of eIDAS 2.0 is the requirement that each Member State provide at least one European Digital Identity Wallet. The EUDI Wallet should be described as a certified wallet solution or wallet instance rather than merely as a mobile application. In practice, many early implementations will be mobile-first, but the Regulation does not reduce the Wallet to a phone app as it provides a legal and technical framework for electronic identification, authentication, storage and presentation of PID and electronic attestations of attributes, interaction with relying parties, and the creation of qualified electronic signatures, which Article 5a(5)(g) of Regulation 2024/1183 requires Member States to make available to natural persons free of charge for non-professional purposes.²¹ Credentials and attestations may be issued by public bodies, qualified trust service providers, or other actors within the applicable trust framework.

Another key feature of eIDAS 2.0 is the expansion of trust services. The regulation introduces new categories such as electronic ledgers and electronic attestations of attributes, including qualified electronic attestations of attributes. These services enable verifiable claims to be requested, issued, stored, presented and validated in a way that may differ from full electronic identification. This distinction is central for Estonia because many current public-service interactions identify the user first and then query authoritative

¹⁹ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. Official Journal of the European Union L 257, 28 August 2014, pp. 73-114. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910> [Accessed 3 June 2026]

²⁰ Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework. Official Journal of the European Union L 2024/1183, 30 April 2024. Available from: <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng> [Accessed 3 June 2026]

²¹ Regulation (EU) 2024/1183, Art. 5a(5)(g).

registers, whereas wallet-based flows may allow a user to present a specific attribute or proof without disclosing a full identity profile where the relying party does not need it.

Person identification data (PID) are the core identity data associated with the Wallet and used to identify the wallet holder in interactions that require identification. Electronic attestations of attributes are different: they are verifiable claims about a person or legal entity, such as age, qualification, entitlement or professional status. PID-based identification is therefore not the same legal or technical operation as selective disclosure of attributes.

3.3. ESTONIA'S EUDI WALLET MVP AND EARLY IMPLEMENTATION CHOICES

In 2024, Estonia received an EUDI Wallet minimum viable product (MVP) and began exploring how wallet issuance, verification and governance can be integrated with this established landscape.²² The MVP, delivered by Cybernetica, is positioned as an early implementation aligned with the ARF and designed to support digital credential issuance.²³ It introduces attribute-focused credential presentation and selective disclosure mechanisms, reflecting the wallet's privacy-preserving design goals.

The MVP is used here as evidence of Estonia's implementation direction and design assumptions, not as evidence that the final Estonian Wallet will necessarily adopt all MVP design choices.

Embedding the wallet into Estonia's mature ecosystem raises transition questions that extend beyond software development. Key issues include how to anchor wallet-issued person identification data in existing population registers, how to integrate wallet-based flows with the established TARA login pattern, and how Mobile-ID and Smart-ID should be positioned in a future wallet-centric regime. Equally important are governance choices: who provides the wallet, how certification and supervision are organised, and how liability is allocated when cross-border verification fails or when users require recovery support.

²² Riigi Infosüsteemi Amet. (2023) RIA ja Cybernetica Alustavad Eesti Digiidentiteedi Kukru Väljatootamist. [online] 14 November. Tallinn: RIA. Available from: <https://www.ria.ee/uudised/ria-ja-cybernetica-alustavad-eesti-digiidentiteedi-kukru-valjatootamist> [Accessed 3 June 2026]

²³ Riigi Infosüsteemi Amet and Cybernetica. (2023) Digikukru I Etapi Analüüs. Version 1.0.1, 21 December. [online] Tallinn: RIA. Available from: <https://www.ria.ee/sites/default/files/documents/2024-01/Digikukru-I-etapi-analuus.pdf> [Accessed 3 June 2026]

4. THEORETICAL FRAMEWORK

4.1.IDM TAXONOMY

Hölzmer et al.²⁴ proposed a multi-layer taxonomy developed through repeated iterations that combined structured literature reviews with hands-on evaluation of implemented solutions, with the aim of producing a robust classification scheme. The taxonomy consists of six layers and 22 dimensions, grouped into two broad domains: “theory” and “practice.” On the theory side, it focuses on outcomes for individuals and organisations that use identity systems, namely user wholeness, data autonomy, and application usability. On the practice side, it captures the technology stack, architecture sharing, and system trust.

We chose this taxonomy as the original paper already demonstrated its usefulness for analysing wallet-based identity solutions. In that study, however, the wallet served mainly as an illustrative example. In our study, we treat the wallet as the primary object of analysis, which allows us to examine the Estonian implementation in greater depth and to position it more clearly against Estonia’s existing eID landscape. Although the original work does point toward comparison, it does so only to show that the taxonomy can be applied across different eID solutions, rather than making comparison a central analytical goal.

4.2.INSTITUTIONAL THEORY

Institutional theory has been applied to e-government through diverse concepts including institutional pressures (coercive, mimetic, normative) and institutional arrangements such as legitimacy, regulation, and standards. Studies identified critical mechanisms that shape e-government outcomes: path dependence constrains development through positive feedback loops from past decisions, institutional entrepreneurs enable change by mobilizing resources and changing institutional logics, and regulatory/coercive dimensions prove most effective in certain implementation contexts.

²⁴ Hölzmer, P., Schönrich-Sedlmeir, J. and Imeri, A. (2025) A Taxonomy of Modern User-Centric Identity Management: From Theory to Practice. In: European Conference on Information Systems (ECIS 2025), Amman, Jordan, 11-13 June. [online] AIS Electronic Library. Available from: <https://aisel.aisnet.org/ecis2025/datamgmt/datamgmt/8/> [Accessed 3 June 2026]

5. METHODOLOGY

This study uses a structured legal-technical case-study methodology to compare Estonia's current identity ecosystem with the EUDI Wallet model and its associated legal, technical and governance requirements. The method is qualitative. The comparison is organised around predefined dimensions derived from the IdM taxonomy and then interpreted through institutional theory.

Sources and scope. The primary sources are EU legislation, Estonian legal and policy materials, RIA and Cybernetica implementation documents, official technical and governance materials concerning the EUDI Wallet and ARF, and academic literature on user-centric identity management, e-government institutionalisation and privacy-preserving wallet design. The study does not make claims about final production-level wallet performance or mass user adoption, because Estonia's EUDI wallet remains in an early implementation phase. Practitioner review by an Estonian eID specialist was used for triangulation of the Estonian institutional and technical context.

Analytical procedure. The analysis proceeded in four steps. First, the article identified the relevant wallet requirements and functions, including PID issuance, attestations of attributes, relying-party verification, selective disclosure, assurance, certification, recovery and cross-border interoperability. Second, it mapped these functions against Estonia's ID-card, Mobile-ID, Smart-ID, TARA, X-Road and Eesti.ee service environment. Third, each dimension was assessed for alignment and divergence. Fourth, the resulting pattern of scores was interpreted through institutional theory to explain why specific frictions arise in a mature and path-dependent e-state.

Use of frameworks. The IdM taxonomy is applied as the comparative instrument because it allows the analysis to distinguish user control, data autonomy, application usability, technology stack, architecture sharing and system trust. Institutional theory is then used to explain the frictions revealed by the taxonomy: path dependence, regulatory pressure, legitimacy expectations, public-private role allocation and established service routines shape how Estonia can absorb a wallet-mediated EU identity model.

Scoring logic for Table 1. The values High (H), Medium (M) and Low (L) are qualitative ordinal assessments, not quantitative measurements. For alignment, H means that existing Estonian arrangements already substantially satisfy. M means partial fit requiring adaptation. L means weak fit or the absence of a comparable function. For divergence, H means a material difference. M means a difference that can potentially be managed. L means a minor difference. Borderline cases are marked as ranges, such as L-M or M-H.

6. RESULTS

This section synthesises the comparative mapping of Estonia's existing eID ecosystem and the EUDI Wallet model. Rather than restating the full set of dimensions individually, it reports the principal discontinuities that are legally and institutionally salient for implementation in Estonia.

Table 1 summarises alignment, divergence, and the expected transition frictions across the ecosystem:

Dimension	Estonia eID ecosystem (today)	EUDI Wallet model	Align-ment	Diver-gence	Transition friction
Governance	State-led core identity and federated service delivery; strong national coordination	Multi-actor ecosystem: wallet providers, PID providers, RPs, qualified trust service providers (QTSPs), supervisors; EU-driven interoperability	M	H	Reallocation of roles/responsibilities; who controls wallet, PID, attributes, coordination overhead
Identity assurance	Mature, high-assurance identity (ID-card/ Mobile-ID/ Smart-ID); established trust model	Assurance framed via eIDAS 2.0 ecosystem + wallet assurance/security requirements	H	M	Translating Estonia's mature assurance into wallet-centric compliance evidence; audits, conformity, certification pathways
Credential model	Credential/attribute use often service-specific; strong reliance on national identifiers and registries	Credential/attribute portability across borders; wallet stores and presents attributes	M	H	Issuance and lifecycle management of verifiable credentials; revocation/updates; attribute provenance and quality guarantees
User control/ consent	Strong digital identity, but many flows remain service-driven; user control varies by service	Stronger explicit user mediation (presentation, consent, selective disclosure by design)	M	H	UX and legal design: consent fatigue, default settings, meaningful choice; liability when user-mediated disclosure fails
Data minimisation/ selective disclosure	Minimisation exists, but often limited by identifier-centric flows and legacy patterns	Minimisation and (privacy-preserving) selective disclosure are core expectations	M	H	Re-engineering relying party processes; moving from "ID and queries" to "claims/attributes"; legal basis and technical proof alignment

Dimension	Estonia eID ecosystem (today)	EUDI Wallet model	Alignment	Divergence	Transition friction
Interoperability	Extremely strong nationally (X-Road, TARA); cross-border eID via eIDAS 2.0 node but not wallet-native	Cross-border interoperability is a primary objective; common wallet architecture/specs	M	H	Interoperability is also semantic, governance, and liability harmonisation; versioning and compatibility burdens
Reliance/ verification model	Trust anchored in national infrastructure; verification often online against registers/ services	Verification via wallet-presented credentials + trust lists/ attestations; mixed online/offline validation	M	M	Operational redesign for verifiers; evidence standards; handling offline modes and freshness/validity checks
Roles & liability	Roles are comparatively clear in national regime; liability expectations embedded in national practice	More layered responsibility chain across actors; liability depends on role definitions and compliance	L-M	H	Contracting and risk allocation; incident handling; attribution of failures (wallet vs issuer vs verifier vs registry)
Supervision & compliance	Centralised/ known supervisory environment; compliance maturity high	Broader compliance surface: wallets, issuers, verifiers, trust-service and wallet-provider functions, cybersecurity requirements	M	H	Multi-regulator coordination, audits, reporting duties; compliance costs for new actors; supervision overlaps/gray zones
Security & recovery	Strong cryptographic identity; established recovery/ renewal channels; high user adoption	Security requirements are strict; recovery must work across providers and borders	H	M	Recovery flows (lost device, compromise) across wallets/issuers; usability versus security; social engineering risks
Market structure	Established domestic actors; high baseline adoption and public trust	Potentially more competition (wallet providers, credential issuers) and EU-wide market dynamics	M	M-H	Adoption messaging; migration fatigue; ecosystem coordination costs
Strategic “continuity vs change”	Continuity in trust + infrastructure; change mainly incremental	Paradigm shift toward wallet-mediated, attribute-centric, interoperable ecosystem	M	H	Redistributing control and retooling processes while maintaining Estonia’s high-trust baseline

The H/M/L values were assigned by the authors on the basis of the documentary corpus and subsequently validated against the practitioner triangulation referred to above.

6.1.PLACE OF CONTROL AND GOVERNANCE

Governance and Roles & liability both show medium or low alignment and high divergence. Estonia's eID ecosystem is anchored in a strongly coordinated national model: Assurance and authentication are institutionally settled, and service delivery builds on standardised national infrastructure. The EUDI Wallet model shifts mediation towards the wallet and distributes governance across more actors (wallet providers, issuers, relying parties, trust-service roles, supervisors). Transition friction: The core change is thus not "building assurance," but reallocating control and accountability, i.e. the question who issues, who validates, who governs lifecycle rules, and who is held liable when wallet-mediated flows fail.

6.2.DATA MINIMISATION AND SELECTIVE DISCLOSURE

For Data minimisation/selective disclosure and Credential model divergence is assessed as high. Estonia supports minimisation in practice, but many established flows remain identifier-centric and rely on subsequent online verification against registries. The EUDI Wallet model is designed for attribute-centric presentation and, increasingly, privacy-preserving/selective disclosure as a default interaction pattern. Transition friction: In Estonia, relying party processes and legal/organisational expectations must move from "identify-then-query" to "present-only-what-is-needed," including validity, provenance, and revocation handling.²⁵

6.3.INTEROPERABILITY AND CROSS-BORDER USABILITY

Estonia's interoperability is exceptionally strong domestically, supported by unified governance and shared semantics. The EUDI Wallet targets cross-border interoperability, which requires not only technical compatibility but also semantic alignment, predictable verification practices, and shared trust and assurance expectations across Member States. Transition friction: Estonia's national success does not directly translate into wallet-native cross-border usability; harmonisation burdens expand from APIs to governance, semantics, and liability.

²⁵ Álvarez, I. A., Hölzmer, P. and Sedlmeir, J. (2025) Privacy Evaluation of the European Digital Identity Wallet's Architecture and Reference Framework. *Computers & Security*, 160, 104707. Available from: <https://doi.org/10.1016/j.cose.2025.104707> [Accessed 3 June 2026]

6.4.TRANSPARENCY, EXPLAINABILITY, AND USER TRUST

Estonia benefits from high baseline trust and familiar e-service routines, which often substitute for transaction-level transparency. Wallet-mediated identity use makes disclosure choices more explicit (what is requested, what is shared, and why), but visibility alone can increase user burden. Transition friction: The system should deliver meaningful, usable transparency at scale. Otherwise consent fatigue and routinized acceptance can undermine the legitimacy of user-mediated disclosure and increase risk for disputes.

6.5.SECURITY AND RECOVERY

For Security & recovery Estonia has high alignment but continuing medium friction because recovery must operate across wallet providers, issuers and credential lifecycles. Estonia's eID solutions combine strong cryptography with mature operational practices, including renewal and recovery pathways that users and institutions understand. The EUDI Wallet concentrates identity utility in a device-centric wallet and introduces multi-provider recovery complexity (wallet provider, issuer, credential lifecycle). Transition friction: Estonia faces the challenge of restoring access securely without enabling takeover, while keeping recovery practical enough to support adoption.

6.6.ROLES, RESPONSIBILITY, AND LIABILITY ALLOCATION

In Estonia's national model, roles and responsibility are comparatively legible within a coherent institutional landscape. The EUDI Wallet ecosystem expands the role set and fragments responsibility across issuance, storage, presentation, verification, trust lists, and supervision. Transition friction: Liability attribution becomes harder in incidents (wrong issuance, weak verification, UI-induced disclosure errors, revocation failures), so legal and contractual arrangements must make responsibility operationally clear to preserve trust in a more distributed ecosystem.

7. DISCUSSION

7.1.LEGAL RISK IF ESTONIA PORTS ITS REGIME UNCHANGED

If Estonia attempts to transpose its nationally mature eID regime into the EUDI Wallet ecosystem without redesigning governance and accountability, the primary legal risk is a mismatch between responsibility and technical reality, which literature partially even considers a human rights issue.²⁶ Estonia's existing model is supported by stable institutional roles and a coherent trust anchor. In a wallet-centric ecosystem, the transaction chain is distributed across multiple actors and layers, and cross-border reliance places greater weight on shared verification practices and interoperable compliance expectations.

This legal risk follows directly from the comparative table. The strongest national continuity lies in security and assurance, while the highest divergence lies in governance, liability, attribute lifecycle management and cross-border reliance. A purely technical port would therefore address the areas where Estonia is already strong and leave unresolved the areas where the EUDI Wallet produces the most institutional change.

Porting the regime unchanged risks: (i) uncertain attribution of fault in incidents, (ii) fragmented compliance duties across actors, and (iii) reduced legal defensibility of identity transactions when contested cross-border (e.g., disputes over validity, provenance, revocation status, and the operational meaning of "assurance"). In a high-trust setting, such legal-institutional gaps can undermine trust even where core cryptographic security remains strong.

7.2.LIABILITY ARCHITECTURE UNDER EIDAS 2.0

The eIDAS framework allocates civil liability through Article 13 of Regulation 910/2014, which imposes liability on trust service providers for damage caused intentionally or negligently to any natural or legal person, with a partial reversal of the burden of proof for qualified trust service providers.²⁷ Regulation 2024/1183 extends this architecture to the new wallet-mediated transaction chain, in particular by imposing distinct obligations on wallet providers in addition to those of qualified trust service providers issuing electronic attestations of attributes.²⁸ For Estonia, the practical question is how these layered duties translate into a domestic role model: which

²⁶ Kaplane, A. (2025) *The European Digital Identity Wallet: A New Human Right Unlocked?* *Nordic Journal of Human Rights*, 43 (3), pp. 304-316. Available from: <https://doi.org/10.1080/18918131.2025.2551458> [Accessed 3 June 2026]

²⁷ Regulation (EU) No 910/2014, Art. 13. See further Dumortier, J. (2016) *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)*.

²⁸ Regulation (EU) 2024/1183, recitals (38)-(40) and the corresponding articles on wallet-provider obligations and liability.

actor bears primary liability for an erroneous PID issuance, for a failure of revocation propagation, or for a wallet-side disclosure error caused by interface design. Where multiple actors contribute to a single failure (e.g. wallet provider, PID issuer, relying party, QTSP), the prospect of joint liability under general private-law principles, mediated by the Estonian Law of Obligations Act (*Võlaõigusseadus*, VÕS),²⁹ becomes relevant. A nationally articulated role model should therefore not merely allocate functions but also predefine the regress and apportionment mechanics among co-liable actors, in line with the contributory-fault and joint-debtor provisions of the VÕS.

7.3.WHERE EIDAS 2.0 CREATES AMBIGUITY

eIDAS 2.0 creates ambiguity at the interfaces between actors and functions.³⁰

- **Role boundaries:** Functions that may be nationally integrated (proofing, issuance, presentation, verification, revocation) become separable and potentially provided by different actors. Obligations can exist without a single actor being operationally positioned to fulfil them end-to-end;
- **Supervision perimeter:** The compliance surface expands and may implicate multiple supervisory logics. Ambiguity arises where supervisory competences overlap, or where enforcement depends on cross-border coordination;
- **Liability attribution:** Wallet-mediated identity transactions introduce additional points of failure. Absent clear allocation of duties and evidentiary expectations (including “reasonable verification” and revocation/freshness checks), responsibility can become contested and remediation delayed.
- **Assurance equivalence in practice:** Formal assurance categories require operational grounding. Disputes may arise where assurance depends on implementation details (offline/online validation, credential freshness, revocation status) that differ across ecosystems.

²⁹ *Võlaõigusseadus* [Law of Obligations Act]. Republic of Estonia. Tallinn: Riigi Teataja. In Estonian/English. Available from: <https://www.riigiteataja.ee/en/eli/ee/506112024004/consolide/current> [Accessed 3 June 2026]

³⁰ See also Wong-Toropainen, S. (2024) Problematising User Control in the Context of Digital Identity Wallets and European Digital Identity Framework. In: Prifti, K. et al. (eds.) *Digital Governance. Information Technology and Law Series*, vol. 39. The Hague: T.M.C. Asser Press, pp. 115-136. Available from: https://doi.org/10.1007/978-94-6265-639-0_6 [Accessed 3 June 2026]

7.4.INTERACTION WITH ADJACENT EU INSTRUMENTS

Wallet-mediated transactions do not operate within eIDAS 2.0 alone. The selective disclosure of attributes engages the GDPR, in particular the lawful-basis requirements of Article 6 and the data-protection-by-design obligation of Article 25.³¹ Where relying parties are online platforms within the meaning of the Digital Services Act, the wallet-based identification of users intersects with DSA obligations on traceability of traders (Article 30) and on protection of minors.³² Where wallet-presented attributes feed automated decision-making, the AI Act may apply, particularly where the relying party operates a high-risk system relying on biometric or identity-related input.³³ A complete legal mapping of the Estonian implementation must therefore treat the EUDI Wallet not as an isolated trust-service instrument, but as a node within a multi-instrument private-law and regulatory environment.

7.5.THE WALLET RELATIONSHIP AS A CONTRACTUAL STRUCTURE

Beyond regulatory compliance, wallet-mediated identity is sustained by a network of private-law relationships: between the wallet provider and the holder (typically a consumer); between the wallet provider and relying parties; and between the relying party and the holder in the underlying transaction. Where the holder is a natural person, the wallet-holder relationship is, in Estonian law, subject to the consumer-protection regime of the Law of Obligations Act, in particular the standard-terms control under §§ 35-45 VÕS, which transposes the Unfair Contract Terms Directive 93/13/EEC.³⁴ This implies, *inter alia*, that broad limitations of wallet-provider liability, unilateral modification rights, and consent-by-use clauses are exposed to substantive review. A complete national role model

³¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union L 119, 4 May 2016, pp. 1-88. Available from: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 3 June 2026]

³² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). Official Journal of the European Union L 277, 27 October 2022, pp. 1-102. Available from: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> [Accessed 3 June 2026]

³³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union L 2024/1689, 12 July 2024. Available from: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> [Accessed 3 June 2026].

³⁴ Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts. Official Journal of the European Communities L 95, 21 April 1993, pp. 29-34. Available from: <https://eur-lex.europa.eu/eli/dir/1993/13/oj> [Accessed 3 June 2026]. For the Estonian transposition see *Võlaõiguseadus* [Law of Obligations Act], §§ 35-45.

should therefore pre-empt foreseeable standard-terms disputes by specifying minimum content for wallet terms of service and minimum disclosure duties at the point of credential presentation.

7.6. IMPLICATIONS FOR ESTONIA'S IMPLEMENTATION STRATEGY

The results indicate that Estonia's advantage lies in an already mature trust baseline; the central question is how to preserve that baseline under a distributed, wallet-mediated model. The transition therefore requires governance and legal design that follow the transaction chain: clearly defined roles, enforceable verification expectations, coherent supervision, and recovery procedures that are both secure and workable. Without this, Estonia risks importing cross-border interoperability obligations while exporting domestic role clarity.

8. RECOMMENDATIONS

Recommendation for Implementation strategy and continuity: Estonia should treat the EUDI Wallet as an ecosystem extension during the transition rather than as an immediate one-to-one replacement of existing identity means. A coexistence approach should keep ID-card, Mobile-ID, Smart-ID, TARA and relevant Eesti.ee functions available for a defined transition period, while specifying which use cases move to wallet-mediated PID or attribute presentation. This recommendation follows from Table 1: Estonia has high continuity in assurance and security, but high divergence in control, data minimisation, credential portability and presentation. Managed coexistence preserves the strengths of the existing regime while allowing wallet-specific added value to be demonstrated in bounded contexts.

Recommendation for Governance: Estonia should settle legal status, governance and role allocation early and explicitly. A national role model should identify who provides the wallet, who provides PID, who issues public-sector and private-sector attestations, which actors qualify as trust service providers, how relying parties are registered and supervised, and which authority coordinates incident handling. The framework should allocate responsibility for issuance, presentation, verification, status management, revocation, validity checks and recovery support, and it should clarify how liability attaches across those functions in incident and dispute scenarios. In parallel, Estonia should publish a legal mapping of how population-register data, existing national credentials, electronic signatures and electronic attestations of attributes interact within wallet-mediated transactions.

Recommendation for Technical interoperability and national assets: Estonia should build the technical transition on existing national

infrastructure assets rather than bypassing them. Where consistent with EU specifications, TARA, GovSSO, X-Road, certificate validation services and registry interfaces should be used as bridging assets for wallet issuance, verification and cross-border reliance. Implementation should be accompanied by conformance testing and documented integration profiles for issuers and relying parties, including verification practice, relying-party authentication, attribute semantics, revocation and freshness checks. This approach aligns with the paper's central finding that the key challenge concerns harmonisation of layers and roles, not replacement of deficient infrastructure.

Recommendation for Phased deployment and use-case governance:

Estonia should phase implementation around a limited number of high-value use cases rather than broad deployment from the outset. Priority should be given to use cases in which wallet-specific capabilities - especially selective disclosure, portable attestations, cross-border verification and default wallet-based qualified electronic signatures for natural persons - produce demonstrable legal or practical benefits beyond simple login. A narrower, use-case governed rollout reduces systemic risk, enables iterative refinement of verifier onboarding, support and recovery processes, and allows supervision to stabilise before the Wallet becomes a general-purpose channel.

Recommendation for User adoption, transparency, and recovery:

Estonia should treat adoption as a legal-design and communication obligation, not merely as a consequence of mandate. User-facing materials should distinguish existing credentials, the Eesti.ee application and the EUDI Wallet in functional terms: authentication, signing, service access, PID presentation and attribute presentation. Selective disclosure should be explained through standardised notices and interaction patterns that support meaningful comprehension rather than routinised consent. Estonia should maintain familiar fallback mechanisms during the transition and should treat recovery as a core trust-and-usability feature, specifying minimum recovery guarantees and user remediation pathways.

9. CONCLUSION

In this work, we argued that embedding the EUDI Wallet into Estonia is not primarily a problem of creating trusted digital identity, but of fitting a harmonised wallet-centred EU model into a mature, path-dependent, and already trusted national ecosystem. Our major findings were, in order of importance, that the main discontinuity lies in the redistribution of control, access, and presentation; that the most consequential frictions concentrate in legal-governance alignment (including role and liability allocation) and cross-border interoperability rather than in basic assurance, authenticity, or security; and that user burden may increase during channel coexistence even where user autonomy improves. Accordingly, the principal implication of this work is to guide a phased implementation strategy in which Estonia treats the wallet as an ecosystem extension, settles legal and governance roles early, and uses TARA and X-Road as bridging assets for selected high-value use cases before broad rollout.

Similarly to Hölzmer et al., the analysis confirms that identity systems must be understood across multiple, interlocking layers rather than reduced to a single technical component. Unlike much of the existing work, however, this article applies a layered lens to a *mature* e-state and shows that the principal discontinuity introduced by the EUDI Wallet is not the absence of trust or security, but the transition challenge of reallocating control, responsibilities, and interoperability expectations in a wallet-mediated, cross-border ecosystem.

These findings are significant because they show that the eventual impact of the EUDI Wallet in digitally advanced member states will depend less on building trust from scratch than on redistributing control, interoperability, and accountability without eroding the assurance, usability, and institutional clarity that already sustain successful national systems.

The analysis assumes that the EUDI Wallet can be treated as a reference architecture and governance model on the basis of official legal and technical documentation, and that Estonia's distributed ID-card, Mobile-ID, Smart-ID, TARA, and X-Road ecosystem can be validly compared with that target state at ecosystem level despite the asymmetry of components. The study is limited to desk research with practitioner triangulation and to an early implementation phase, so it cannot yet observe realised user adoption, final governance settlements, production-level recovery performance, or fully operational cross-border verification in practice.

Future work should revisit the Estonian case after broader deployment with empirical evidence from users, issuers, verifiers, and cross-border

transactions, so that the early friction patterns identified here can be tested against realised institutional outcomes over time.

LIST OF REFERENCES

- [1] Aavik, G. and Krimmer, R. (2016) Integrating Digital Migrants: Solutions for Cross-Border Identification from E-Residency to eIDAS. A Case Study from Estonia. In: Scholl, H. J. et al. (eds.) *Electronic Government (EGOV 2016)*. Lecture Notes in Computer Science, vol. 9820. Cham: Springer, pp. 151-163. Available from: https://doi.org/10.1007/978-3-319-44421-5_12 [Accessed 3 June 2026].
- [2] Álvarez, I. A., Hölzmer, P. and Sedlmeir, J. (2025) Privacy Evaluation of the European Digital Identity Wallet's Architecture and Reference Framework. *Computers & Security*, 160, 104707. Available from: <https://doi.org/10.1016/j.cose.2025.104707> [Accessed 3 June 2026].
- [3] Babel, M. et al. (2025) Self-Sovereign Identity and Digital Wallets. *Electronic Markets*, 35, art. 28. Available from: <https://doi.org/10.1007/s12525-025-00772-0> [Accessed 3 June 2026].
- [4] Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts. Official Journal of the European Communities L 95, 21 April 1993, pp. 29-34. Available from: <https://eur-lex.europa.eu/eli/dir/1993/13/oj> [Accessed 3 June 2026].
- [5] Degen, K. and Teubner, T. (2024) Wallet Wars or Digital Public Infrastructure? Orchestrating a Digital Identity Data Ecosystem from a Government Perspective. *Electronic Markets*, 34, art. 50. Available from: <https://doi.org/10.1007/s12525-024-00731-1> [Accessed 3 June 2026].
- [6] Dumortier, J. (2016) *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)*. [online] Available from: <https://ssrn.com/abstract=2855484> [Accessed 3 June 2026].
- [7] European Commission. (n.d.) *Estonia*. [online] eIDAS Community. Available from: <https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/62885749/Estonia> [Accessed 3 June 2026].
- [8] Gakh, V. et al. (2024) Enhancing Privacy Risk Modeling in Practice: A Case Study of an E-Justice System. *IEEE Access*, 12, pp. 183851-183874. Available from: <https://doi.org/10.1109/ACCESS.2024.3509332> [Accessed 3 June 2026].
- [9] Hölzmer, P., Schönrich-Sedlmeir, J. and Imeri, A. (2025) A Taxonomy of Modern User-Centric Identity Management: From Theory to Practice. In: *European*

- Conference on Information Systems (ECIS 2025), Amman, Jordan, 11-13 June. [online] AIS Electronic Library. Available from: <https://aisel.aisnet.org/ecis2025/datamgmt/datamgmt/8/> [Accessed 3 June 2026].
- [10] id.ee. (2024) *Trust Services: Authentication Services*. [online] Tallinn: id.ee. Available from: <https://www.id.ee/en/article/trust-services-authentication-services/> [Accessed 3 June 2026].
- [11] *Isikut Tõendavate Dokumentide Seadus [Identity Documents Act]*. Republic of Estonia. Tallinn: Riigi Teataja. In Estonian. Available from: <https://www.riigiteataja.ee/akt/102072013047?leiaKehtiv=> [Accessed 3 June 2026].
- [12] Kaplane, A. (2025) The European Digital Identity Wallet: A New Human Right Unlocked? *Nordic Journal of Human Rights*, 43 (3), pp. 304-316. Available from: <https://doi.org/10.1080/18918131.2025.2551458> [Accessed 3 June 2026].
- [13] Kattel, R. and Mergel, I. (2019) Estonia's Digital Transformation: Mission Mystique and the Hiding Hand. In: Compton, M. E. and 't Hart, P. (eds.) *Great Policy Successes*. Oxford: Oxford University Press, pp. 143-160. Available from: <https://doi.org/10.1093/oso/9780198843719.003.0008> [Accessed 3 June 2026].
- [14] Laud, P. and Roos, M. (2009) Formal Analysis of the Estonian Mobile-ID Protocol. In: Jøsang, A., Maseng, T. and Knapskog, S. J. (eds.) *Identity and Privacy in the Internet Age (NordSec 2009)*. Lecture Notes in Computer Science, vol. 5838. Berlin, Heidelberg: Springer, pp. 271-286. Available from: https://doi.org/10.1007/978-3-642-04766-4_19 [Accessed 3 June 2026].
- [15] Lips, S., Bharosa, N. and Draheim, D. (2020) eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. In: Chugunov, A. et al. (eds.) *Electronic Governance and Open Society: Challenges in Eurasia (EGOSE 2020)*. Communications in Computer and Information Science, vol. 1349. Cham: Springer, pp. 75-89. Available from: https://doi.org/10.1007/978-3-030-67238-6_6 [Accessed 3 June 2026].
- [16] Lips, S. et al. (2023) Management of National eID Infrastructure as a State-Critical Asset and Public-Private Partnership: Learning from the Case of Estonia. *Information Systems Frontiers*, 25, pp. 2439-2456. Available from: <https://doi.org/10.1007/s10796-022-10363-5> [Accessed 3 June 2026].
- [17] *Rahvastikuregistri Seadus [Population Register Act]*. Republic of Estonia. Tallinn: Riigi Teataja. In Estonian/English. Available from: <https://www.riigitea>

- taja.ee/en/eli/ee/511012023005/consolide/current [Accessed 3 June 2026].
- [18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union L 119, 4 May 2016, pp. 1-88. Available from: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 3 June 2026].
- [19] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). Official Journal of the European Union L 277, 27 October 2022, pp. 1-102. Available from: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> [Accessed 3 June 2026].
- [20] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework. Official Journal of the European Union L 2024/1183, 30 April 2024. Available from: <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng> [Accessed 3 June 2026].
- [21] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union L 2024/1689, 12 July 2024. Available from: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> [Accessed 3 June 2026].
- [22] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. Official Journal of the European Union L 257, 28 August 2014, pp. 73-114. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910> [Accessed 3 June 2026].
- [23] Riigi Infosüsteemi Amet. (2023) *RIA ja Cybernetica Alustavad Eesti Digiidentiteedi Kukru Väljatöötamist*. [online] 14 November. Tallinn: RIA. Available from: <https://www.ria.ee/uudised/ria-ja-cybernetica-alustavad-eesti-digiidentiteedi-kukru-valjatootamist> [Accessed 3 June 2026].
- [24] Riigi Infosüsteemi Amet. (n.d.) *Central Authentication Services*. [online] Tallinn: RIA. Available from: <https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/central-authentication-services> [Accessed 3 June 2026].

- [25] Riigi Infosüsteemi Amet. (n.d.) *Data Exchange Layer X-tee*. [online] Tallinn: RIA. Available from: <https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee> [Accessed 3 June 2026].
- [26] Riigi Infosüsteemi Amet. (n.d.) *Eesti App*. [online] Tallinn: RIA. Available from: <https://www.ria.ee/en/state-information-system/personal-services/eesti-app> [Accessed 3 June 2026].
- [27] Riigi Infosüsteemi Amet and Cybernetica. (2023) *Digikukru I Etapi Analüüs*. Version 1.0.1, 21 December. [online] Tallinn: RIA. Available from: <https://www.ria.ee/sites/default/files/documents/2024-01/Digikukru-I-etapi-analuus.pdf> [Accessed 3 June 2026].
- [28] Tsap, V., Lips, S. and Draheim, D. (2020) Analysing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. In: Kõ, A. et al. (eds.) *Electronic Government and the Information Systems Perspective (EGOVIS 2020)*. Lecture Notes in Computer Science, vol. 12394. Cham: Springer, pp. 159-173. Available from: https://doi.org/10.1007/978-3-030-58957-8_12 [Accessed 3 June 2026].
- [29] *Võlaõigusseadus [Law of Obligations Act]*. Republic of Estonia. Tallinn: Riigi Teataja. In Estonian/English. Available from: <https://www.riigiteataja.ee/en/eli/ee/506112024004/consolide/current> [Accessed 3 June 2026].
- [30] Wong-Toropainen, S. (2024) Problematising User Control in the Context of Digital Identity Wallets and European Digital Identity Framework. In: Prifti, K. et al. (eds.) *Digital Governance*. Information Technology and Law Series, vol. 39. The Hague: T.M.C. Asser Press, pp. 115-136. Available from: https://doi.org/10.1007/978-94-6265-639-0_6 [Accessed 3 June 2026].

<<< ARTICLES

BOOK REVIEWS >>>

DOI 10.5817/MUJLT2026-44540

OVERCOMING TECHNOLOGY'S MYTHS – A REVIEW OF LAW AND TECHNOLOGY: A METHODOICAL APPROACH

by

KATARZYNA KATANA *

Calo R. (2025) Law and Technology: A Methodical Approach. Oxford University Press, 160 p.

1. INTRODUCTION

Legal scholarship—especially within modern, results-oriented academia¹—is currently facing accusations of hovering between moral philosophy and actual science.² Legal scholars routinely operate on moral presumptions invoked in the letter of the law, drawing from them conclusions applicable to actual reality. The traditional aim of legal scholarship is to derive norms from the law on paper, interpret them, systematise them, and assess their functionality in light of the current state of affairs. In doing so, legal scholars usually merely touch upon the issue of methodology, or do not invoke it at all.³

The situation has slightly changed for legal scholars examining the relationship between law and technology. This branch of legal scholarship is still considered novel and still organising itself⁴(also in the scope of methodology) and at the same time as such open to approaches outside traditional doctrinal research.

* Katarzyna Katana; Masaryk University in Brno, Faculty of Law, Institute of Law and Technology; Ph.D. candidate; Practising attorney in Poland; E-mail: 584138@mail.muni.cz

¹ Duncan, N. J. and Hutchinson, T. (2012). *Defining And Describing What We Do: Doctrinal Legal Research*. Deakin Law Review, 17(1), pp. 86, 90-91.

² Calo R. (2025) *Law and Technology: A Methodical Approach*. Oxford University Press, p. 8.

³ Calo R. (2025) *op. cit.* p. 9.

⁴ Calo R. (2025) *op. cit.* p. 4.

However, the novelty of this branch may be debatable, given that technology has been a societal phenomenon for over a century or even more⁵, and the field of law and technology is already more than two decades old. This issue and many more are discussed by Ryan Calo, a professor of law at the University of Washington and author of the 2025 book “Law and Technology: A Methodical Approach” by Oxford University Press, which is being reviewed in this paper.

2. STRUCTURE AND KEY AREAS

In the introduction, Calo discusses⁶ different approaches present in the literature—starting with the disruption approach, which sees law as aiming to restore ex-ante the status quo (including damaged societal values). He also mentions⁷ minority approach which aims to assess technology through previous stages of development to predict future impact.

Then, in the first, longest chapter, entitled “Technology as a social fact”, the author presents⁸ several myths around technology, including characteristics of technology as being inevitable, and difficult or undesirable to regulate, as it would kill progress. Then Calo aims to define what technology actually is.⁹ In addition the author recalls¹⁰ a tendency of legal scholars to fixate on the particular instance of given technology, not on a bundle of technological affordances¹¹ that constitute the system. Scholars would rather analyse drones instead of the development of digital and kinetic technologies and their legal dimensions. As Calo points out¹² existing legislation aims at specific technology, not a broader context or underlying layers of concern posed by the type of given innovation (for example, laws focus on delivery robots or drones, not on the issues related to presence of unmanned vehicles conducting constant surveillance of the surroundings, including private spaces due to its core need of knowledge of the environment in the process of movement).

Another mistake made by scholars is to assume that technology will shape behaviours and society in a single, inevitable way. The author additionally

⁵ Calo R. (2025) *op. cit.* pp. 52-53.

⁶ Calo R. (2025) *op. cit.* p. 19.

⁷ Calo R. (2025) *op. cit.* p. 12.

⁸ Calo R. (2025) *op. cit.* p. 21.

⁹ Calo R. (2025) *op. cit.* p. 24.

¹⁰ Calo R. (2025) *op. cit.* p. 27.

¹¹ To better illustrate this term, it is helpful to consider the examples provided by the author. For instance, Calo describes the ability to act at a distance or speak with anonymity as affordances of technology. See Calo R. (2025) *op. cit.* p. 31.

¹² Calo R. (2025) *op. cit.* p. 26.

highlights¹³ that an important factor is being overlooked, namely the hidden intentions or interests of the creators of a given technology in relation to their responsibility for the technology's emerging behaviours.

The presumption of perceived ungovernability comes up several times, "fetishism" of constant innovation and positioning technology as the sole force bettering or securing several social values, from health to security. Calo furthermore points out¹⁴ so-called technological exceptionalism, as a perceived difference of technology from other social phenomena.

In the second chapter, the author outlines¹⁵ the differences between STS and legal scholarship. STS, which goes by several names, such as "science and technology studies" or "science, technology and society studies" is a science focused on how science and technology are developed, by whom and to what effect on society. It perceives technology as a social fact.

The law instead is focused around normativity and pragmatism. The traditional aim of legal scholarship is to identify a problem and provide a solution, thus, as the author notes, many are starting to see law as a social phenomenon (legal realism) and do not hesitate to use methods typical to social sciences, as qualitative or quantitative.

As the author invokes,¹⁶ the STS may give a legal scholarship a broader, more nuanced understanding of the subject matter of the influence of technology on societal experience. As he additionally mentions,¹⁷ the use of STS helped him to develop his understanding of technology as a contingent bundle of affordances, rather than a stable construct.

Chapter 3 presents the proposed, structured (step by step) methodology of analysing relation between law and technology.

The first step is¹⁸ to select and define technology and provide the reader with an explanation of why that specific technology was chosen, far beyond simply invoking the importance of the technology or its novelty.

The author recommends,¹⁹ *inter alia*, justifying whether the technology differs from previous technologies. The next step of the methodology is to analyse the detailed scope of the inquiry,²⁰ whether the inquiry focuses on technology in general or in its specific instances. After that, the prospective scholar should analyse what exactly the given technology

¹³ Calo R. (2025) *op. cit.* p. 21.

¹⁴ Calo R. (2025) *op. cit.* p. 47.

¹⁵ Calo R. (2025) *op. cit.* p. 53.

¹⁶ *Ibid.*

¹⁷ Calo R. (2025) *op. cit.* p. 79.

¹⁸ Calo R. (2025) *op. cit.* p. 90.

¹⁹ Calo R. (2025) *op. cit.* p. 94.

²⁰ Calo R. (2025) *op. cit.* p. 93.

changes in human capabilities, what avenues of behaviour or thought technology opens, changes or forecloses.²¹ Then the analyst should name stakeholders²² and judge the possible influence in their reality, through the lenses of the available method, including, for example, the paradigm of value sensitive design or responsible innovation.

Subsequently, the scholar should point out what exactly innovation changes,²³ including not only visible, but also hidden characteristics (or in other words, intended or unintended), and envision societal change over time. The part of legal analysis shall include²⁴ naming the normative baseline of the assessment, including the criteria of assessment, with emphasis given to the goal aimed by the author in the work.

Analysts should also consider under which area of law the technology will be scrutinised and why this specific area has been chosen, and name the project type as well.²⁵ The selection of types starts with archetypal legal scholarship pathways (like *inter alia* doctrinal recasting, comparative or theoretical, historical, critical, institutional assessment).

As the author argues,²⁶ there are also at least four specific directions of assessment of technology projects through the lenses of law, which include the disruption approach, so measuring change (in a broader meaning) caused by the technology and proposed changes to the law and institutions to address this change. The other ones are Governance or Tech Assessment, in which one assesses costs and benefits of the technology and propose law and adequate policy frameworks to channel technology in the desired direction. There are also the internal and critical projects where scholars reflect on the nature of technology in relation to law or empirical research, in this case scientist studies sociological contexts of technology, by using qualitative, quantitative or mixed research methods.

At the end, the scholar shall propose²⁷ legal intervention to address mapped goals and concerns, and beforehand map the space of relevant solutions.

The fourth chapter demonstrates²⁸ the practical application of the proposed methodology through a series of examples. The author uses three specific examples (case studies), to illustrate his methodology: assessment of

²¹ Calo R. (2025) *op. cit.* p. 95.

²² Calo R. (2025) *op. cit.* p. 96.

²³ Calo R. (2025) *op. cit.* p. 98.

²⁴ Calo R. (2025) *op. cit.* p. 111.

²⁵ Calo R. (2025) *op. cit.* p. 105.

²⁶ Calo R. (2025) *op. cit.* p. 107.

²⁷ Calo R. (2025) *op. cit.* pp. 16, 112.

²⁸ Calo R. (2025) *op. cit.* pp. 122-134.

augmented reality, legal consequences of “hacking” machine learning (with distinction to the intent), cochlear implants and their legal (including human rights) implications.

From the beginning to end of the book, societal assumptions about technology come to light, and the author carefully curates his narrative around them.

As Calo points out,²⁹ the trope of fast-moving technology, too fast for any accurate regulation, is governing how the relationship between law and technology is being viewed by many. The author recalls³⁰ a specific “Catch-22” (known as Collingridge’s dilemma³¹) that policymakers face: they hesitate to intervene too early due to the inability to predict all the social consequences, but this leads to an inability to regulate later on, as the public perception of the technology has already been merged with the technology. However, as the author argues,³² technology is not distinct from any other social fact successfully regulated by law.

Moreover, the book is structured around several key terms. One of them is affordance, understood in the technological contexts as a capacity of technology to reshape human experience or environment by altering affordances.

A recurring theme is the reference to the “Law of the horse”³³, which argues that the scope of any technology is already covered by many existing areas of law and creating a separate technology law is akin to introducing a “law of the horse” - and is similarly unnecessary.

Each chapter concludes with a list of references and a separate section of recommended readings.

²⁹ Calo R. (2025) *op. cit.* pp. 5-6.

³⁰ Ibid.

³¹ Collingridge D.(1980) *The Social Control Of Technology*. Frances Pinter, pp. 13-21.

³² Calo R. (2025) *op. cit.* p. 47.

³³ Easterbrook F. H.(1996) *Cyberspace and the Law of the Horse*. University of Chicago Legal Forum 207.

3. ASSESSMENT OF THE CONTENT

Primarily, it is worth noting that Ryan Calo is an excellent storyteller, and each passage is packed with a high number of real-world examples, and those also of historic nature. The book is very recent, having been published in 2025. The content is – despite its academic nature – easy to read, regardless of the level of previous expertise in the subject. At the same time, the book relies heavily on literature, including the classic one. References to, *inter alia*, Lessig's canonical "Code is law"³⁴ are recurrent. The author's thoughts are not merely a recounting of what has gone before, but lead him to his intended conclusions, namely the formulation of a coherent methodology for the field in question. The author does not claim to have invented the methodology from scratch, as he points out, the 'disruption approach' to technology is the most prevalent among scholars.³⁵ The book's role is primarily to organise and systematise the issues previously addressed in the literature, it does not propose a revolutionary method, nor does it aspire to do so.

Calo consistently argues³⁶ that meaningful research in law and technology requires interdisciplinary collaboration, emphasising that no single discipline can adequately address complex societal questions and legal scholars should in many instances take a lead of such interdisciplinary teams.³⁷

The book has its limitations because, being rooted in a US context, it draws on typically US examples; however, this does not prevent the creation of a universal model which, as the author indicates, is open to modification. Furthermore, the author notes the direction in which European regulation (AI Act³⁸, DSA³⁹)⁴⁰ is moving in terms of regulatory models for technology law, but does not assess or evaluate it. It is worth to notice, Calo's methodology may not be fully applicable to the EU legislation without certain adjustments. A clear example of this split is existence in same areas of law of highly codified, formal principles such as the "safe harbour"⁴¹ rules under the DSA,

³⁴ Lessig L. (1999) *Code And Other Laws Of Cyberspace*. Basic Books.

³⁵ Calo R. (2025) *op. cit.* p. 133.

³⁶ Calo R. (2025) *op. cit.* p. 139.

³⁷ Calo R. (2025) *op. cit.* pp. 110-111.

³⁸ Regulation (EU) 2024/1689 Of The European Parliament And Of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act or AI Act), Official Journal of the European Union 2024/1689 12.7.2024

³⁹ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act or DSA), Official Journal of the European Union, L 277, 27.12.2022,

⁴⁰ Calo R. (2025) *op. cit.* pp. 115, 141.

⁴¹ Article 6 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

which strictly limit the liability of intermediaries for the content transmitted or stored by their means. Such precise statutory limitations can preclude full application of Calo's methodology, as they stop a prospective analyst from fully evaluating a technology's affordances and its varying impacts on stakeholders, as the predetermined formal rule already dictates the legal outcome and limits the scope of inquiry.

4. CONCLUSION

Ryan Calo's book is highly recommended for both students and experienced legal practitioners, including academics, primarily with a view to standardising or refreshing the methodological framework employed in everyday work. The author proposes a clear step-by-step process for assessing technology through a legal lens. It will be useful both to those who need an initial introduction to a standardised approach to constructing legal arguments, and as a reminder to experienced researchers of the need to structure their analysis so that the audience (often without a legal background, e.g. in the case of policymakers) is aware of the basis and sources of the conclusions drawn, as well as their limitations. Perhaps some readers from the legal profession will also respond positively to the author's call to engage more boldly in multidisciplinary projects, drawing on other fields whilst also contributing their own. As the author notes, lawyers are predestined to play a leading role in such teams. By heavily referencing sociological scholarship (specifically STS methods,⁴² like case study⁴³ or actor network theory⁴⁴ which recognizes the agency embedded in artifacts), the author does not necessarily help the study of law escape the dilemma of being overly rooted in moral criteria. However, by systematising the methodology of these analyses, he makes it far easier to position law as a rigorous discipline that can be framed within a solid methodological structure.

⁴² Calo R. (2025) *op. cit.* p. 53.

⁴³ Calo R. (2025) *op. cit.* p. 56.

⁴⁴ Calo R. (2025) *op. cit.* p. 58.

LIST OF REFERENCES

- [1] Calo R. (2025) *Law and Technology: A Methodical Approach*. Oxford University Press
- [2] Collingridge D.(1980) *The Social Control Of Technology*. Frances Pinter, pp. 13-21
- [3] Duncan, N. J. and Hutchinson, T. (2012). *Defining And Describing What We Do: Doctrinal Legal Research*. Deakin Law Review, 17(1), pp. 83-119
- [4] Easterbrook F. H.(1996) *Cyberspace And The Law Of The Horse*. University of Chicago Legal Forum 207
- [5] Lessig L. (1999) *Code And Other Laws Of Cyberspace*. Basic Books, A Member of the Perseus Books Group
- [6] Regulation (EU) 2024/1689 Of The European Parliament And Of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Official Journal of the European Union 2024/1689, 12 July 2024. Available from: <http://data.europa.eu/eli/reg/2024/1689/oj> [Accessed 18 June 2026]
- [7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Official Journal of the European Union, L 277, 27 December 2022. Available from: <http://data.europa.eu/eli/reg/2022/2065/oj> [Accessed 18 June 2026]

MUJLT Official Partner (Czech Republic)

**ROWAN[®]
LEGAL**

ROWAN LEGAL, advokátní kancelář s.r.o
<https://rowan.legal>

Cyberspace 2025 Partners

**ROWAN®
LEGAL**



LIST OF ARTICLES

Ugochukwu Godspower Ehirim: Regulating the Emerging Mobile Money Services and National Digital Currencies in Nigeria and South-Africa.....3

Viona Rashica: The Evolution of Digital Diplomacy: The Impact of Technological Advancements on Diplomatic Practice.....33

Jan Wittlin: Legal and Regulatory Compliance Challenges for Equity Token Secondary Market Operators in the European Union.....59

Nimrod Mike: Another View on Article 22 GDPR: The Future of Automated Decision-Making.....87

Yuliia Kravchenko, Thomas Hoffmann, Eric Blake Jackson: Embedding a Harmonised EU Identity System into a Mature National E-State: An Estonian Case Study.....119

LIST OF BOOK REVIEWS

Katarzyna Katana: Overcoming Technology’s Myths – A Review of Law and Technology: A Methodical Approach.....145