The Impact of Data Protection Legislation on Fintech and Financial Inclusion

RALUCA ANICA ONUFREICIUC[1], PH.D. STUDENT
PARIS-PANTHÉON-ASSAS UNIVERSITY, FRANCE; TEACHING ASIST. "NICOLAE TITULESCU" UNIVERSITY OF BUCHAREST, ROMANIA,
DR RAUL FELIX HODOŞ[2], PH.D. STUDENT
THE BUCHAREST UNIVERSITY OF ECONOMIC STUDIES; ASSOCIATE PROFESSOR PHD, "1 DECEMBRIE 1918" UNIVERSITY, ALBA IULIA, ROMANIA
CRINA MALCOCI[3], PH.D. STUDENT
UMFST "GEORGE EMIL PALADE" TÂRGU MUREŞ, ROMANIA

Abstract: *This paper examines the relationship between fintech, data protection legislation, and financial inclusion, highlighting both the opportunities and systemic risks associated with the digital transformation of finance. Drawing on theoretical perspectives, regional case studies, and regulatory analysis, the study shows that fintech can expand access to financial services through digital payments, algorithmic credit, automated savings, and robo-advised investments. Yet these mechanisms also create risks of over-indebtedness, algorithmic discrimination, digital exclusion, and cybersecurity vulnerabilities. The paper argues that robust data protection frameworks, such as the EU's General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act), are not barriers to innovation but preconditions for trust and sustainable inclusion. Comparative evidence from Africa, Asia, Latin America, the United States, and Europe demonstrates that the quality of data governance determines whether fintech becomes a tool for democratization or a vector of new inequalities. The conclusion emphasizes that data protection and financial inclusion are inseparable: without clear rights, transparency, and accountability in the use of artificial intelligence, digital finance risks producing superficial rather than genuine inclusion.*
Keywords: *artificial intelligence, data protection, financial inclusion, fintech, GDPR.*

1. INTRODUCTION

Over the past two decades, fintech has become one of the most dynamic phenomena transforming the global economy. Whereas in the past access to financial services depended on the proximity of a bank branch, the existence of collateral, or a credit history, today it can be reduced to owning a mobile phone with internet access and a few minutes required to download an application. This transformation is not only technological but also social and political. It brings to

[1] Raluca Anica Onufreiciuc, PhD candidate Paris-Panthéon-Assas University, France; Nicolae Titulescu University of Bucharest, Faculty of Law, Romania, Assistant Professor, Faculty of Law and Administrative Sciences, Stefan cel Mare University of Suceava, ORCID: https://orcid.org/0009-0007-2583-1766
Scopus ID: 58562295800; Onufreiciuc, Raluca Anica – Author details – Scopus Preview; Scopus preview – Scopus – Search for an author profile Web of Science Researcher ID: FQL-0191-2022
Google Scholar:https://scholar.google.com/citations?user=EC0-uN4AAAAJ&hl=ro; https://profesionisti.juridice.ro/raluca-onufreiciuc
[2] Dr Raul Felix Hodoş, Associate Professor, "1 Decembrie 1918" University, Alba Iulia, Romania and Ph.D. Student (his 2nd PhD) – The Bucharest University of Economic Studies Romania, and ORCID: 0000-0001-8500-135X, Scopus Author ID: 58563100400 , Web of Science Researcher ID ADG-7045-2022 Raul Felix Hodos – Google Scholar
[3] Crina Malcoci (Cucoara), PhD Student UMFST "George Emil Palade" Târgu Mureș -ORCID: https://orcid.org/0009-0006-3881-0190
SCOPUS ID: https://id.elsevier.com/settings/redirect?code=RZOQaMF6LyNoT3ZISFYpYa9Tsd-bK6ikoJIUUfCF
WEB OF SCIENCE RESEARCHER ID: OZD-5277-2025
GOOGLE SCHOLAR: https://scholar.google.ro/citations?view_op=list_works&hl=ro&user=xsLb_iYAAAAJ

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

the forefront the promise of a more democratic financial world, in which traditional barriers disappear, and inclusion becomes possible for groups that have been marginalized for decades.

Financial inclusion is now recognized as an essential component of sustainable development. Datasets published by the World Bank in the *Global Findex Database 2021* show that more than 1.4 billion adults did not have access to a formal bank account[4]. This exclusion is not only an economic issue but also a social one: without access to secure payments, savings, credit, or insurance, individuals remain vulnerable to financial shocks, deprived of entrepreneurial opportunities, and dependent on the informal economy. Consequently, financial exclusion amplifies poverty and inequality.

Fintech promises to change this reality through mechanisms such as digital payments, microcredit, automated savings, and the democratization of investment. There are numerous examples: *M-Pesa*[5] in Kenya enabled money transfers via SMS, Revolut[6] and Wise[7] reduced the costs of international remittances, Nubank[8] democratized access to credit cards in Brazil, and Robinhood[9] opened capital markets to millions of retail investors. However, these innovations cannot be understood without considering the role of data and its governance. Unlike traditional banks, fintechs rely on the intensive processing of massive volumes of data – from classic identifiers (name, address, bank account) to behavioural, biometric, and inferential data. In this sense, data protection is not a secondary element but one of the keys to the success or failure of fintech as an instrument of financial inclusion.

2. THEORETICAL FOUNDATIONS

The link between financial development and economic growth has been consistently documented in economic literature. Beck, Demirgüç-Kunt, and Levine[10] showed that financial deepening stimulates GDP growth and reduces social inequalities by facilitating access to capital for SMEs and households. However, access to financial services remains uneven. Women, rural populations, and people without stable incomes are often excluded from traditional banking services. Amartya Sen, through the capability approach, offered another dimension[11] to this analysis. He argued that development should not be measured solely by economic indicators but by the real freedoms individuals can exercise. Access to financial services is thus a condition for exercising economic and social freedom. Financial inclusion is not only about the number of accounts opened but about people's ability to plan for the future, protect their resources, and develop their potential.

Within this theoretical framework, fintech emerges as a disruptive innovation. Philippon shows that fintech reduces transaction costs and increases competition, bringing benefits to consumers and the economy[12]. Arner, Barberis, and Buckley describe fintech as the fourth financial

[4] Demirgüç-Kunt, A., Klapper, L. & Singer, D., 2022. *The Global Findex Database 2021*.Washington: World Bank, pp. 11–15.
[5] M-Pesa — Investopedia, "M-Pesa", https://www.investopedia.com/terms/m/mpesa.asp.
[6] More about Revolut, in https://www.revolut.com/en-US/
[7] Further details about Wise, in https://wise.com/
[8] See more about the largest fintech bank in Latin America, in https://nubank.com.br/
[9] https://robinhood.com/us/en/
[10] Beck, T., Demirgüç-Kunt, A. & Levine, R., „Finance, inequality and the poor," in *Journal of Economic Growth*, 12(1), 2207, pp.27–28.
[11] Sen, A., *Development as Freedom*, 1999, New York: Knopf, pp.35–40.
[12] Philippon, T., „The FinTech opportunity," *NBER Working Paper Series*, No. 22476, 2016, Cambridge, MA: National Bureau of Economic Research, pp.2–4.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

revolution, after the creation of modern banks, mass credit, and financial globalization[13]. The central element is how technology is used to reach segments ignored by traditional systems.

3. FINTECH, ARTIFICIAL INTELLIGENCE AND DATA PROTECTION

What differentiates fintech from banking institutions is not only the absence of costly physical infrastructure but the intensive use of emerging digital technologies, especially artificial intelligence (AI). Machine learning algorithms are used to assess credit risk, detect fraud, personalize offers, and manage portfolios through robo-advisors. These systems have the potential to expand access to finance for individuals without a banking history, using alternative data such as utility payments, mobile phone records, or even online browsing behaviour[14].

However, AI raises serious issues of fairness and transparency. Barocas and Selbst[15] showed that algorithmic models can generate indirect discrimination when they rely on proxy data that reflect structural inequalities. A relevant case is Apple Card[16], where the credit algorithm was accused of gender discrimination, with women receiving lower credit limits than men with similar profiles. This episode[17] demonstrated that, without legal safeguards, fintech can transform "inclusion" into a new form of exclusion. Here the impact of GDPR is crucial, providing a unique framework for user protection. Article 22 of GDPR[18] prohibits fully automated decisions producing legal effects without explicit consent or additional safeguards. Thus, when a fintech uses AI to refuse a loan, it must provide the possibility of human review and the right to contest the decision. In this way, European legislation[19] not only protects privacy but directly contributes to fairer financial inclusion.

In the long run, the integration of AI into fintech will make data protection even more central. Complex algorithmic models are difficult to explain and audit, which accentuates the need for transparency and accountability rules. The recently adopted AI Act[20] classifies financial scoring systems as high-risk applications, obliging operators to implement strict governance measures. This approach confirms that data and AI regulation is an integral part of financial inclusion strategies: without safeguards, public trust disappears, and fintech adoption stagnates.

3.1. Regional Case Studies: Fintech, Data Protection, and Financial Inclusion

The regional analysis shows that fintech has enormous inclusion potential, but its impact is determined by the quality of data protection legislation and the way AI is used. Africa and Asia have demonstrated that technology can bring millions of people into the system, but in the absence of clear rules, inclusion remains vulnerable to abuse. Latin America[21] democratized access, but cyber and

[13] Arner, D.W., Barberis, J. & Buckley, R.P., The evolution of Fintech: A new post-crisis paradigm?, in *Georgetown Journal of International Law*, 47(4), 2016, p. 1271.

[14] Borges, D. & Lutz, E., Algorithmic discrimination in digital credit markets: An analysis of fairness, transparency and accountability, in *Journal of Banking Regulation*, 22(2),2021, pp.141–143.

[15] Barocas, S. & Selbst, A.D., Big data's disparate impact, in *California Law Review*, 104(3), 2016, p. 674.

[16] See more details in https://www.apple.com/apple-card/

[17] BBC News, "Apple's 'sexist' credit card investigated by US regulator," 2019, https://www.bbc.com/news/business-50365609.

[18] European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4 May 2016, art. 22.

[19] Finance Watch, "The Digital Fairness Act must ensure a safer, fairer retail finance marketplace," (04 November 2025),https://www.finance-watch.org/policy-portal/digital-finance/the-digital-fairness-act-must-ensure-a-safer-fairer-retail-finance-marketplace/

[20] European Union, Regulation (EU) 2024/1689 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act), OJ L 202, 12 July 2024.

[21] World Bank, "Ciberseguridad en América Latina y el Caribe," World Bank Blogs, https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

data risks are high. The United States[22] exemplifies rapid innovation without adequate protection, while Europe confirms that data protection is the foundation of authentic and sustainable inclusion.

3.1.1. Sub-Saharan Africa – M-Pesa and the Data Protection Dilemma

Sub-Saharan Africa is often considered the global laboratory of financial inclusion through fintech. Launched in 2007, M-Pesa enabled money transfers via SMS, without the need for a classic bank account. Within a few years, the platform served over 20 million users in Kenya and Tanzania, most of them previously excluded from the formal financial system[23]. The impact on household welfare was significant: access to secure payments increased consumption and reduced vulnerability to economic shocks. Yet M-Pesa and similar solutions raised serious concerns about data protection. Users were required to provide identification information and accept that their transactions would be centrally stored. In the absence of a framework comparable to GDPR, such data could be used for commercial or political purposes. As fintechs become dominant players, the lack of clear data protection legislation undermines user trust and limits the sustainability of inclusion.

As AI begins to be used for credit scoring and fraud detection in Africa, risks multiply. If algorithmic models are applied without transparency obligations and without appeal guarantees, there is a danger that the same vulnerable groups included through mobile payments may be excluded through automated credit mechanisms[24]. The conclusion for Africa is that fintech has shown enormous potential, but the future of inclusion depends on creating a legal framework for data protection and AI governance.

3.1.2. Asia – India and China Between Inclusion and Control

In Asia, fintech has experienced spectacular growth. India has become emblematic through the combination of biometric identification via Aadhaar[25], digital payments through UPI, and the expansion of microcredit platforms. The *Global Findex Database* shows that the share of adults with a bank account rose from 53% in 2014 to 80% in 2021, largely due to digital payments[26].

However, this rapid inclusion also brought risks. Hundreds of microcredit apps offered instant loans, evaluated through algorithms relying on alternative data such as mobile phone history. IMF[27] (*International Monetary Fund*) documented cases of over-indebtedness and abusive collection practices. From a data protection perspective, the *Digital Personal Data Protection Act*[28] introduced modern rules, but its excessive reliance on consent has created the phenomenon of "consent fatigue"[29]. Users accept conditions without understanding their implications, undermining trust, and limiting the effectiveness of protection.

China, through Ant Group[30] and its integrated financial ecosystems, has included millions of people in the formal financial circuit. Yet the regulatory philosophy[31] is different: the *Personal Information Protection Law* (PIPL) offers protection similar in form to GDPR, but in practice data can be used for purposes of national. AI is widely used for social scoring and credit assessment,

[22] "EU General Court Upholds EU–U.S. Data Privacy Framework," Ethics & Compliance – Swiss Association, https://ethics-compliance.ch/eu-general-court-upholds-eu-u-s-data-privacy-framework/

[23] Jack, W. & Suri, T., Risk sharing and transaction costs: Evidence from Kenya's mobile money revolution, in *American Economic Review*, 104(1), 2014, pp.185–190.

[24] Advisense, "The EU AI Act and Its Implications for Credit Risk Models in Banking," 19 March 2025, https://advisense.com/2025/03/19/the-eu-ai-act-and-its-implications-for-credit-risk-models-in-banking/.

[25] More about *My Aadhaar*, in https://uidai.gov.in/en/

[26] Demirgüç-Kunt *et al.*, 2022, pp. 12–14

[27] IMF, *Fintech and Financial Inclusion*, 2023, Washington, pp.8–10.

[28] Republic of India, Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, 11 August 2023.

[29] Bhatia, G., The Digital Personal Data Protection Act in India: Promise and pitfalls, in *Juridical Tribune*, 13(2), 2023, p.89.

[30] More details about Ant Group, in https://www.antgroup.com/en

[31] Standing Committee of the National People's Congress, 2021. *Personal Information Protection Law (PIPL)*. Beijing: NPC.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

raising fundamental issues of autonomy and inclusion. Here, data protection does not guarantee fairness but serves political control.

The conclusion for Asia is ambivalent: fintech has expanded inclusion dramatically, but without a robust and balanced data protection framework, this inclusion remains fragile and subject to manipulation.

3.1.3. Latin America – Democratizing Banking but Data Vulnerabilities

Latin America is notable for fintechs that democratized access to financial services. Nubank, founded in 2013 in Brazil, attracted over 70 million customers by offering fee-free credit cards and a simple digital interface[32]. Mercado Pago[33], part of the Mercado Libre ecosystem, provided digital payment and savings solutions, becoming a major regional player. However, data protection regulation remains fragmented. BIS[34] warns that the lack of GDPR-like standards exposes consumers to cyber risks and commercial misuse of data. Moreover, the adoption of AI for credit scoring or fraud detection often occurs without clear obligations for audits or transparency. In this context, inclusion generated by fintech is real but unstable, relying more on platform reputation than on legal guarantees.

Latin America thus offers a paradox: fintech reduced costs and expanded access, but the absence of strong data protection risks undermining trust and limiting long-term progress.

3.1.4. Europe – Regulation as the Foundation of Sustainable Inclusion

Europe provides the clearest example of the role of data protection in supporting inclusion. European fintechs operate in an environment regulated by GDPR, PSD2[35], and, more recently, the AI Act. PSD2 introduced open banking, allowing third-party providers to access bank account data, but only with explicit consent and under strict security standards[36]. GDPR obliges fintechs to respect principles such as minimization, transparency, and accountability. In addition, CJEU jurisprudence strengthens these rules. The *Schufa Holding AG* case (C-634/21)[37] established that credit scores generated by algorithms are automated decisions, requiring fintechs to provide the right to appeal and human review.

The integration of AI in European fintech is governed by the AI Act (2024), which classifies financial scoring systems as high-risk applications and requires strict auditability. The result is slower inclusion compared to Asia or Latin America, but also more sustainable: users adopt fintech services because they trust that their data is protected and that decisions are made fairly.

3.1.5. United States – Fast Innovation, Fragmented Protection

The United States has produced some of the world's most famous fintechs, from Robinhood to LendingClub[38]. These platforms democratized investment and credit but were also involved in major controversies. The Apple Card case, where women received lower credit limits than men, illustrated the risk of algorithmic discrimination in the absence of strict transparency rules[39]. Unlike the EU, the US lacks a unified federal data protection law. The California Consumer Privacy

[32] Dorfleitner, G., Hornuf, L. & Kreppmeier, J., 2023. Promise not fulfilled: FinTech, data privacy, and the GDPR. *Electronic Markets*, 33(4), pp.1189–1192.

[33] Further details about Mercado Pago, in https://www.mercadopago.com.ar/

[34] BIS, Fintech and financial inclusion: drivers and policy implications, in *BIS Quarterly Review*, March 2022, pp. 52–53.

[35] European Union, Directive (EU) 2015/2366 on payment services in the internal market (PSD2), OJ L 337, 23 December 2015.

[36] European Commission, "Questions and Answers: Commission confirms adequacy decision for EU–U.S. Data Privacy Framework," Press corner, 2024, https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_5555

[37] Court of Justice of the European Union, Case C-634/21, *Schufa Holding AG v. Others*, judgment of 7 December 2023, ECLI:EU:C:2023:XXX.

[38] More about this platform. in https://www.lendingclub.com/

[39] Borges & Lutz, 2021, pp. 141–143.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

Act[40](2018) offers rights similar to GDPR[41], but only at the state level. Elsewhere, regulation is sectoral: HIPAA[42] for health, GLBA[43] for financial data. This fragmentation leaves major gaps in user protection and undermines trust. Although innovation is rapid, the resulting inclusion is shallow and vulnerable. Users may be excluded or discriminated against by opaque models, with no effective mechanisms for appeal. The US thus exemplifies the limits of fintech when robust data protection is absent.

The regional analysis demonstrates that fintech has immense potential for inclusion, but its impact is shaped directly by the quality of data protection legislation and the use of artificial intelligence. Africa and Asia show that technology can bring millions into the system, but without clear rules inclusion remains fragile. Latin America democratized access, but data and cyber risks are high. The US illustrates what fast innovation without protection means, while Europe confirms that robust data governance is the cornerstone of authentic and sustainable inclusion.

4. FINTECH MECHANISMS AND THE ROLE OF DATA PROTECTION IN INCLUSION

4.1. Digital Payments – From the Remittance Revolution to Data Protection Challenges

Digital payments represent the most visible dimension of financial inclusion through fintech. In many emerging economies, the possibility of sending and receiving money through mobile phones has meant, for the first time, integration into the formal financial system. According to World Bank data[44], between 2010 and 2021 the global average cost of international remittances fell from 9.3% to under 6%, largely due to competition generated by fintech platforms such as Wise and Revolut. AI plays a crucial role in digital payments, particularly in fraud detection and user authentication. Machine learning algorithms analyse transaction patterns to identify suspicious activity in real time. While these technologies increase security, they also require the collection and processing of highly sensitive data, including geolocation and behavioural information.

Under GDPR, such processing is considered high-risk. Location data, for instance, qualify as personal data and may only be processed if there is a clear and proportionate legal basis[45]. This framework ensures that inclusion through digital payments does not compromise privacy. In regions where no equivalent rules exist, the same technology that facilitates inclusion can expose users to surveillance or commercial exploitation of their data. Thus, data protection becomes a decisive factor in whether digital payments are adopted and trusted by vulnerable populations.

4.2. Alternative Credit – Algorithms, Scoring, and the Risk of Discrimination

Credit is the most sensitive dimension of financial inclusion. Traditional banks often exclude individuals without collateral or formal credit histories. Fintechs introduced innovative credit models based on algorithmic scoring. Instead of relying solely on classical banking history, these systems use alternative data such as utility payments, mobile phone records, and even online behaviours. In this way, millions of previously excluded individuals gain access to credit. Machine learning models identify predictive risk patterns in vast datasets. Borges and Lutz[46] showed that this approach may

[40] State of California, California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.100–1798.199 (enacted 28 June 2018).
[41] IAPP, "GDPR matchup: The California Consumer Privacy Act 2018", 31 July 2018, https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act
[42] United States Congress, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[43] United States Congress, Gramm–Leach–Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999).
[44] World Bank, 2022. *The Global Findex Database 2021*. Washington: World Bank, pp. 9–15.
[45] European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 4 May 2016, art. 4.
[46] Borges & Lutz, 2021, pp. 142.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

reduce exclusion but also risks reinforcing indirect discrimination when algorithms rely on proxies like postal codes, which correlate with socio-economic status or ethnicity.

In this sense, Article 22 of GDPR prohibits individuals from being subject to fully automated decisions with significant legal effects unless explicit consent or meaningful safeguards are provided. This rule protects inclusion by granting users the right to contest algorithmic decisions and request human review. In the US, the absence of an equivalent framework allowed cases like Apple Card[47], where women received lower credit limits than men with similar profiles, without clear explanations. China presents an even more controversial case: social scoring systems integrate financial behaviour with other aspects of civic life[48]. Without genuine guarantees of informational autonomy, algorithmic credit becomes a mechanism of control rather than inclusion. In Europe, by contrast, GDPR and the AI Act classify such scoring systems as high-risk and subject them to transparency and audit obligations, thus making inclusion both fairer and more sustainable.

4.3. Digital Savings and Financial Literacy – Profiling Users Responsibly

Digital savings solutions represent another way fintech contributes to inclusion. Applications known as "robo-savers" automatically round up payments and transfer the difference into savings accounts or investment funds. The World Economic Forum[49] shows that these mechanisms significantly increase savings among low-income users. Moreover, apps like Monzo[50] or Revolut integrate budgeting tools and personalized notifications, improving digital financial literacy. Often AI is used to analyse user transactions and build behavioural profiles, enabling personalized recommendations. Personalized features can indeed encourage higher savings, but they also bring significant concerns related to profiling. Under Article 22 GDPR, profiling is subject to explicit safeguards, requiring controllers to explain the underlying decision-making logic and to offer users the possibility to object.

This transforms data protection into a mechanism of inclusion: users who know their data are processed transparently, and who have control over personalization, are more likely to trust and adopt digital savings tools. Where these guarantees are absent, digital savings can become another arena of commercial manipulation rather than a path to empowerment.

4.4. Democratized Investments – Robo-Advisors and Algorithmic Auditability

Investments have traditionally been the preserve of wealthy individuals with advanced financial knowledge. Fintech has changed this paradigm. Platforms like Robinhood, eToro[51], and Betterment[52] allow small investors to access markets with minimal capital, while robo-advisors create customized portfolios based on risk profiles. Malverti, Bulgarelli, and Villa[53] showed that robo-advisors reduce costs and democratize market participation. However, these systems rely heavily on artificial intelligence, which processes user data to generate investment strategies. The risk lies in oversimplification: intuitive interfaces may obscure the complexity of financial markets and expose inexperienced users to significant losses.

The European Banking Authority[54] has warned that excessive simplification must be accompanied by transparency about risks. GDPR imposes explainability obligations, and the AI Act classifies robo-advisors as high-risk systems, subjecting them to strict audit requirements. These

[47] BBC News, 2019, https://www.bbc.com/news/business-50365609

[48] Liu, C., & Rona-Tas, A., Trusting by Numbers: An Analysis of a Chinese Social Credit System Governance Infrastructure, in Critical Sociology, 51(6), 2024, 1247-1265. https://doi.org/10.1177/08969205241246528

[49] World Economic Forum, The Future of Data-Driven Finance, 2022, Geneva, pp. 22–23.

[50] See also https://monzo.com/

[51] More about eToro, in https://www.etoro.com/ro/

[52] Further details in https://www.betterment.com/

[53] Malverti, R., Bulgarelli, D. & Villa, A., 2018. Robo-advisors and portfolio management. *Journal of Financial Transformation*, 47, pp.15–28, pp.16–19.

[54] EBA, *Report on the use of digital platforms in the EU banking and payments sector*, 2022, Paris, pp. 9–14.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

rules protect users and ensure that democratized investments contribute to genuine inclusion. In the United States, where such obligations do not exist at the federal level, Robinhood[55] has been accused of encouraging speculative trading among young users without adequate disclosure of risks. This demonstrates that without clear regulation, investment democratization may lead to new forms of exclusion: those with knowledge and resilience benefit, while others bear the costs of hidden risks.

5. INTERMEDIATE SYNTHESIS

Across payments, credit, savings, and investments, the same lesson emerges: data protection and AI governance are indispensable for fintech to deliver authentic financial inclusion. Where GDPR, the AI Act, or similar frameworks apply, inclusion is sustainable because it is built on trust and fairness. Where regulation is absent or fragmented, inclusion risks being superficial, marred by exploitation, discrimination, and erosion of confidence.

A. Systemic Risks of Fintech and Implications for Inclusion

Although fintech is widely associated with reducing barriers to access and democratizing financial services, practice and scholarship demonstrate that innovation can generate systemic risks that undermine both inclusion and data protection. Four risks stand out: digital over-indebtedness, algorithmic discrimination, the digital divide, and cybersecurity vulnerabilities.

B. Digital Over-Indebtedness

The flexibility of fintech credit, while beneficial for access, can easily lead to over-indebtedness. Unlike traditional banks, which apply prudential requirements, fintech platforms often provide instant loans based on alternative data such as mobile phone records or utility payments. In India, the proliferation of microcredit apps led to widespread over-indebtedness and even social crises, with reports of extreme pressure from collectors[56]. In Kenya, following the success of M-Pesa, instant credit services created "debt traps" for vulnerable users[57]. In this case, data protection rules are meant to keep things from going wrong. The principle of minimisation in the GDPR says that you cannot collect too much user data and that processing must be clear. The AI Act goes even further by saying that AI-powered credit scoring is very risky and needs close supervision. These frameworks protect not only privacy but also the long-term viability of financial inclusion by making sure that credit decisions are fair and responsible.

C. Algorithmic Discrimination

Algorithmic scoring and decision-making create another critical risk: discrimination. Even when algorithms are designed to be neutral, they can reproduce existing social inequalities by relying on proxy data. Barocas and Selbst[58] showed that variables such as postal codes or device types may indirectly correlate with ethnicity or gender, leading to exclusionary outcomes. The Apple Card case remains emblematic. Women received lower credit limits than men with similar profiles, and in the absence of GDPR-like obligations, they lacked the right to explanation or appeal. By comparison, Article 22 GDPR[59] bars the imposition of fully automated decisions that produce legal or similarly significant effects unless appropriate human intervention or explicit consent is in place. The AI Act reinforces this protection by imposing mandatory audit and governance requirements on high-risk algorithmic systems, including those used in credit-scoring and other financial decision-making contexts.

---

[55] More about this U.S.-based commission-free trading platform launched in 2013, in https://robinhood.com/eu/en/

[56] IMF, 2023, p. 9.

[57] BIS, 2022, p. 52.

[58] Barocas, S. & Selbst, A.D., Big data's disparate impact, in *California Law Review*, 104(3), 2016, p. 674.

[59] de Hert, P. & Lazcoz, G., "Radical rewriting of Article 22 GDPR on machine decisions in the AI era," European Law Blog (11 October 2021), https://www.europeanlawblog.eu/pub/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/release/1.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

Thus, in Europe, data protection law directly supports inclusion by ensuring that automated credit systems remain transparent, contestable, and fair. Where such frameworks are absent, fintech risks reproducing or even amplifying discrimination rather than overcoming it.

D. The Digital Divide

Fintech is often presented as a universal solution, but in reality it risks deepening the digital divide. In 2021, OECD[60] noted that access to digital services presupposes technological infrastructure, smartphones, and digital literacy. Rural populations, the elderly, and women in emerging economies are often left behind.

In Africa, while M-Pesa integrated millions into the financial system, the poorest communities lacking stable mobile networks or access to devices were excluded[61]. In India, limited digital literacy meant that formal access to fintech services often translated into precarious use, with users unable to understand contractual terms.

Here, data protection intersects with equity. GDPR requires that consent be informed and freely given, and obliges operators to provide clear, accessible information adapted to vulnerable users. This transforms data protection into a tool for inclusion: legislation ensures that services are not only available but also understandable and safe to use.

E. Cybersecurity Vulnerabilities

Fintech platforms process vast amounts of highly sensitive data – financial, biometric, and behavioural. Any breach undermines trust and jeopardizes inclusion. ENISA[62] (2022, pp. 12–18) highlights that fintechs are frequent targets of phishing, ransomware, and social engineering attacks.

GDPR requires operators to notify both authorities and users within 72 hours of a data breach. This obligation reinforces confidence, as users know they will be informed and protected. In jurisdictions without such requirements, users may remain unaware of data leaks for years, eroding trust and deterring participation in digital finance. Data protection thus becomes synonymous with resilience: without cybersecurity safeguards, inclusion collapses.

FINAL CONCLUSIONS AND POLICY RECOMMENDATIONS

The analysis conducted throughout this chapter demonstrates that fintech can truly transform financial inclusion, yet this promise can only be fulfilled within a strong framework of data protection and governance of artificial intelligence. The opportunities created by digital finance are clear: mobile payments lower remittance costs, algorithmic scoring extends credit to the unbanked, digital savings tools improve financial literacy, and robo-advisors democratize investments. But these innovations cannot be separated from the risks they generate. Digital over-indebtedness, algorithmic discrimination, the digital divide, and cybersecurity vulnerabilities are not marginal issues; they strike at the heart of financial inclusion.

Over-indebtedness illustrates the paradox of access without safeguards. "The rapid proliferation of instant microcredit applications in India and Kenya demonstrates that inclusion can become a debt trap when credit is extended irresponsibly." In this context, data protection rules are more than a privacy tool: they establish proportionality and transparency, limiting the misuse of user information for predatory offers. Similarly, algorithmic discrimination shows that artificial intelligence can replicate social inequalities. The Apple Card case revealed how opaque models can penalize women despite equivalent creditworthiness. European legislation, through Article 22 of GDPR and reinforced by the AI Act, responds by requiring human oversight and algorithmic audits.

[60] OECD, Financial Consumer Protection and Financial Inclusion in the Digital Age, 2021, Paris, pp.21–23.
[61] Jack, W. & Suri, T., Risk sharing and transaction costs: Evidence from Kenya's mobile money revolution. *American Economic Review*, 104(1), 2014, pp.185–190.
[62] ENISA, *Threat Landscape for Financial Services*, 2022, Athens, pp.12–18.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

These legal mechanisms transform the right to data protection into a guarantee of equity in access to financial services.

The digital divide further illustrates the complexity of inclusion. Even when services are available, they cannot be used effectively if individuals lack devices, connectivity, or digital literacy. Here, data protection law interacts with social policy: by demanding that information be presented in clear and accessible language, GDPR creates a duty for fintechs to design services that are understandable and inclusive. In contrast, where such obligations are absent, access remains formal but fragile. Cybersecurity vulnerabilities add another layer. Without strong safeguards, breaches undermine user trust and discourage participation in digital finance. Europe's obligation to notify breaches within seventy-two hours under GDPR is an example of how regulation can maintain trust and preserve inclusion.

Comparative experience suggests that Europe, with its integrated framework of GDPR, PSD2, and the AI Act, provides the most coherent model. Inclusion here may progress more slowly, but it is underpinned by trust and sustainability. Asia and Africa show impressive expansion, but in the absence of robust frameworks, inclusion is vulnerable to exploitation. Latin America illustrates both the democratizing power of fintech and the risks of fragmented regulation, while the United States demonstrates that rapid innovation without unified protection produces shallow inclusion marked by repeated scandals.

Looking ahead, artificial intelligence will intensify these challenges. Algorithms are becoming increasingly complex and opaque, raising urgent questions of explainability and accountability. The European AI Act anticipates this reality by classifying financial scoring systems as high-risk, requiring transparency and auditability. Yet the debate is only beginning. In the near future, financial inclusion will not depend solely on the availability of fintech platforms but on how societies regulate AI and integrate data protection into broader economic and social governance.

The broader conclusion is that data protection and financial inclusion are inseparable. Far from being a barrier, legislation on data protection is the infrastructure of trust without which no digital financial service can thrive. Where rules are robust, users feel safe to participate, adoption increases, and inclusion becomes real. Where protection is weak or fragmented, inclusion is only apparent, leaving users exposed to debt, discrimination, and insecurity. In this light, the governance of data and AI is not only a legal necessity but a condition for equitable economic development. Fintech can fulfil its democratizing promise, but only if it is built on the solid foundation of respect for rights, transparency in technology, and a vision of finance as a public good that serves society as a whole.

BIBLIOGRAPHY

Advisense, "The EU AI Act and Its Implications for Credit Risk Models in Banking," 19 March 2025,https://advisense.com/2025/03/19/the-eu-ai-act-and-its-implications-for-credit-risk-models-in-banking/.

Arner, D.W., Barberis, J. & Buckley, R.P., "The evolution of Fintech: A new post-crisis paradigm?", *Georgetown Journal of International Law*, 47(4), 2016, pp.1271–1319.

Barocas, S. & Selbst, A.D.,"Big data's disparate impact". *California Law Review*, 104(3), 2016, pp. 671–732.

BBC News, "Apple's 'sexist' credit card investigated by US regulator,"2019, https://www.bbc.com/news/business-50365609.

Beck, T., Demirgüç-Kunt, A. & Levine, R., "Finance, inequality and the poor", *Journal of Economic Growth*, 12(1), 2007, pp.27–49.

Bhatia, G., The Digital Personal Data Protection Act in India: Promise and pitfalls. *Juridical Tribune*, 13(2), 2023, pp.87–90.

BIS, *Fintech and financial inclusion: drivers and policy implications*. *BIS Quarterly Review*, March 2022, pp.45–67.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

Borges, D. & Lutz, E., "Algorithmic discrimination in digital credit markets: An analysis of fairness, transparency and accountability". *Journal of Banking Regulation*, 22(2), 2021, pp.139–152.

Costea, Maria, and Simion Costea. *Diplomație și actori geopolitici în epoca interdependenței complexe [Diplomacy and Geopolitical Actors in the Age of Complex Interdependence]*. Cluj-Napoca, Napoca Star, 2021.

Costea, Maria, Costea Simion, "Ukraine between EU and Eurasian Regional Project in 2013", p.113-131, in *Transylvanian Review*, Vol. XXIV, Supplement No. 1, 2015 DOI: 10.5281/zenodo.15564422

Court of Justice of the European Union, *Case C-634/21, Schufa Holding AG v. Others, judgment of 7 December 2023*, ECLI:EU:C:2023:XXX.

Demirgüç-Kunt, A., Klapper, L. & Singer, D., *The Global Findex Database 2021*, 2021, Washington, pp.9–20.

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S. & Hess, J., *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*, 2022, Washington, pp.11–15.

Dorfleitner, G., Hornuf, L. & Kreppmeier, J., Promise not fulfilled: FinTech, data privacy, and the GDPR. *Electronic Markets*, 33(4), 2023, pp.1187–1206.

EBA, *Report on the use of digital platforms in the EU banking and payments sector*, 2022, Paris, pp.9–14.

ENISA, *Threat Landscape for Financial Services*, 2022, Athens, pp.12–18.

*** „EU General Court Upholds EU–U.S. Data Privacy Framework," *Ethics & Compliance – Swiss Association*, https://ethics-compliance.ch/eu-general-court-upholds-eu-u-s-data-privacy-framework/

European Commission, "Questions and Answers: Commission confirms adequacy decision for EU–U.S. Data Privacy Framework", Press corner, 2024, https://ec.europa.eu/commission/presscorner/ detail/en/qanda_ 19_5555

European Union, *Directive (EU) 2015/2366 on payment services in the internal market (PSD2),* OJ L 337, 23 December 2015.

European Union, *Regulation (EU) 2016/679 (General Data Protection Regulation),* OJ L 119, 4 May 2016.

European Union, *Regulation (EU) 2024/1689 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act),* OJ L 202, 12 July 2024.

Finance Watch, "The Digital Fairness Act must ensure a safer, fairer retail finance marketplace", (04 November 2025),https://www.finance-watch.org/policy-portal/digital-finance/the-digital-fairness-act-must-ensure-a-safer-fairer-retail-finance-marketplace/

Hert de, P. & Lazcoz, G., "Radical rewriting of Article 22 GDPR on machine decisions in the AI era," European Law Blog (11 October 2021), https://www.europeanlawblog.eu/pub/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/release/1.

IAPP, "GDPR matchup: The California Consumer Privacy Act 2018", 31 July 2018, https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act

IMF, *Fintech and Financial Inclusion*, 2023, Washington, pp.8–10.

Jack, W. & Suri, T., "Risk sharing and transaction costs: Evidence from Kenya's mobile money revolution". *American Economic Review*, 104(1), 2014, pp.183–223.

Liu, C., & Rona-Tas, A., "Trusting by Numbers: An Analysis of a Chinese Social Credit System Governance Infrastructure", *Critical Sociology*, 51(6), 2024, pp. 1247-1265. https://doi.org/10.1177/08969205241246528

Malverti, R., Bulgarelli, D. & Villa, A., Robo-advisors and portfolio management. *Journal of Financial Transformation*, 47, 2018, pp.15–28.

M-Pesa — Investopedia, "M-Pesa", https://www.investopedia.com/terms/m/mpesa.asp.

Natea, Mihaela Daciana; Costea, Maria; Costea, Simion. *EU Security and Multicultural Societies. Dealing with a Russian Empire Revival*, Paris, L'Harmattan, 2024

Natea, Mihaela Daciana; Costea, Simion (eds), *EU Law and Politics at the Crossroads: Navigating the Complexities of AI, Digitalization, Data Protection, Security, and Radicalization (L'Europe unie/United Europe, Paris, 20/2023, special volume),* Cluj-Napoca: Napoca Star, 2023. DOI 10.5281/zenodo. 15182658

Natea, Mihaela Daciana; Costea, Simion (eds), *The EU foreign and security dilemmas in a challenging world (L'Europe unie/United Europe 19/2023, special volume)* Cluj- Napoca: Napoca Star, 2023

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

Natea Mihaela Daciana, The European Knowledge-Security Nexus: Science Diplomacy as a Policy Tool Against Hybrid Threats, Europolity-Continuity and Change in European Governance, nr6/2025
OECD, *Financial Consumer Protection and Financial Inclusion in the Digital Age*, 2021, Paris, pp. 21–25.
Philippon, T., "The FinTech opportunity". *NBER Working Paper Series*, No. 22476, 2016, Cambridge, National Bureau of Economic Research, pp.2–4.
Republic of India, Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, 11 August 2023.
Sen, A., *Development as Freedom*, 1999, New York.
Standing Committee of the National People's Congress, *Personal Information Protection Law (PIPL)*, Beijing, 2021.
State of California, *California Consumer Privacy Act of 2018 (CCPA),* Cal. Civ. Code § 1798.100–1798.199 (enacted 28 June 2018).
United States Congress, *Gramm–Leach–Bliley Act (GLBA),* Pub. L. No. 106-102, 113 Stat. 1338 (1999).
United States Congress, *Health Insurance Portability and Accountability Act of 1996 (HIPAA),* Pub. L. No. 104-191, 110 Stat. 1936 (1996).
World Bank, "Ciberseguridad en América Latina y el Caribe", *World Bank Blogs*, https://blogs.worldbank.org/en/ latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
World Bank, *The Global Findex Database 2021*, 2022, Washington.
World Economic Forum, *The Future of Data-Driven Finance*, 2022, Geneva.
Websites:
https://www.revolut.com/en-US/
https://wise.com/
https://nubank.com.br/
https://robinhood.com/us/en/
https://www.apple.com/apple-card/
https://uidai.gov.in/en/
https://www.antgroup.com/en
https://www.mercadopago.com.ar/
https://www.lendingclub.com/
https://monzo.com/
https://www.etoro.com/ro/
https://www.betterment.com/

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3