ALGORITHMIC BIAS AND DATA PRIVACY IN AML TRANSACTION MONITORING: A COMPARATIVE ANALYSIS OF INDIA, UZBEKISTAN AND EUROPEAN UNION

Shashank Sidharth
Dual Degree Master's LL.M. Student,
National Forensic Sciences University, India and
Tashkent State University of Law, Uzbekistan
https://doi.org/10.5281/zenodo.21187281

Abstract

Banks and payment platforms increasingly rely on outside software vendors to run the artificial intelligence and machine learning systems behind their anti-money laundering (AML) and Know Your Customer (KYC) checks. This arrangement lets institutions process enormous volumes of transaction data far more efficiently than legacy systems allowed, but it also raises a hard question: when something goes wrong, who actually answers for it?

If a third-party AI vendor builds a transaction-monitoring tool that leaks personal data or wrongly flags innocent customers, who carries the legal responsibility the company that wrote the code, or the bank that bought and deployed it?

Across India, Uzbekistan, and the European Union, the financial institution not the vendor acts as the primary custodian of customer data and remains fully, non-delegable liable for algorithmic discrimination or privacy breaches caused by an outsourced AI system. A vendor contract cannot transfer away a bank's statutory duties.

Keywords: automated transaction monitoring, algorithmic bias, data privacy, third-party outsourcing, non-delegable liability, DPDP Act 2023, Law on Personal Data (Uzbekistan), EU GDPR, EU AI Act.

1. Introduction

Criminal networks now move money through digital channels faster than old rule-based monitoring software can track. In response, banks have largely replaced these legacy systems with AI-driven models that can flag suspicious patterns in something close to real time. Building such a model from scratch demands data-science expertise that most banks, payment providers, and fintech platforms simply do not have in-house, so the common route is to buy ready-made AI software or hire a specialist vendor to build a custom monitoring engine.

That choice creates a structural problem. A vendor's algorithm typically operates as a black box, its internal logic shielded by trade secrets and proprietary code that the bank cannot fully inspect. When that code wrongly tags an ordinary customer's spending as money laundering and freezes the account, or when a breach on the vendor's side exposes sensitive transaction data, the question of who is to blame becomes contentious very quickly.

Vendors tend to argue that their software is only advisory and that final responsibility sits with whoever deploys it. Banks, for their part argue that they should not be punished for flaws buried in code they neither wrote nor can see. This article examines that disagreement directly. Drawing on India's Digital Personal Data Protection (DPDP) Act, 2023, Uzbekistan's Law "On Personal Data" No. ZRU-547, and the European Union's General Data Protection Regulation (GDPR) alongside its Artificial Intelligence Act, it asks where legal liability actually lands when financial surveillance is outsourced.

2. Key Concepts and Theoretical Frameworks

The Outsourcing Paradox in Automated Financial Surveillance

Modern transaction monitoring sorts customers into risk categories using machine-learning models. Once that work is outsourced, two parties end up sharing the task. The vendor builds the algorithm, tunes its parameters, and trains it on an initial dataset; the bank or payment operator then feeds the live model real transaction data geolocations, merchant categories, the frequency of transfers, and so on.

The resulting paradox is fairly simple to state: the vendor controls the logic of the system, while the bank controls the data flowing into it. Neither side fully controls the outcome on its own, yet only one of them "the bank" answers directly to the regulator and the customer when that outcome goes wrong.

The Theory of Non-Delegable Statutory Responsibility

Companies routinely hire contractors precisely to move operational risk off their own books. Data protection law generally refuses to let that trick work where personal data is concerned. Because an individual's data is treated as an extension of their privacy rights, the entity that signed the customer up in the first place cannot point to a vendor contract and walk away from its obligations. Liability stays anchored to whichever institution faces the customer directly this is what lawyers mean when they describe a duty as "non-delegable."

Operational Reality and the AI Vulnerability Curve

It would be convenient to assume that buying a more sophisticated AI system automatically lowers a bank's exposure to both financial crime and legal risk. The empirical research does not support that assumption. Lyeonov, Hrytsenko, Trojanek, and Popp (2025) describe an inverted U-shaped relationship between how heavily an institution leans on AI and how well its AML function actually performs. A moderate amount of automation helps: it clears routine work and catches the obvious cases. But once an institution leans on complex, outsourced models without keeping any local oversight, the system becomes easier to defeat rather than harder.

Organised criminal groups study the predictable behaviour of standard vendor software and adjust their transaction patterns to stay beneath the radar. Lyeonov et al. (2025) find that how secure an AML system really is depending less on the sophistication of the AI itself and more on the domestic institutional framework surrounding it local oversight, internal compliance habits, and the like. So, when an outsourced model misses a layering scheme because it was built for a generic market rather than tuned to local risk, the institution that failed to supervise its own system cannot shift that failure onto the vendor that wrote the code.

Surveillance Mandates Against Fundamental Privacy

A second, deeper tension runs through all of this: state demands for financial surveillance sit uneasily next to the citizen's right to privacy. Trela (2025) examines the legal gaps between anti-money-laundering mandates and privacy guarantees, largely through a comparative study of Japan's AML/CFT regime set against practice in Germany, France, and Poland. When a bank moves from simple threshold checks to full behavioural profiling, it crosses from routine business administration into something closer to surveillance of the individual customer.

Trela (2025) frames this as a persistent mismatch between two bodies of law pulling in opposite directions: financial-intelligence rules push banks to gather and retain as much customer data as possible, while data-protection law penalises exactly that kind of broad, opaque profiling. Buying third-party software does not resolve this tension if anything, it sharpens it, since an unvetted vendor model is more likely to breach data-minimisation principles and leave the deploying bank exposed to penalties under privacy law.

3. Comparative Legal Frameworks and Liability Allocation

3.1 India: The Data Fiduciary Carries the Risk

India's digital payments market, dominated by the Unified Payments Interface (UPI), sits under the anti-money-laundering rules of the Prevention of Money-Laundering Act (PMLA), 2002. When Indian banks bring in third-party AI software to meet PMLA's monitoring requirements, their data obligations are set out separately, in the Digital Personal Data Protection (DPDP) Act, 2023.

The Fiduciary and the Processor

The DPDP Act splits responsibility between two roles.

• **Data Fiduciary [Section 2(i)]:** whoever decides why and how personal data is processed in this context, the bank or payment app.

• **Data Processor [Section 2(l)]:** whoever processes that data on the Fiduciary's instructions here, the AI vendor.

How the Act Assigns Liability

Section 8(1) closes the obvious escape route. It states that a Data Fiduciary remains responsible for complying with the Act "irrespective of any agreement to the contrary," even where the actual processing was carried out by its Data Processor. This is generally read as creating an effectively non-delegable, vicarious form of liability: a contract clause that tries to shift blame onto the vendor has no effect on the bank's statutory exposure.

Section 8(3) adds a duty of accuracy. If an outsourced model runs on flawed logic or biased training data and wrongly labels an ordinary customer's cash withdrawal as a "structurally anomalous" transaction leading to a frozen account the bank cannot point to a vendor bug as a defence. Under Section 8(3), the duty to keep the data behind a decision complete and accurate sit with the bank.

3.2 Uzbekistan: Owner and Operator Roles under the Law on Personal Data

Uzbekistan's banking sector runs its monitoring obligations under the Law "On Countering the Legalisation of Proceeds from Criminal Activity…" No. ZRU-258, which requires automated internal monitoring systems. Where a bank brings in an outside AI vendor to handle that data, the governing rules come from the Law of the Republic of Uzbekistan "On Personal Data" No. ZRU-547, available through the national legal database at lex.uz/docs/4831939.

Owner and Operator

Article 4 of the law sets out two roles.

• **Mulkdor (the Owner):** the entity that holds the personal data database in this case, the bank.

• **Operator:** whoever is authorised to process the data on the owner's behalf, which can include a third-party AI platform running cloud-based analytics.

How Liability Falls

Article 9 identifies the owner and the operator as the law's two participants, and Article 19 sets the substantive requirements both must meet when processing data. Read together, they put the burden of security on the owner: the bank has to ensure that any contractor handling its database applies proper technical safeguards. If a vendor suffers a breach, Article 31 confirms that the bank, as owner, remains the institution that the state and the customer deal with directly.

The territory question has shifted recently, and any analysis written before early 2026 is now out of date on this point. Until then, Article 27-1 required that the personal data of Uzbek citizens be collected, organised, and stored exclusively on servers physically located inside Uzbekistan a rule that created real friction for banks using international cloud-based AI vendors. Amendments that entered into force on 27 March 2026 relaxed this considerably.

Most categories of personal data may now be processed and stored abroad, provided the processor meets Uzbekistan's information-security standards and remains under the oversight of its authorised state bodies. A narrower category biometric data, genetic data, and the personal data of telecommunications-service users must still stay on Uzbek soil. In practical terms, a bank sending an AI vendor transaction data outside that narrow category no longer automatically breaches the localisation rule, though it still has to document that the vendor satisfies the security conditions the amended law sets out.

3.3 The European Union: Joint Controllers and the AI Act

The EU runs the most protective framework of the three, layering the GDPR together with the newer AI Act.

Controller Responsibility under the GDPR

GDPR Article 4(7) defines the bank as the "Data Controller." Article 24 then puts the burden of proof on the bank: it must be able to show that whatever an outside vendor does with its data on its behalf meets the data-minimisation principle in Article 5 and the fairness requirements that apply to profiling.

If a vendor goes further than plain processing if it starts using the bank's own customer data to retrain and improve its own commercial models it stops being a simple processor. Under GDPR Article 26 and the case law on joint controllership developed by the Court of Justice of the European Union, the vendor and the bank can become joint controllers, both jointly and severally liable for any privacy violation or discriminatory profiling that follows.

The AI Act's Two-Sided Liability

The EU AI Act (Regulation (EU) 2024/1689) splits obligations between the company that builds the system and the one that runs it.

- **The Provider (the AI vendor):** bound by AI Act Article 16 to test the system for demographic bias, log its operation transparently, and build in a human override.
- **The Deployer (the bank):** bound by AI Act Article 26 to monitor the system while it is live, feed it clean input data, and keep a genuine human in the loop.

A bank that buys an unvetted model and lets it run unsupervised risks heavy fines for that deployment failure alone, regardless of how carefully the vendor built the underlying system.

4. The Tripartite Liability Matrix

The table below summarises how exposure differs across the three jurisdictions once a bank outsources its automated transaction monitoring.

Regulatory Metric	India (DPDP Act, 2023)	Uzbekistan (Law on Personal Data, ZRU-547)	European Union (GDPR / AI Act)
Primary target of state penalties	The Data Fiduciary (the bank). Processors are not fined directly by the Board; the Fiduciary absorbs the initial liability.	The mulkdor, or owner (the bank). State regulators hold the bank directly liable for any mishandling of data by its agents.	Dual liability. Regulators can fine the Controller (the bank) up to 4% of global annual turnover under the GDPR, or fine the AI Provider directly under the AI Act.
Contractual protection	Void against the state. Section 8(1) nullifies any contract clause that tries to shift	Limited. The bank stays responsible for auditing its vendor's security measures	Joint and several liability. Under GDPR Article 26, if a vendor reuses bank data to

Regulatory Metric	India (DPDP Act, 2023)	Uzbekistan (Law on Personal Data, ZRU-547)	European Union (GDPR / AI Act)
	statutory liability onto the vendor.	under Article 19, regardless of what the contract says.	train its own models, both parties face full enforcement exposure.
Consequences of automated mistakes	The bank is liable for inaccurate, automated decisions under Section 8(3).	The bank Is liable for processing that deviates from its stated collection purpose, under Article 12.	The bank is liable under GDPR Article 22 if an account is frozen without genuine human review, and under AI Act Article 26 for inadequate oversight of a deployed system.

Table 1: Tripartite Liability (India, Uzbekistan and European Union)

5. Technical and Legal Safeguards

Outsourcing AML software does not have to mean accepting open-ended liability. Two practical measures go a long way toward closing the gap between what a vendor builds and what a bank can defend to a regulator.

Tokenising Data before It Leaves the Bank

To meet the data-minimisation rules under both the GDPR and the DPDP Act, a bank can strip out personally identifying details names, national ID numbers, phone numbers before any raw transaction record reaches the vendor's algorithm, replacing them with anonymous tokens. The AI model then only ever sees transaction patterns: amounts, timing, frequency. Even if the vendor suffers a serious breach, there is no personal data in the leaked dataset to expose.

Making the Model Explainable

GDPR Article 22 and DPDP Act Section 8 both push back against fully opaque, "black-box" decisions. A practical response is to require vendors to build in local explainability layers like SHapley Additive exPlanations (SHAP), for instance that translate a model's internal reasoning into something a compliance officer can actually read:

Flag Priority Score = (Rapid Destination Shift: +45) + (High-Velocity Micro-Payments: +30) − (Verified Merchant History: −15)

A readout of this kind gives a bank's compliance team something concrete to review before confirming an automated account freeze, rather than asking them to take the algorithm's word for it.

6. Conclusion

Outsourcing the technology behind AML monitoring does not outsource the legal responsibility that comes with it. In India, Uzbekistan, and the EU alike, the institution that holds the customer relationship stays on the hook for the accuracy, security, and fairness of the system it deploys, regardless of who wrote the underlying code.

The research supports this from two directions: heavy, unsupervised reliance on AI creates real operational vulnerabilities (Lyeonov et al., 2025), and the gap between surveillance mandates and privacy rights creates real legal ones (Trela, 2025). A bank cannot hide behind a vendor's trade secrets or its own technical ignorance when something goes wrong. The practical answer is active governance: tokenise data before it reaches a vendor,

demand explainable models, and keep a human genuinely in the loop before any algorithm gets to restrict a customer's access to their own money.

References

1. European Union. (2016). 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 (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
2. European Union. (2024). 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). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
3. Lyeonov, S., Hrytsenko, L., Trojanek, R., & Popp, J. (2025). Who benefits from AI in money laundering in Europe: The organised criminals or the AML services? Human Technology, 21(1), 222–245. https://ht.csr-pub.eu/index.php/ht/article/view/461
4. Republic of India. (2023). The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Ministry of Electronics and Information Technology. https://www.meity.gov.in/
5. Republic of India. (2002). Prevention of Money-Laundering Act, 2002. Financial Intelligence Unit India. https://fiuindia.gov.in/
6. Republic of Uzbekistan. (2019). Qonun "Shaxsga doir ma'lumotlar to'g'risida" No. O'RQ-547 (Law on Personal Data), as amended through 26 March 2026. https://lex.uz/docs/4831939
7. Republic of Uzbekistan. (2004). Qonun "Jinoiy faoliyatdan olingan daromadlarni legallashtirishga… qarshi kurashish to'g'risida" No. O'RQ-258 (Law on Countering the Legalisation of Proceeds from Criminal Activity). https://lex.uz/docs/1399896
8. Reserve Bank of India. (2025). Reserve Bank of India (Commercial Banks – Know Your Customer) Directions, 2025 (RBI/DOR/2025-26/169, DOR.AML.REC.No.88/14.01.002/2025-26, 28 November 2025, updated 29 December 2025). https://www.rbi.org.in/
9. Trela, M. (2025). Artificial intelligence in financial security: Legal challenges in Japan's AML/CFT regime and comparative insights from selected EU countries. Security and Defence Quarterly, 52(4). https://doi.org/10.35467/sdq/214090