Observatoire ARGA

Cross-Border Data, Compliance Screening and Procedural Safeguards: A Structural Risk Assessment for the Digital Economy and Financial Integration in Latin America

Author:

Sergey Khrabrykh — President of ARGA, PhD
Ekaterina Khomutinnikova

Organization: Observatoire ARGA – Sanctions and Compliance Unit

Mailing address: 21 rue de l'Aviation, 64600 Anglet, France

Contacts: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org

Paris, 17 February 2026

Table of Contents

EXECUTIVE SUMMARY

The digital economy of Latin America relies on stable cross-border data exchange, automated compliance systems, and trust in financial infrastructure. However, the integration of multiple data sources — including sanctions lists, adverse media, international notifications, judicial registries, and private compliance databases — into automated screening systems creates a new class of structural risks.

The core problem lies in the mismatch between the speed at which digital risk signals spread and the speed at which they can be corrected. Erroneous, outdated, or contextually distorted data may generate a long-term "reputational trace," affecting access to banking services, cross-border payments, investment flows, and participation in digital platforms.

This report provides:
– an analysis of cross-border data architecture in the region;
– a typology of compliance-screening vulnerabilities;
– the concept of a "data-to-decision audit trail" as a transparency standard;
– a model for rectification and clean-up of data;
– recommendations for ECLAC on shaping a regional data governance agenda within financial and digital sectors.

DIGITAL ECONOMY AND COMPLIANCE AS TRUST INFRASTRUCTURE

2.1 Data as the foundation of financial integration

Financial systems across the region increasingly rely on:
– remote identification;
– digital KYC procedures;

– algorithmic risk scoring;
– automated transaction monitoring.

2.2 The role of trust

Trust in data accuracy and integrity underpins:
– access to banking services;
– fintech development;
– e-commerce;
– cross-border trade.

When data is unreliable or cannot be corrected, trust in financial infrastructure deteriorates.

ARCHITECTURE OF CROSS-BORDER DATA IN AML/SANCTIONS AND KYC FRAMEWORKS

3.1 Data sources

– governmental lists and registries;
– international notifications;
– judicial databases;
– media and adverse media;
– private compliance providers.

3.2 Cross-border propagation

Information generated in one jurisdiction may rapidly spread through:
– data provider APIs;
– global screening platforms;
– internal databases of international banks.

3.3 Synchronization challenges

Data updates, corrections, or deletions are often not synchronized across systems and jurisdictions.

VULNERABILITIES: DATA CONTAMINATION, OUTDATED RECORDS, LOW-QUALITY SOURCES

4.1 Data contamination

An incorrect entry in a single source may be replicated across multiple systems.

4.2 Outdated data

Records may remain in private databases even after cases are closed or allegations are dismissed.

4.3 Low-quality source material

Media publications without judicial confirmation may be treated as high-risk signals.

4.4 Algorithmic amplification

Automated systems tend to amplify any negative signal regardless of legal status or context.

PROCEDURAL SAFEGUARDS IN THE ERA OF AUTOMATED SCREENING

5.1 Right of access and correction

Individuals and entities should have:
– access to data concerning them;
– the ability to request corrections;
– reasonable processing timelines.

5.2 The “opaque refusal” problem

Financial institutions often deny services without disclosing reasons, citing internal risk policies.

5.3 Balancing security and rights

Regulators must maintain a balance between AML effectiveness and the right to data rectification.

SECONDARY EFFECTS: FINTECH, E-COMMERCE, INVESTMENT, CROSS-BORDER TRADE

6.1 Fintech

Unreliable data may restrict:
– access to payment systems;
– banking partnerships;
– international expansion.

6.2 Cross-border trade

Erroneous compliance blocks slow transactions and increase costs.

6.3 Investment

Investors consider not only legal frameworks but also practical data governance risks and the likelihood of false restrictions.

THE “DATA-TO-DECISION AUDIT TRAIL” MODEL

7.1 Source transparency

Each decision should have traceability including:
– source of signal;
– date;
– procedural status.

7.2 Reliability tiers

Data should be classified as:
– confirmed by judicial decision;
– under investigation;
– media-based.

7.3 Periodic review

Automated systems should include mechanisms for periodic reassessment of data.

RECTIFICATION AND CLEAN-UP: DATA CORRECTION AND REMOVAL STANDARDS

8.1 Rectification

Correction procedures should include:
– clear submission channels;
– defined review timelines;
– notification of outcomes.

8.2 Clean-up

After cancellation or correction:
– internal and external databases must be updated;
– relevant units notified;
– updates recorded in audit trails.

8.3 Regional harmonization

ECLAC may support development of shared regional principles for data correction and removal.

RECOMMENDATIONS FOR ECLAC AND NATIONAL REGULATORS

– develop regional guidance on compliance data transparency;
– establish working groups on rectification and clean-up mechanisms;

– integrate algorithm auditability into digital economy policy frameworks;
– promote balance between security and procedural safeguards;
– strengthen cooperation between data protection and financial regulators.

CONCLUSION

Cross-border data has become critical infrastructure for Latin America's digital economy. Its quality, transparency, and correctability directly affect financial integration, fintech development, and investment climate stability.

Improving data governance standards, implementing audit trails, and strengthening rectification mechanisms will enhance trust in financial systems and support regional resilience.

ARGA Observatory presents this report as a contribution to regional dialogue on balancing digitalization, security, and procedural safeguards.

APPENDIX A. TERMINOLOGY

Data contamination — propagation of incorrect records across databases
Adverse media — negative media references used in compliance screening
Audit trail — traceability of decisions
Rectification — correction of data
Clean-up — procedural updating and removal of records

APPENDIX B. COMPLIANCE DATA QUALITY ASSESSMENT CHECKLIST

– source reliability
– procedural stage
– date and relevance
– independent verification
– availability of correction mechanisms
– review procedures
– documentation and traceability