Observatoire ARGA

Report on Sanctions and Compliance for 2025

TRANSFORMATION OF INTERNATIONAL LAW IN THE ERA OF SMART REGULATION

Sanctions Architecture, Export Control, Digital Risk Governance and the New Global Normativity

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Division

Correspondence Address: 14 rue Jacques Laffitte, Bayonne, 64100

Contact: info@argaobservatory.org

Paris, 15 November 2025

Table of Contents

Executive Summary

International law is entering a new epoch — the epoch of Smart Regulation, in which regulation ceases to be reactive and becomes preventive, adaptive, digital and multilayered.

The classical model of international law relied on:

• state sovereignty,

• conventions and treaties,

• slow mechanisms of ratification and enforcement.

However, between 2014–2025, this model was replaced by a new regulatory environment built on dynamic norm-creation, digital monitoring, hybrid legal–sanctions architecture, and algorithmic risk governance.

Smart Regulation does not replace international law — it becomes its digital regulatory superstructure, capable of:

• blocking transactions without a court order,

• halting international deals in seconds,

• automatically identifying high-risk actors,

• cutting access to financing without criminal proceedings,

• managing exports of dual-use technologies based on AI analytics,

• generating new norms faster than traditional legal reforms can occur.

Sanctions lists, AML frameworks, export-control regimes, due-diligence procedures, crypto-monitoring rules, ESG-GPU compliance and cross-border regulatory filters have become not merely legal tools — they have transformed into centres of normative power that can influence states, corporations and individuals far more effectively than classical mechanisms of international law.

This system creates a new type of global order in which the sources of norms include not only states but also:

• international regulators (OFAC, EU Sanctions Authority, BIS, FinCEN),

• FATF and OECD standards,

• digital platforms,

• financial networks and crypto-infrastructure,

• transnational corporations and banks,

• neural-network–based risk-assessment algorithms.

The ARGA Observatory report systematically describes the transformation of international law within the framework of Smart Regulation, analysing the new structure of the sanctions architecture, export-control regimes, digital monitoring of capital flows, crypto-operations and supply chains — and offering a forecast of how global regulation will evolve by 2030.

Special attention is given to:

• the evolution of international law from treaty-law to risk-law,

• the creation of multilayered digital normativity,

• new regimes of transnational control,

• the expanding role of private regulators and financial institutions,

• the shifting balance between law and algorithm.

Smart Regulation becomes the central framework for the future of global politics and economics. This report captures the moment of transition — and describes the architecture of a world in which norms are created faster than they can be ratified.

1. Methodology

The report is based on a multi-component research model that combines legal analysis, comparative law, sanctions analytics and the study of digital regulatory instruments. The methodological foundation includes:

• analysis of international and supranational legal norms (UN Charter, UNCAC, UN Sanctions Framework, OECD standards, EU acquis), along with specialised regulatory acts of the US, UK and EU governing sanctions, export control and financial compliance;

• study of sanctions documentation of the European Union, OFAC/US Treasury, HM Treasury UK, BIS, and licensed mechanisms for blocking/authorising export operations;

• monitoring of digital regulatory regimes — MiCA (Markets in Crypto-Assets), DORA (Digital Operational Resilience Act), NIS2 Directive, EU AI Act — with subsequent comparison of enforcement practices;

• analysis of cross-border law-enforcement operations conducted by Interpol, Europol, Eurojust, and FIUs (Financial Intelligence Units), including cases relating to crypto flows, export-control violations and sanctions evasion;

• comparative study of the legal systems of the EU, the United States, the United Kingdom and major Asian jurisdictions (UAE, China, Singapore, Hong Kong, South Korea) with a focus on Smart Regulation and digital law-enforcement;

• field research by ARGA Observatory, including case studies of sanctions architecture, digital criminology, AML/CFT regimes, due-diligence of cross-border supply chains and international financial investigations;

• expert interviews and closed professional consultations with sanctions lawyers, AML/CTF specialists, former regulators, crypto-analysts and key participants in the due-diligence and export-control industries.

The methodology is aimed at constructing an analytical model of Smart Regulation — a system in which law, sanctions policy, digital mechanisms and global markets form a single architecture of governance.

2. Introduction: A New Era of International Regulation

International law is entering a phase of profound transformation that many scholars already describe as a shift from the classical normative model to the Smart Regulation regime — a system in which legal decisions are formed not only through political agreements but also through digital analytics, sanctions-based mathematics, economic risk coefficients and algorithmic regulation.

While in the 20th century international law relied on treaties, judicial mechanisms and diplomatic processes, between 2014–2024 it began to operate as a dynamic digital–sanctions architecture, in which legal norms are no longer fixed once and for all but are updated in real time depending on:

- security threats,
- capital flows,
- financial transactions,
- export of critical technologies,
- and intelligence-derived data.

Modern international regulation is simultaneously:

— digital, because normativity is embedded in monitoring systems, data analytics and AI-driven compliance mechanisms;

— integrated, because sanctions, AML, cyber law, trade regulation and human rights now function as interconnected modules;

— sanctions-and-finance–driven, since access to capital, SWIFT, crypto exchanges, semiconductors and technologies has become a lever of geopolitical power;

— dynamic, because rules now change not over years but over weeks — under the pressure of emerging risks;

— risk-based, where the key legal criterion becomes not the fact of violation but the *probability of harm* associated with a state, an organisation or a technology.

Thus, global regulation is shifting from a model of postfactum punishment to a model of predictive governance, where enforcement is built on assessing probable threats, tracing transactions, analysing digital behavioural signals and using autonomous algorithms to control supply chains.

The ARGA Observatory report examines Smart Regulation as a new stage in the evolution of international law — not a replacement for existing norms, but an *overarching framework* that turns law into the infrastructure of global risk governance.

3. Architecture of Smart Regulation

The ARGA Observatory identifies five key modules that together constitute the new architecture of international regulation. Each module is not simply a set of norms but an independent power circuit, a risk-governance system tightly integrated with all others.

3.1. Sanctions Law as the Core of the New Normativity

Sanctions have ceased to be merely instruments of foreign policy — they have become the central legal module of the global regulatory system.

— Integration of sanctions into compliance

Sanctions lists, sectoral bans, service restrictions and technology controls are now embedded in the operational routines of:

- banks and fintech,
- transport and logistics companies,
- insurers,
- IT and telecommunications providers,
- energy and commodity traders.

For corporations, sanctions law has become a "supra-legal layer": even if an operation is technically legal in a national jurisdiction, sanctions risk forces companies to refuse deals, assets or partners.

— Secondary sanctions and extraterritoriality

Secondary sanctions make the entire system truly global.

Companies and states outside U.S., EU or UK jurisdiction still comply — because:

- loss of access to the dollar system,
- disconnection from SWIFT,
- or exclusion from the EU market

is a stronger incentive than national legislation.

This creates extraterritorial normativity, where geopolitical power is expressed through financial and technological dependencies.

— Monitoring third-country intermediaries

Smart Regulation focuses not only on sanctioned jurisdictions but on the intermediaries:

- UAE, Turkey, Kazakhstan, Kyrgyzstan, Armenia, Georgia,
- the Caucasus transit routes,
- Southeast Asian jurisdictions,
- the Balkans.

Legal instruments now include:

- *high-risk intermediary registers*,
- blacklists of logistics and re-export operators,
- enhanced due diligence for parallel import and re-routing chains.

— Sanctions as rapid amendments to international law

Sanctions increasingly function as fast-track international regulation.

Through sanctions regulations, states can:

- impose technology bans,
- block transactions,
- restrict services,
- freeze assets,

without waiting for multilateral treaties.

Corporations then internalise these restrictions, translating them into internal policies, banking compliance and court practice.

3.2. Export Control and the Rise of Dual-Use Regulation

The second module of Smart Regulation is export control — now a geoeconomic architecture, not a narrow security tool.

— Control of AI and cryptographic technologies

The classical model (missiles, nuclear materials, weapons) is being replaced by a wider framework that regulates:

- algorithms and AI models;
- encryption technologies;
- cyber-infrastructure;
- cloud computing and API access;
- knowledge transfer (“know-how export”).

Export control has become a gatekeeper of digital sovereignty.

— Semiconductor and electronics restrictions

Chips, CNC machines, telecom components and UAV electronics are now under:

- licensing regimes,
- capacity thresholds,
- precision limits,
- end-user bans.

Export control determines technological and military power balances, shaping entire industrial chains.

— Oversight of supply-chain networks

Instead of evaluating a single exporter, Smart Regulation evaluates the whole chain:

- manufacturing hubs,
- repackaging facilities,
- freight forwarders,
- insurance companies,
- financial intermediaries,
- warehouse operators.

The law now regulates the *network*, not the actor.

— Digital tracking tools

Export control integrates:

- serial-number databases,
- product tracing,
- blockchain-based supply-chain tools,
- customs-data algorithms.

Decision-making becomes data-driven: algorithms flag suspicious routes and match patterns across distributed datasets.

3.3. AML/CFT as the Universal Regulatory Language

Anti–money laundering (AML) and countering terrorist financing (CFT) have become the universal, politically neutral platform of Smart Regulation.

— AML as the global common denominator

Regardless of geopolitical tensions, AML rules allow regulators to:

- freeze accounts,
- block transactions,
- demand source-of-funds evidence,
- expose beneficial ownership.

AML is the baseline consensus enabling cross-border governance even between states that disagree politically.

— Risk-Based Approach (RBA)

The transition from rule-based to risk-based supervision makes banks quasi-regulators:

- they assess country, sector, client and transaction risk,

- they design their own internal risk models,
- liability shifts to corporate compliance decisions.

This effectively delegates large parts of international law enforcement to private actors.

— Travel Rule and global traceability

The Travel Rule (including its crypto extensions) ensures that:

- originator and beneficiary data
- accompany every transaction

  across banks, crypto exchanges and payment systems.

This merges sanctions control, AML and counter-terrorist finance into a single interconnected digital fabric.

— Integration of FIUs into a transnational intelligence network

Financial Intelligence Units (FIUs):

- exchange data,
- create unified risk profiles,
- initiate freezes and alerts,
- direct signals to regulators and banks.

The result is a transnational field of financial intelligence in which national borders lose operational significance.

3.4. Digital Regulation

The fourth module is digital regulation, led primarily by the European regulatory framework (AI Act, MiCA, DORA, NIS2). Together, these instruments establish the global standard for next-generation governance.

— AI Act

The regulation of artificial intelligence introduces the concept of system risk profiles:

legal obligations depend on the level of risk posed to human rights, safety and democratic processes.

Prohibited, high-risk and limited-risk AI systems are regulated differently, transforming international law into a matrix of technology-governance models rather than a static code of prohibitions.

— MiCA

The Markets in Crypto-Assets Regulation creates the first comprehensive legal regime for:

- stablecoins,
- crypto-asset service providers,
- exchanges.

MiCA integrates digital assets into the traditional financial regulatory perimeter, bringing them under sanctions compliance, AML supervision and prudential oversight.

— DORA

The Digital Operational Resilience Act defines cyber-resilience, incident management, ICT-provider oversight and stress testing as legal obligations, not optional technical standards.

Failure to comply triggers supervisory and sanctions consequences.

DORA effectively makes operational resilience a legal pillar of financial stability.

— NIS2

The updated Network and Information Security Directive expands the list of "essential" and "important" entities, turning cybersecurity into a mandatory component of corporate responsibility across critical and high-risk sectors.

— Transformation of corporate and financial law

Collectively, these acts ensure that core governance components — IT architecture, AI systems, data processing, cryptoassets — become objects of direct legal regulation, not merely internal corporate policy.

The law becomes embedded into software code, system architecture and business processes.

3.5. Transnational Legal Compliance

The fifth module is cross-border compliance and smart due diligence, which turn corporations and financial institutions into active carriers of international law.

— Smart due diligence

Counterparty checks increasingly rely on:

- algorithmic risk-analysis systems,
- OSINT/FININT tools,
- ESG metrics,
- human-rights risk indicators.

Due diligence has evolved from a legal audit into an assessment of alignment with global normativity — sanctions, human rights, sustainability and climate-risk standards.

— Beneficial ownership control

Requirements to disclose:

- ultimate beneficial owners,
- trust structures,
- SPVs and offshore entities,

mean that anonymous control of major assets is becoming increasingly impossible.

A transparent, end-to-end map of ownership is emerging, enabling regulators to track capital flows and monitor high-risk actors.

— ESG and human-rights monitoring

Smart Regulation now embeds Human Rights Due Diligence and assessments of risks linked to:

- forced labour,
- corruption,
- involvement in repression or conflict,
- environmental violations.

This transforms major corporations into conduits of international law: they must disengage from partners and projects that present elevated human-rights or governance risks.

— Influence on international courts

International judicial and quasi-judicial bodies (EU courts, ECtHR, arbitration panels, tribunals) increasingly rely on:

- sanctions lists and blacklists,
- export-control determinations,
- AML findings,
- digital-regulation standards.

This shifts the logic of adjudication: courts absorb, validate and institutionalize components of Smart Regulation, embedding them into the corpus of international law.

4. Geography of Smart Regulation

The global system of Smart Regulation is evolving unevenly: it has centres of norm-production, jurisdictions that amplify norms, exporters of regulatory standards, and regions that primarily absorb them.

In the 2020s, four macro-regions have emerged as the principal engines of normative power, each shaping its own model of digital-sanctions governance.

Together, they define the logic of cross-border law, international compliance and the redistribution of sovereignty.

4.1. European Union — the world's primary generator of normative power

Between 2023–2025, the EU became the central factory of Smart Regulation, producing regulatory models that then scale far beyond Europe.

- EU AI Act introduces a risk-based system for AI and effectively becomes the global matrix for algorithmic governance.
- MiCA establishes the first comprehensive legal framework for crypto-assets, stablecoins and service providers.
- NIS2 and DORA create mandatory regimes for cybersecurity and digital operational resilience across banks, fintech, telecoms and critical infrastructure.
- ESG/HRDD standards turn human-rights protection into a legally measurable element of global supply chains and investment flows.

The EU functions as a law exporter: corporations in Latin America, Africa, the Middle East and Asia adapt operations not for market access, but to comply with European requirements.

This makes the Union the core of the global normative ecosystem.

4.2. United States — the world's sanctions and financial enforcement platform

If the EU *produces* norms, the United States provides the coercive infrastructure that enforces them: sanctions, the dollar system, global banking.

- OFAC defines the backbone of the global sanctions architecture, including secondary sanctions that compel obedience far outside US jurisdiction.
- FinCEN sets AML/CFT standards, implements the Travel Rule, and provides intelligence on digital transactions.
- Export-control authorities (CHIPS Act, BIS) determine global access to advanced semiconductors, AI technologies and cryptography.
- FCPA case law turns the US into the hub of criminal-financial enforcement against multinationals.

The American model relies on the US dollar as an instrument of law: access to the dollar infrastructure equals legal compliance; losing that access functions as a de facto international sanction.

4.3. United Kingdom — the centre of global due diligence and sanctions innovation

After Brexit, the UK created a hybrid model of Smart Regulation, combining regulatory flexibility with strong sanctions tools.

- UK Sanctions Act allows rapid asset freezes, swift list expansion and autonomous action from the EU and US.
- The UK is a global leader in corporate due diligence: London sets standards for verifying beneficial owners, SPVs and trusts.
- English law has become a key mechanism for resolving cross-border disputes, including sanctions litigation.

The UK plays the role of a bridge jurisdiction, linking American sanctions power with European regulatory density.

London's courts transform Smart Regulation into enforceable law, rather than a declaratory framework.

4.4. Asia (Singapore, South Korea, Japan) — the technological axis of Smart Regulation

Asian economies constitute a parallel centre of normative development, where Smart Regulation grows around technological security and export-control governance.

- Singapore is a model of risk-based AML regulation, crypto-oversight and advanced fintech compliance.
- South Korea develops high-precision control over semiconductors, telecom technology and military electronics.
- Japan combines stringent export standards with a more moderate sanctions regime, forming a hybrid normative model.

Asia is a key node of Smart Regulation in the field of dual-use technology and digital security.

It acts as a parallel standard-setting centre, competing with the EU and the US in shaping the regulatory logic for artificial intelligence and the crypto-economy.

5. Case Studies

Smart Regulation manifests itself not in declarations but in the way sanctions, export control, AML, digital regulation and legal mechanisms operate simultaneously, forming a new integrated architecture of coercion.

Below are three model cases illustrating this transformation.

Case 1 — Sanctions + Export Control + AML → A Single Integrated Pressure System

Scenario:

A European company *A* supplies industrial equipment and microchips to Asia, where the final buyer is a trader linked to parallel import into a sanctioned jurisdiction.

USDT-settlements, offshore warehouse hubs and nominal intermediaries are used to obscure the route.

How Smart Regulation responds:

1. Export control flags the dual-use status of microprocessors

   (BIS + EU Dual-Use Regulation).

2. AML/FinCEN detect a suspicious transaction route — a crypto off-ramp tied to a high-risk jurisdiction.
3. Sanctions lists (OFAC + EU Restrictive Measures) identify a high-risk end-user → shipment blocked.
4. Financial institutions freeze payments under enhanced due diligence.
5. Interpol + FIUs receive requests to review the chain.

Outcome:

The company loses access to foreign markets, assets are frozen, contracts terminated.

One case activates three regulatory verticals at once — sanctions, export control, AML — functioning as a single logic of Smart Regulation.

Case 2 — Algorithmic Surveillance and Digital Control Infrastructure

Scenario:

A global electronics manufacturer deploys AI-driven supply-chain monitoring using customs databases and platform APIs.

The algorithm automatically detects:

- anomalous transit routes (UAE → Caucasus → EAEU),
- sudden fluctuations in shipment volumes,
- discrepancies between purchase price and export declaration,
- USDT-linked off-bank payments.

How Smart Regulation works:

1. AI Act sets the framework for autonomous risk-scoring algorithms.
2. MiCA + AML Travel Rule create the legal basis for monitoring crypto operations.
3. DORA + NIS2 require continuous oversight of supply chains as critical infrastructure.
4. Data is transmitted to FIUs and Europol → a cross-border compliance review is triggered.

Outcome:

The platform creates self-executing compliance: sanctions enforcement occurs inside the code, without direct state intervention.

This is Smart Regulation — *law operating as algorithm*.

Case 3 — Extraterritorial Pressure and Sanctioned Projection of Sovereignty

Scenario:

A group of European banks services imports from Central Asia.

The goods are not under sanctions, but the ultimate beneficiary is linked to a Russian energy holding.

How Smart Regulation acts extraterritorially:

1. OFAC secondary sanctions → EU banks block transactions to avoid losing access to dollar clearing.
2. Financial regulators demand enhanced due diligence + proof of no sanctioned beneficiary involvement.
3. Deals are paused, counterparties' assets frozen.
4. The company switches payments to crypto → it lands on AML watchlists.
5. FIUs + Europol compile a dossier → the company receives a "high-exposure" risk profile.

Outcome:

Even without a formal legal prohibition, the company is effectively excluded from the market.

Smart Regulation functions as a mechanism of economic selection.

6. Global Consequences

The emergence of a new regulatory architecture is not merely transforming control instruments — it is reshaping the very *principle* by which international law operates.

Sanctions, financial compliance, export-control regimes and digital due diligence turn law from a static rule into a dynamic, real-time system.

Below are the key structural effects.

1. Convergence of International and Corporate Law

In the 20th century, international law existed separately from corporate regulation.

Today, the boundaries have collapsed.

Transnational corporations, banks, stock exchanges, fintech operators and even technology platforms have acquired de facto regulatory subjecthood: they must apply sanctions law, export control, AML, KYC, the Travel Rule, ESG obligations and algorithmic risk models.

- Law is no longer enforced *only* by states — it is executed by algorithms, payment systems, private banks and tech corporations.
- International regulation becomes distributed, no longer dependent on the political will of individual states.

This marks a shift from a state-centred international law → to a multi-node corporate-normative system.

2. Decline of Classical International Law

The traditional mechanism — treaty → ratification → enforcement — is being replaced by:

sanctions → financial blocking → instantaneous applicability.

- An OFAC or EU decision acts faster and more forcefully than a UN resolution.
- Consensus-based international law loses out to law embedded in transactional systems.
- Delegating enforcement to private actors reduces the time between norm and outcome from years → to hours.

Smart Regulation thus produces self-executing law.

3. Emergence of a Global System of Digital Monitoring

Control shifts from legislation to data infrastructure.

- FIUs monitor transactions in real time.
- AI tracks shipments via customs databases, IoT logistics and blockchain.
- Crypto-flows are analysed through on-chain tools.
- Ownership chains are mapped via corporate registries.

Global monitoring now follows the principle:

“risk = regulatory action,”

not “violation → reaction.”

The system acts preventively — blocking deals, accounts and exports *before* any formal violation occurs.

4. Consolidation of Sanctions as a Universal Instrument of Power

Sanctions become the political-economic equivalent of military force:

- they restrict access to technology and finance,
- reshape corporate strategies,
- reallocate capital and trade routes,
- trigger restructuring of logistics and digital payments.

Smart Regulation makes sanctions automatic and scalable:

Banks and fintechs apply them without external commands, relying on risk-scores, AI filtering and cross-referenced OFAC–EU–FinCEN–FIU datasets.

5. Increased Legal Complexity and a Higher Compliance Threshold

Corporations no longer operate within a single national system.

Any cross-border transaction must simultaneously pass through:

- a sanctions filter,
- export-control checks,
- AML/KYC procedures,
- crypto and digital monitoring,
- ESG/Human-Rights-Due-Diligence.

The number of regulatory layers grows, and compliance errors now equal criminal risk.

International law enters a phase of high-friction regulation — characterised by high legal complexity, high enforcement speed and high cost of non-compliance.

7. Forecast 2025–2030

1. Emergence of a Global Digital Regulator

Between 2025 and 2030, we can expect the gradual formation of a *de facto* global digital regulator — not as a single organisation, but as a connected ecosystem of platforms: sanctions registries (OFAC, EU listings, UK HMT), global AML systems, export-control databases, KYC/EDD providers, payment networks and crypto-analytic infrastructures.

The integration of sanctions data, suspicious transactions, supply chains, beneficial ownership structures and digital assets will mean that any significant economic action — from opening a bank account to completing an M&A — will pass through a unified, multi-layered risk-screening system.

In practice, this will produce a *"virtual supranational regulator"*, one that does not require a political mandate because its decisions are executed automatically through transaction refusals, access blocks, or compliance filters embedded in infrastructure.

2. Global Blacklists of Intermediaries

Given the growth of evasion schemes, parallel imports, sanctions middlemen and grey logistics hubs, by 2030 we are likely to see consolidated global lists not only of sanctioned persons and companies, but of:

- brokers,
- logistics operators,
- fintech intermediaries,
- crypto and OTC platforms

that systematically participate in sanctions evasion, export-control violations or AML breaches.

Such registries will be used by banks, insurers, logistics giants and BigTech as a standard part of due diligence.

Inclusion in a "registry of high-risk intermediaries" will effectively mean regulatory death: loss of access to banking, insurance, licences, trading platforms and international markets.

3. Integration of AI into International Law

Between 2025 and 2030, AI will cease to be a supporting compliance tool and will become a structural element of law enforcement.

AI systems will:

- analyse supply chains and transactions,
- model sanctions and export-control risks,

- detect evasion patterns, crypto-mixing, nested structures and trade-based money laundering,
- generate regulatory signals that banks and regulators treat as actionable.

This will create algorithmic due diligence and partly algorithmic enforcement, where the reason for denying a deal or blocking a transaction is not a court decision, but an AI-generated risk assessment.

This will trigger an entirely new legal debate:

the legitimacy of automated decisions, transparency of models, appealability, and the compatibility of AI "black boxes" with due-process and human-rights standards.

4. Stricter Requirements for Companies and Individuals

Corporations will be forced to build multi-layered compliance systems: sanctions law, export control, AML/CFT, ESG, digital compliance and AI governance.

We can expect:

- stronger personal liability for directors and beneficial owners,
- broader disclosure requirements for ownership, wealth sources and links to high-risk jurisdictions,
- transformation of the individual financial profile (HNWIs, PEPs, crypto holders) into an object of continuous monitoring.

For individuals — especially those linked to high-risk states, sectors or digital assets — this will mean reduced anonymity and higher barriers to global financial and investment services.

For companies — the need to embed legal and compliance capacities into strategic decision-making, not just operational processes.

5. Unification of Human Rights Mechanisms

As Smart Regulation expands, a parallel counter-movement for rights protection will inevitably grow. By 2030 we can expect:

- closer coordination between the ECtHR, EU courts, UN bodies and regional mechanisms (OAS, AU, CoE) in cases involving sanctions, extradition, digital restrictions and asset freezes,
- development of human rights due diligence standards for regulators and international bodies, not only for corporations,
- emergence of case law challenging algorithmic and sanctions-financial actions as violations of fair trial, privacy or non-discrimination.

In the long term, this will form a new *"digital-sanctions branch" of international human-rights law*, where the protected interests include not only classical freedoms, but also:

- the right to access financial infrastructure absent proven violations,
- the right to review automated regulatory decisions,
- protection from arbitrary use of sanctions, AML and export control as tools of political or corporate coercion.

8. Recommendations of ARGA Observatory

To International Institutions

International organisations (UN, Council of Europe, OECD, World Bank, FATF and relevant regional structures) must move from fragmented regulation to developing *coherent, harmonised standards* of Smart Regulation. This concerns not only sanctions, AML and export control, but also digital security, data governance, accountability for algorithmic decisions and legal safeguards for individuals affected by these mechanisms.

A key priority is the creation of framework principles establishing minimum standards of transparency, justification and verifiability for regulatory actions in the digital environment — including sanctions listings, asset freezes, automated risk analysis and cross-border data exchange.

Equally necessary is the development of interoperable digital platforms with clearly defined rules for access, data validation and the correction of erroneous records. This involves establishing technical and legal standards for linking sanctions registries, export-control systems, AML platforms, beneficial ownership databases and crypto-analytic tools. Such integration will reduce duplication, contradictions and arbitrary interpretation of information across jurisdictions.

Finally, international institutions should initiate the creation of global Smart Regulation Risk Indices — composite indicators reflecting the level of sanctions, export control, AML and digital vulnerabilities in each jurisdiction. These indices must assess not only the existence of rules, but also enforcement practice, abuse levels, politicalisation of regulatory decisions and the effectiveness of appeal mechanisms. This will give financial markets, corporations and human-rights bodies a more objective and comparable picture of regulatory risks.

To Regulators in the EU, the US and Asia

Regulators in the key economic centres — especially the EU, the United States, the United Kingdom, Singapore, Japan and South Korea — must work towards a *coordinated, interoperable* system of digital control, based on mutual recognition of standards and minimum regulatory benchmarks.

This requires a gradual convergence of approaches to:

- sanctions and restrictive measures,
- export control and dual-use regulation,
- AML/CFT regimes,
- crypto-asset regulation,
- AI governance,
- cybersecurity requirements.

The goal is to minimise regulatory arbitrage and close “compliance loopholes” exploited via third countries.

A crucial element will be the development of sanctions–digital analytics: specialised systems capable of detecting in near-real time the connections between sanctioned actors, supply chains, financial transactions, digital assets and high-risk intermediaries. Regulators should not simply publish sanctions lists — they must cultivate analytic infrastructures that allow banks, corporations and supervisory bodies to assess aggregated risk using multi-layered digital data.

Due diligence must be tightened qualitatively, not only quantitatively. This means transitioning from formal "tick-box" compliance to genuine risk-based assessment, where:

- analysis covers not only country and sector, but also involvement in evasion schemes, use of crypto-tools, participation in supply chains and digital infrastructure;
- enhanced transparency of beneficial ownership and sources of funds is required for high-risk actors;
- special protocols are adopted for verifying requests from jurisdictions with high levels of politicalised prosecutions, sanctions abuse and Interpol misuse.

At the same time, regulators must strengthen safeguards against overreach by establishing procedures for appeal, protection of good-faith actors and preventing discrimination on national or political grounds under the guise of risk management.

To Academia and Research Centres

Universities, think tanks and specialised research institutes must systematically develop Smart Regulation as an independent interdisciplinary field, integrating international law, economics, political science, digital security, criminology, data science and AI ethics.

Key tasks include:

- designing academic programmes, analytical methods and research projects that reflect the complex nature of new regulatory instruments and their effects on states, businesses and individuals;
- building robust databases of sanctions and export-control cases, examples of Interpol/AML/sanctions abuse, decisions of national and international courts, and regulatory practices in the digital and crypto-economy;
- ensuring that such datasets are suitable both for legal analysis and for machine learning or quantitative studies, enabling researchers to test hypotheses on the relationship between Smart Regulation, human rights, market stability and politicalisation of enforcement.

Finally, academia must actively develop interdisciplinary empirical research, combining legal analysis with digital and economic data. This includes:

- modelling regulatory scenarios and their impact on international trade and human rights;
- assessing how algorithmic systems affect access to justice and finance;
- conducting comparative studies across regions to understand divergent approaches to Smart Regulation.

Such research will equip international institutions and regulators with an evidence base for reforms and serve as a counterbalance to potential over-securitisation or politicalisation within the emerging global normative system.

9. Conclusion

The transition to Smart Regulation is not merely an update of international law — it is a paradigm shift in which law ceases to function as a reactive mechanism and becomes an active instrument

of global governance. International normativity is becoming faster, more technological, multilayered, and based not on declarations and precedents of the past but on data, algorithms, sanctions filters, export-control matrices and real-time risk governance.

This transformation blurs the boundaries between public international law, private regulation, corporate responsibility, digital security and financial control. Sanctions are no longer exclusively a political tool — they have become the architectural framework around which the regulation of trade, cryptocurrencies, export technologies, supply chains and transnational transactions is built. Export control, AML/CFT, MiCA, the AI Act, DORA and NIS2 function as interconnected modules of a unified system, producing new obligations for states, corporations and individuals.

As a result, Smart Regulation forms an entirely new legal reality:

• States lose the monopoly on norm-creation — regulatory actors now include supranational bodies, private platforms, financial regulators and even transaction-analysis algorithms;

• The rule of law acquires a digital nature — digital traces, automated monitoring and data analytics become not simply evidence, but structural elements of the legal system itself;

• Sanctions, supply-chain control and crypto-regulation become the core of international security, where compliance is demonstrated not through diplomacy but through the technical ability to execute a transaction;

• Human rights protection must evolve in parallel with regulatory mechanisms, otherwise the digital jurisdiction will overpower the humanitarian one.

Thus, the new era of Smart Regulation is a space in which international law becomes, for the first time in history, a cyber-financial architecture. Not a text but a code. Not a mere constraint but an operating system for global governance.

The ARGA Observatory report lays the theoretical and analytical foundation for further study of this system, identifying the key nodes of transformation, the risks for human rights and the international economy, and the directions for future reforms. In this new world, the winners will be the states and institutions capable of thinking in data, regulating infrastructures rather than isolated events, and constructing law that operates at the speed of the digital age.

Sources

1. EU Sanctions Map, https://sanctionsmap.eu/#/main.
2. European Commission, Overview of sanctions and related resources, https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en.
3. EUR-Lex, Dual-use export controls, https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html.
4. BIS, Export Administration Regulations, https://www.bis.gov/regulations/ear.
5. Wassenaar Arrangement, Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 1996, https://www.wto.org/english/res_e/booksp_e/int_exp_regs_part3_5_e.pdf.

6. OECD, Regulatory Policy and Governance, 25 October 2011, https://www.oecd.org/en/publications/regulatory-policy-and-governance_9789264116573-en.html.
7. Edmont Group, Principles for information exchange between financial intelligence units, July 2025, https://egmontgroup.org/wp-content/uploads/2022/07/EG-Principles-for-Information-Exchange-Revised-July-2025.pdf.
8. Atlantic Council, John Forrer, Economic Sanctions, June 2017, https://www.atlanticcouncil.org/wp-content/uploads/2017/06/Economic_Sanctions_web_0614.pdf.
9. OECD, Due Diligance Guidance for Respobsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, Third Edition, 6 April 2016, https://www.oecd.org/en/publications/oecd-due-diligence-guidance-for-responsible-supply-chains-of-minerals-from-conflict-affected-and-high-risk-areas_9789264252479-en.html.
10. Henry Farrell, Abraham L. Newman, Weaponized Interdependence : How Global Economic Networks Shape State Coercion, 01 July 2019, https://direct.mit.edu/isec/article/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic.