How the Brussels Effect Hinders Innovation in the Global South

By Ayesha Bhatti | January 26, 2026

The European Union prides itself on its ability to set global policy through regulatory action, a phenomenon known as the Brussels Effect. The Brussels Effect has shaped regulation across sectors including food, chemicals, and technology, often by imposing rules that other countries feel compelled to adopt in order to access EU markets. In the technology sector, prominent examples include the General Data Protection Regulation (GDPR), as well as more recent digital laws such as the Digital Services Act (DSA) and the Digital Markets Act (DMA). Although European policymakers often celebrate regulatory export as a diplomatic success, the mandatory adoption of EU-style digital rules amounts to regulatory imperialism for many Global South countries, limiting technology adoption, raising compliance costs, and undermining the ability of local firms to compete with Western ones. Rather than submit to the EU, Global South countries should adopt flexible rules that reflect their own local interests and goals.

Europeans frequently celebrate the EU's reputation as a global rule maker as a diplomatic triumph. Through the Brussels Effect, the EU exports its regulations beyond its borders by setting rules that foreign governments and companies feel compelled to follow. Digital regulation provides the clearest example of this dynamic, as the GDPR and newer laws such as the DSA, the DMA, and increasingly the Artificial Intelligence Act (AIA) have become global reference points.

This regulatory power carries significant costs for countries with different economic and technological realities. EU-style digital rules impose high compliance burdens, limit experimentation, and restrict data use in ways that harm innovation. For Global South countries, mirroring EU rules raises barriers to widespread technology adoption, constrains domestic firms, and entrenches the dominance of Western competitors in global markets.

Rather than harmonise with EU rules, Global South countries should assert regulatory autonomy and pursue digital governance frameworks that remain flexible, innovation-friendly, and tailored to local needs. As countries consider AI governance strategies, policymakers should avoid mimicking EU legislation and instead pursue the following priorities:

- Reject wholesale adoption of EU-style AI and data rules.
- Build flexible, interoperable, and regionally grounded AI governance models that promote innovation and economic complementarity.
- Strengthen regional cooperation to shape AI rules collectively.

THE BRUSSELS EFFECT IS AN EXERCISE IN REGULATORY IMPERIALISM

While often portrayed as an example of Europe's soft power, the Brussels Effect is better understood as a form of coercion. The global uptake of EU digital rules is frequently driven by economic pressure and legal asymmetry. Through such mechanisms as extraterritorial enforcement and trade dependencies, the EU compels third countries to adopt regulatory frameworks that reflect European priorities rather than local ones. This dynamic reflects a deeper pattern of "regulatory imperialism", wherein the EU leverages its market power and global influence to impose its rules beyond its borders, with little regard for the consequences on innovation, sovereignty, or inclusive digital governance.

The EU has indeed influenced the adoption of global policies, norms, and standards, positioning itself as the world's regulatory pacesetter across a range of policy areas. From genetically modified organisms (GMOs) to data protection and chemicals regulation, the EU has leveraged its market power and legal frameworks to export its rules globally, often compelling other countries to adopt its rules without meaningful input or dialogue.

In 2000 for example, the EU played a leading role in internationalising its GMO policy via the Cartagena Protocol on Biosafety, introducing a global framework modelled on European preferences that restricted GMO trade.[1] In data protection, the EU encouraged the adoption of the Council of Europe's Convention 108 as a steppingstone to GDPR-style rules for countries looking to access the European market.[2] By the time the EU enacted the GDPR in 2018, commentators were already confirming its global influence, citing how countries from Colombia to South Korea to Bermuda were "falling in line with Europe".[3] Indeed, one study found

strong signs of the Europeanisation of data privacy standards across non-European nations, as governments scrambled to ensure continued market access and political favour.[4]

Whilst some proponents of this approach argue that the EU is demonstrating principled leadership, others rightly criticize the EU for imposing its rules onto another jurisdiction through coercive means such as market access conditions or extraterritorial legal frameworks, resulting in widespread rule adoption without democratic participation by those impacted or regard for local contexts.[5]

EU policymakers celebrate this effect as the voluntary adoption of EU values. From its founding treaties to its foreign policy strategy, the EU identifies itself as a normative power, promoting a rules-based global order grounded in democratic principles and human rights.[6] When the GDPR came into effect, then-Commissioner for Justice Věra Jourová openly declared, "We want to set the global standard [for privacy]."[7] The European Parliament echoed that ambition two years later. It welcomed the fact that "a number of third countries have aligned their data protection laws with the GDPR", and proudly claimed that the law had placed the EU at the forefront of international data governance.[8]

The former president of the European Council—an institution referred to as "the law-maker-in-chief" that defines the political direction and general priorities of the EU—said in a speech at the Munich Security Conference in 2022:

> Our standards, inspired by our European values, tend to become global standards. And this is true in many sectors. For instance, in the chemicals sector, our standards have become global standards. In the digital field, the [GDPR] had a similar effect, and we are working on our [DSA] and [DMA].[9]

President Charles Michel presents the global spread of EU rules as evidence that other countries agree with the values on which EU policymakers have based those rules as well as the rules themselves. Yet, this framing obscures the power dynamics that often drive other countries to copy EU regulations. President Michel contradicted his own values-based view, openly acknowledging earlier in the same speech that the EU "is a much more powerful global actor than we think. Our strength is anchored in our prosperity, our economic power, and our capacity to use it in order to influence the world".

In other words, the EU influences non-EU countries through structural economic and political leverage, pressuring governments to align with EU market rules or risk losing access. This dynamic makes global adoption of EU standards less about voluntary alignment around shared values and more about power-based coercion. The irony deepens given the EU's self-professed role as a defender of global free trade.

Far from fostering sustainable consensus, the EU export rules that impose high compliance costs on countries that have no voice in shaping them. There is limited, if any, consideration in the EU policymaking process of the downstream effects of EU law on non-EU jurisdictions, despite the fact EU lawmakers understand their extraterritorial impact—a gap that raises questions about the democratic legitimacy of what is, in practice, a form of unilateral international rulemaking.

The consequences of this model have been felt not only in the Global South, where innovation ecosystems struggle under the weight of rigid compliance requirements, but globally, where critics rightly view the EU's digital rules, such as GDPR, as de facto digital trade barriers designed to disadvantage non-EU firms.[10] Given Europe's history of illegal trade practices to promote European-owned businesses in non-tech-related fields, such as the illegal subsidies it paid Airbus to force a European competitor to U.S. rival Boeing, it is unsurprising such an approach now bleeds into digital rules when states increasingly use technological capacity to assert economic power.[11]

The primary vehicles of this power are extraterritorial provisions in its laws and trade policy. The GDPR contains such provisions, ensuring that the law applies to any organization that processes the data of EU citizens, regardless of where the organization is based.[12]

The GDPR's adequacy requirements are another tool for the EU to assert its rules abroad. Under the GDPR, the European Commission has the authority to determine whether a country outside the EU offers an adequate level of data protection. For the EU to reach a decision, the Commission must deem a third country's regulatory framework "essentially equivalent" to those in the EU and, by extension, the GDPR. Without an adequacy decision, the EU limits personal data to flow freely between the EU and a third country, restricting digital trade.

Adequacy decisions therefore become gateways to freely access the EU market, but that decision rests exclusively with the European Commission, the body empowered to determine whether a non-EU country offers an adequate level of data protection. The EU's adequacy regime compels non-EU countries to adapt their frameworks to ones only the Commission can recognise as equivalent. The Commission itself noted in *Schrems II*—a European Court of Justice case that invalidated the EU-U.S. Privacy Shield framework that supported personal data transfers with the United States—that the countries with adequacy decisions have updated data protection legislation to converge with the EU's own.[13]

However, adjusting data protection rules to increase the chances of an adequacy decision may not benefit the local development needs of a third country. For example, despite Japan's preexisting data protection law, an adequacy decision between Japan and the EU was contingent on Japan's adoption of the Supplementary Rules provided for in the decision itself in

order to afford "a higher level of protection of an individual's rights and interests regarding the handling of personal data received from the EU".[14] Similarly, the United Kingdom's adequacy decision is the only one subject to a sunset clause, reflecting a lower level of trust from the EU despite the EU being the country's largest trading partner, and the United Kingdom being the EU's third largest trading partner.[15] This clause gives the European Commission greater flexibility to withdraw or decline to renew the decision in the future, depending on how the United Kingdom's data policies evolve and, in particular, whether they diverge from EU preferences.[16]

Of the 16 adequacy decisions currently in operation, the European Commission has only granted adequacy to two Global South countries: Argentina and Uruguay.[17] There is no such agreement for any country in sub-Saharan Africa, and only three in Asia and the Middle East for which none would constitute a Global South country. India, for example, does not hold an adequacy decision, despite its extensive trade relationship with the EU and a parliamentary recommendation in 2021 for the EU to consider such a decision.[18]

As discussed ahead, the ability to leverage data is a key economic lever for Global South countries. Improved cross-border data flows between businesses encourage them to adopt data-driven models, spurring broader digital transformation and driving productivity gains across the economy. Indeed, one study found a clear link between EU adequacy decisions and enhanced digital trade.[19] Countries that obtained EU adequacy on data protection exhibited an increase in digital trade of up to 14 percent, representing a trade cost reduction of up to 9 percent and more digital trade between other countries that were similarly granted EU adequacy. Restricting data flows, such as the EU withholding an adequacy decision, denies Global South countries access to the substantial economic benefits of the "club effect" of digital trade between countries with adequacy decisions.

Restricting data flows reinforces the disadvantaged position of Global South countries. The promise of EU adequacy pressures Global South countries in comparatively weaker negotiating positions to adopt EU-specific data protection rules in order to secure necessary cross-border data flows rather than developing frameworks to suit their own needs. Most Global South countries struggle to meet EU adequacy requirements due to limited regulatory capacity, insufficient technical expertise, competing development priorities, and institutional constraints, effectively excluding them from seamless participation in the EU-centred digital economy. This exclusion creates a self-reinforcing cycle wherein "adequate" countries become increasingly attractive digital partners, while Global South countries face structural barriers to accessing advanced digital technologies, foreign investment, and global digital value chains. The system forces developing countries to spend resources on adopting

European-style data protection frameworks as a prerequisite for full participation in the global digital economy without actually benefiting from that full participation.

Indeed, India, Kenya, Brazil, and South Africa have all adopted GDPR-style rules, but have yet to receive an adequacy ruling from the EU.[20] Worse still, the EU actively supported Kenya's Data Protection Bill and later held it up as a model of GDPR-inspired reform.[21] The EU's influence here is a one-way street: it urges others to adopt its rules, whilst reserving adequacy as a political tool for major trading partners. That undermines the EU's claim to build a values-based digital order, reducing adequacy to a selective instrument of leverage rather than a genuine mechanism for enabling digital trade based on those shared rules.

The DMA and DSA operate in similar ways to the GDPR in that both require compliance wherein users or recipients of a platform or service are in the EU, regardless of whether the company offering the platform or service is itself established within the EU.[22] Moreover, DMA designations currently apply almost exclusively to non-EU firms, and the first designation of Very Large Online Platforms (VLOPs)—the designation that determines obligations under the DSA—involved only 2 EU firms out of 17 total firms.[23] The EU tends to enact digital economy rules that disproportionately impact firms beyond its borders, reliant on its economic pull to strong-arm conformity and with little pressure to enact balanced rules that rarely affect EU firms.

Trade relations deepen this economic power imbalance, particularly in the Global South where several countries depend on EU trade and investment to support their digital infrastructure. This dependence in turn creates structural pressure to adopt EU-style rules. Indeed, President Michel stated that the EU is "a global trading power and a partner everyone wants to trade with. Our trade deals strengthen our economic base and are underpinned by our fundamental values".[24] This rhetoric hints at the use of trade to spread the adoption of European values.

The EU has strong links to Africa's digital development. For example, the EU makes up 40 percent of South Africa's e-commerce trade.[25] The EU also maintains its Global Gateway Strategy with Kenya, a digital economy package to boost Kenyan connectivity, skills, and inclusive governance across Kenya's green and digital transition.[26] The EU is an active investor in Latin America's digital transformation. In 2021, it finished the Building the Europe Link to Latin America (BELLA) programme for the long-term interconnectivity of European and Latin American research and education communities with a new 6,000 km submarine cable.[27] A recent EU-Brazil Bilateral Digital Dialogue reaffirmed both the EU's and Brazil's commitment to promoting meaningful digital development whilst upholding democratic principles and human rights and reaffirming legal frameworks.[28] Finally, the EU and India recently held a second Trade and Technology Council meeting. The goal of the meeting was to deepen the strategic partnership

on trade and technology which, as of 2023, amounted to €20 billion in digital services.[29]

Each of these regions has adopted GDPR-style rules, with a clear trend emerging towards the wider adoption of EU digital regulations. This emulation is, in part, likely driven by the continued investment and trade between these regions and the EU.

The Brussels Effect cannot be seen as a benign export of European values. Rather, it operates as a form of regulatory imperialism—leveraging market access, power asymmetries, and digital trade dependencies. Whilst subtler than the military power of Europe's colonial past, this approach is no less consequential. The EU imposes its regulatory vision on countries with vastly different economic conditions, political systems, and innovation goals, in turn hindering the ability of Global South countries to leverage innovation for their own benefit and prosperity.

ADOPTION OF GDPR-LIKE RULES HAVE BROUGHT HIGH COSTS TO INNOVATION IN THE GLOBAL SOUTH

The EU's strict take-it-or-leave-it approach has compelled several countries in the Global South to introduce a GDPR-style framework, to their detriment. The GDPR's provisions, including strict purpose specification requirements, data localisation, a centralised enforcement body, and extraterritoriality have hindered the innovation ecosystems of third countries by undermining their data-driven economies, stressing limited state resources and a lack of institutional capacity and directing firm resources from innovation activities to compliance. As a result, third country alignment to global data protection frameworks rooted in European norms, values, and institutions has held them back from reaping the benefits of a data-driven economy.

Undermined Data-Driven Economies

Perhaps the biggest cost to innovation of the GDPR is its restriction on the ability of countries to leverage data for their benefit through cross-border data flows.

In a thriving digital economy, cross-border data flows enable digitalisation, which in turn leads to greater trade openness, the sale of more products in more markets, and increases in trade in services.[30] Yet, in 2019—one year on from the GDPR's introduction—the Organisation for Economic Cooperation and Development (OECD) also found that across several countries, the main challenges to cross-border data flows included uncertainty and interoperability of legal privacy regimes, and also data localisation trends.[31]

The GDPR strongly favours data localisation. Worse still, the spread of data localisation to more countries—such as through the growing adoption of

GDPR-style frameworks—poses a threat to an open, rules-based, and innovative global economy. In fact, by early 2023, nearly 100 data localisation measures were in place across 40 countries.[32] Such requirements under the GDPR significantly restrict the economic gains that come from free-flowing, cross-border data flows, measurably reducing trade, slowing productivity, increasing prices for affected industries, and undermining shared regional governance.

One study found this to be the case across China, Indonesia, Russia, and South Africa, all countries with increasing data restrictiveness tracing as far back as 2013.[33] According to the study, between 2013 and 2018, South Africa's volume of gross output fell by 9.1 percent, productivity fell by 3.7 percent, and prices rose by 1.9 percent due to increased restrictions on data flows. For that same period, Indonesia saw a reduction of volume of gross output by 7.8 percent, lowered productivity by 3.2 percent, and raised prices by 1.6 percent. Both Indonesia and South Africa have long considered data localisation measures as part of these restrictions, notably enacting data protection rules closely aligned to the EU's GDPR on such measures when the EU passed the GDPR.

Before the GDPR, Kenya boasted a relaxed regulatory approach which led to the emergence of nearly 3,500 tech-related ventures in sub-Saharan Africa alone, and an increase in venture capital financing with over $1 billion invested into technology start-up companies from 2012 to 2018.[34] Kenya also had an open government data platform which allowed companies to access crucial data at no cost and to leverage that data to build their own businesses.[35]

After the GDPR, Kenya could no longer market itself as a competitive, data-driven ecosystem, instead adopting its data protection authority (DPA) in 2019.[36] Kenya's DPA heavily borrowed from the EU's GDPR despite alternative rules already in existence within the African continent, including the African Union's Convention on Cyber Security and Personal Data Protection ("the Malabo Convention").[37] As a result, it features some of the GDPR's problematic provisions that hinder innovation, including data localisation, that restrict Kenya's ability to benefit from cross-border data flows. Regrettably, Kenya has also taken its open data initiative offline for the last few years despite efforts for its revival. Reasons for this include a lack of legal framework, likely compounded by the interaction of Kenya's DPA, a lack of clarity around institutional accountability, and a lack of resources.[38]

Limited Resources and Institutional Capacity

Adopting a GDPR-style framework demands domestic resources that developing countries often cannot meet.

The GDPR's data localisation requirements exacerbate already limited resources that could be better applied elsewhere. In particular, data

localisation brings a need for more domestic data centres. The cost includes not only the data centres themselves but also accompanying electricity and skilled labour needs that developing countries, at least within the public sector, currently cannot meet.

In Malaysia for example, the local government rejected almost 30 percent of data centre applications in the last five months of 2024 due to concerns over their strain on local water and electricity supplies.[39] Moreover, the state is struggling to compete in attracting a talent pool to accompany data centres because of a poor monetary conversion rate with the Singaporean dollar, as Singapore is a leading hub for data centres in Southeast Asia.[40]

Across Africa, the issue isn't that data centres are harmful—they are essential for digital growth—but that countries can only support a limited number of them. When regulations require domestic processing, the scarce data-centre capacity that exists is diverted to meet regulatory mandates rather than serve the commercial and innovation needs of local firms. [41] A similar dynamic plays out in Brazil, where millions already face energy shortages and blackouts. [42] Strict localisation rules prevent organisations from using more-efficient data-processing options abroad, slowing down digitisation by forcing data to remain in constrained domestic infrastructure.

Similarly, the GDPR's institutional requirements strain state capacity to deliver effective data protection enforcement.

India enacted its Digital Personal Data Protection Act (DPDPA) in 2023, mirroring key provisions of the EU's GDPR, including establishing a centralised enforcement body to ensure compliance with the DPDPA's provisions. Critics rightly point out that much in the same way as the EU, India's approach, through a central data protection board (DPB), will leave critical enforcement gaps that will result in only large technology companies being targeted.[43] For example, the DPDPA relies on the classification of "significant data fiduciaries" for closer scrutiny, capturing major technology companies and likely leading to enforcement of only the most prominent cases, whilst smaller firms are left largely unregulated.

Moreover, India's DPB would need to regulate roughly 600 million entities across India, a significant task it is not equipped to handle.[44] With no state-level offices and insufficient personnel to manage a potentially ever-growing caseload, this lack of state capacity will mean individuals are unable to appropriately enforce their data protection rights under the legislation.

The DPDPA also borrows from the GDPR's extraterritorial application, meaning foreign companies that operate with Indian personal data are captured by the legislation. However, the DPDPA and India's draft DPDP Rules—which support implementation of the DPDPA—remain silent on how India's DPB will enforce such rules, leaving individuals uncertain about

their rights, and companies uncertain about their legal obligations. This uncertainty ultimately discourages data-driven innovation.[45]

Whilst several African nations have adopted data protection rules akin to the GDPR, very few have the necessary enforcement structures in place. A lack of funding is a common and major barrier to the effective operationalisation of data protection rules akin to the GDPR. For example, Egypt passed its data protection law in 2020, but as of 2022, has yet to establish its DPA, much of which has been due to inadequate funding and capacity building, and a lack of the expertise and process that its data protection law requires.[46] Indeed, this lack of data protection awareness has been a key issue for several African DPAs, including Kenya, Nigeria, and Mauritius. Kenya's DPA has struggled from a lack of funding, contributing to low awareness and therefore ineffective enforcement. The DPA highlighted a resource gap of 76 percent under the government's 2022–2025 strategic plan, meaning it has barely a quarter of the funding and capacity required to carry out its mandated responsibilities.[47]

Interestingly, DPAs within the African continent tend to dedicate less time to enforcement and more to facilitating data transfers. Despite the introduction of data protection laws, cross-border data transfers continue much as before—the only difference is that legislation now forces regulators and companies to navigate an additional layer of bureaucracy. Evidence suggests that in many African countries, DPAs spend most of their limited capacity not on enforcing privacy rights, but rather on facilitating these transfers.[48] For instance, Cape Verde's DPA issued more than 1,300 authorisations for international data transfers in 2022 but imposed no fines or penalties for data protection infringements. Similar patterns are seen across the continent.

In effect, these regimes convert what should be a routine economic activity into an administrative ritual. Under tight budgets, regulators sensibly prioritise enabling data flows over imposing penalties, recognising that such flows bring greater economic benefit than does enforcement-driven deterrence. Yet, the requirement for prior authorisation itself is wasteful. It consumes scarce public sector resources and private sector funding and delays the very transfers that underpin modern commerce.

Firm Resources Directed Away From Innovation Towards Compliance

Within the Global South, three clear costs emerge related to the GDPR: the cost of compliance for small businesses in a predominantly small business economy, a lack of data intensity in knowledge-intensive sectors that restrict entry into a global knowledge economy, and a lack of substantial innovation to leapfrog established competitors. Taken together, both the GDPR itself, and the adoption of GDPR-style frameworks domestically, have had a significant negative impact on innovation within the Global South.

Beyond compliance with a national data protection framework—and the issues associated with that as previously mentioned—individual companies operating within third countries will need to comply with the EU's GDPR if they want to handle EU citizen data. Without an adequacy decision, for which the majority of the Global South lacks, there are two main ways to demonstrate GDPR compliance: adopting binding corporate rules (BCRs) or using standard contractual clauses (SCCs).

BCRs ensure high data protection standards across an entire organisation, which are useful for organisations that operate globally. However, these rules require approval by a data protection authority, meaning internal data protection standards ultimately align with the GDPR, regardless of whether the majority of a company's service operates within the EU. The process of obtaining BCRs is notoriously costly and time consuming, with some approvals taking years.[49]

SCCs rely on pre-approved model clauses adopted by the European Commission to facilitate international data transfers, however; due to their contractual nature, they are potentially enforced through several legal frameworks and require significant effort to implement for organisations with complex international data transfers. Coupled with the GDPR's extraterritoriality provisions, such an approach ensures that practically, the GDPR is the standard at both the country and company levels, and extensive evidence demonstrates that this approach to data protection has drastically hindered innovation, with firm resources dedicated away from those activities towards compliance. Indeed, one study found that with additional resources needed for compliance, the GDPR limited firm capacity to develop entirely new products.[50]

The patchwork of rules to facilitate cross-border data flows as organisations seek to operate globally increases costs for firms of all sizes, disincentivising global value chains. An increasingly complex privacy law ecosystem, for example, can generate new risks wherein firms are uncertain about which often conflicting requirements apply, and to which data and data processing activities. In turn, firms are less data intensive, and less likely to operate globally.[51] In fact, one study found that as a result of the GDPR, EU firms decreased data storage by 26 percent and data processing by 15 percent and incurred a 20 percent increase in the cost of data on average, when compared with U.S. firms.[52]

Less data intensity leads to less profitability. For European firms, the GDPR caused profits to shrink by an average of 8.1 percent—with the main burden falling on smaller businesses, though all firm sizes were negatively affected—with medium-sized companies spending close to $3 million each between 2017 and 2018 to fulfil regulatory requirements.[53] Moreover, the GDPR built barriers to entry into the digital economy by concentrating the market share of large incumbents with more resources and access to data, with some finding that, in practice, the GDPR functions like a 25 percent

tax on smaller companies.[54] Such an effect is harmful globally, where 90 percent of businesses worldwide are micro, small, and medium-sized businesses (MSMEs) responsible for 70 percent of employment and 50 percent of GDP.[55]

Similarly, the GDPR has heavily affected data-intensive sectors such as software and manufacturing, with the former incurring a 24 percent increase in data costs, and the latter 18 percent.[56] As a result, the availability of services has generally decreased. Worse still, the GDPR has also reduced the availability of new services. The GDPR has contributed to a reduction in radical innovation towards incremental innovation, meaning instead of introducing new products, firms have dedicated their time and resources to improving existing ones.[57] Cumulatively, this leads to a reduction in the development and, crucially, adoption of new innovations as individuals are cut off from innovative products.

For example, as of 2022, Kenya has had the highest number of digital agricultural services in Africa, with providers of these services ranging from smaller start-ups to larger companies.[58] Yet, even at the forefront of digital agriculture, penetration amongst Kenyan farmers remains between 20 and 30 percent.[59] One reason for this is many digital agricultural service providers operate across countries and are thereby reliant on cross-border data flows to deliver these services. Data protection laws that thwart this reduce the value proposition of the service, discouraging service providers from expanding into broader markets and limiting the accessibility of these services to their target consumers. One study recommended using aggregator platforms that could make services easier to locate, use, and trust.[60] Such a solution, however, would still require strict compliance with Kenya's DPA that would likely encounter the same issues that individual service providers currently experience.

Moreover, adopting Western rules forces domestic firms to not only compete with each other but also with already dominant Western firms. In Brazil, for example, creating GDPR-style rules domestically has incentivised adoption of privacy enhancing technologies (PETs), but the broader impact of the Brussels Effect—importing EU rules inspired by EU norms, values, and ideals—has meant Western firms, rather than domestic firms, have been better able to seize the economic benefits of a growing PET market. As of 2021, the size of the Brazilian PET market has reached $3 billion, reflecting growing demand for compliance technologies. But that same year, the number of Western PET firms operating in Brazil rose from 0 to 17, outnumbering the 4 domestic ones.[61] In other words, by importing the EU's rules, Brazil has made it easy for established foreign firms to offer compliance-ready solutions at the expense of domestic solutions.

By undermining the ambitions of Global South economies to leverage data, exacerbate already stressed state capacity and institutional capacity, and inhibit firm level data-driven innovation, the GDPR has cost the Global

South countries greatly, holding them back from taking advantage of innovation to improve living standards.

THE EU CONTINUES TO ADOPT DIGITAL REGULATIONS THAT ARE UNFRIENDLY TO INNOVATION WHICH THE BRUSSELS EFFECT AMPLIFIES GLOBALLY

The cost of conforming to EU-style digital regulation is not borne solely by those outside Europe—it is increasingly evident within the EU itself. Far from serving as a model of successful digital governance, the EU continues to entrench a precautionary, heavy-handed model of digital regulation that affects its own innovation. The Brussels Effect amplifies this approach globally, running the risk of Global South countries suffering the same innovation-stifling effects despite having had no meaningful role in shaping the laws the EU expects them to follow.

The Draghi report, authored by former European Central Bank president and former prime minister of Italy Mario Draghi, on the future of European competitiveness makes Europe's lagging innovation diagnosis explicit.[62] It attributes Europe's long-term economic underperformance to a lack of innovation capacity, compounded by regulatory barriers that inhibit scale and deter investment. In fact, in the last 50 years, no EU company with a market capitalisation of more than €1 billion has been created, compared with six U.S. companies with a valuation of more than €1 trillion each in the same period.[63] Meanwhile, nearly 30 percent of Europe's unicorn start-ups have relocated abroad, seeking regulatory environments more conducive to growth.[64]

Draghi identifies the root of this problem in the complexity and overreach of EU digital regulation, highlighting the existence of more than 100 EU tech-focused laws and over 270 active digital regulators across member states.[65] He further criticises GDPR-imposed obligations such as restrictions on cross-border data flows and data processing, which drive up compliance costs and undermine the development of large-scale, integrated datasets essential for AI training. As a result, core elements of the AI value chain—especially AI model training—increasingly take place outside the EU, where the regulatory environment is less restrictive and takes with it any benefits to the EU economy.

Beyond Draghi's assessment of the numerous EU regulations, a growing chorus of critics links this innovation-unfriendly trend to the guiding principle that underpins the establishment of EU regulations: the precautionary principle. Designed to prevent harm in the face of scientific uncertainty, the precautionary principle often results in overly conservative regulation that deters experimentation and dynamic market activity. The GDPR, DMA, DSA, and AIA are all the result of the precautionary principle, with clear consequences on European innovation.

Indeed, the EU's approach is so starkly against innovation efforts that it has led some to the conclusion that Europe's approach is, "If you can't innovate, regulate."[66] Following the GDPR's enactment, studies have found reduced venture capital investment, declining firm profitability, and lower innovation output among affected European tech companies.[67] The regulation has also been linked to a decline in innovation within the app market.[68] While people may debate whether the GDPR has improved privacy, it has clearly come at substantial cost to innovation.

The DMA departs from traditional ex post antitrust liability to ex ante regulatory obligations that lead to unnecessary interventions: the DMA prohibits pro-innovative practices simply because they are carried out by designated "gatekeepers."[69] This approach punishes scale rather than abuse and may obstruct the very kind of growth Europe claims to want. Regulatory uncertainty under the DMA has already had chilling effects on European innovation, with companies such as Apple warning that the rules could delay the rollout of products such as its Apple Intelligence AI tools to the EU.[70]

The DSA, while less directly tied to innovation outcomes, introduces compliance burdens that discourage firms from scaling. Its tiered system of obligations—imposing stricter requirements on "very large" online platforms compared with "large" online platforms—disincentivises companies from growing beyond arbitrary thresholds.[71] Moreover, the combination of obligations under the DSA, DMA, and AIA burdens smaller companies that lack the resources to absorb high compliance costs.[72] The result is a digital playing field skewed not only against innovation but also towards greater market concentration and fewer opportunities for smaller firms.

The AIA further illustrates the EU's negative stance towards innovation. Several high-profile companies have criticised its rigidity and regulatory overreach. Elon Musk's AI company xAI, for instance, has refused to endorse most of the EU's AI Code of Practice, calling it "detrimental to innovation".[73] Meta has issued open warnings to EU regulators, stating that current rules could stifle AI development and slow economic growth.[74] The company also recently refused to sign on to the EU's AI Code of Practice.[75] Former Google CEO Eric Schmidt has similarly remarked that Europe's regulatory model places its companies at a structural disadvantage relative to global peers.[76] Rather than encourage breakthrough development, the EU's rules push companies towards narrow, low-risk innovations that meet bureaucratic requirements but do little to advance global technological frontiers.

Indeed, the precautionary mindset fosters a culture of incrementalism: it rewards conformity over experimentation and deters the creation of non-standard, tailor-made technological solutions.[77] Entrepreneurs are left trying to innovate while being required to prove zero risk—a standard that is not only unreasonable but also fundamentally incompatible with how innovation works.[78] In practice, this transforms innovation into a threat the

EU must mitigate, rather than a force it should cultivate. Nowhere is this more visible than in the AI space, where companies have begun withholding or delaying the launch of key services in Europe due to regulatory uncertainty and complexity.[79]

Together, these trends reveal that the EU's approach to digital regulation, far from supporting innovation ecosystems, actively suppresses them. Whilst the EU is entitled to regulate in such a way for its own member states, the Brussels Effect takes this suppression beyond EU borders. As such, when third countries adopt the EU's digital rulebook, they import the same innovation-restricting framework—often without the economic scale or institutional capacity to absorb its costs. In this way, the EU's rules become a global liability, discouraging growth in such regions as the Global South that would benefit from innovation-friendly governance frameworks.

The Digital Markets Act

The EU introduced the DMA to combat what the Commission viewed as unfair, incontestable competition driven by a dominance of large technology companies.[80] The DMA operates by identifying "gatekeeper" technology companies that provide "core platform services" such as online search engines, app stores, and messenger services. The DMA regulates these gatekeepers to ensure that they do not take advantage of their powerful market position in order to inherently disadvantage other firms or service providers.

The DMA has attracted significant criticism for its shift from traditional case-by-case enforcement against actual harm to preemptive obligations related to a company's relative market position.[81] In particular, the DMA entrenches large firms, discouraging them from innovating to compete, and deterring the successful expansion of small and mid-size firms.[82] By operating in an ex ante regulatory fashion, the regulation distorts innovation incentives that threaten the vitality, dynamism, and competitive fairness of Europe's economy.

In the Global South, several countries have considered DMA-style regulation.

In Brazil, President Luiz Inácio Lula da Silva and his administration have actively promoted an ex ante competition regime, granting new powers to Brazil's competition authority and creating a new specialised digital platforms unit similar to the United Kingdom's Digital Markets Unit.[83] The new unit would operate within a DMA-style framework, identifying gatekeeper platforms and imposing obligations on them to remedy market failures. The proposal's focus on size-based thresholds and presumption of harm punishes the very characteristics that enable firms to deliver best-in-class products and services to the region, including scale, integration, and data capabilities.[84]

India has similarly proposed its draft Digital Competition Bill 2024, aimed at empowering the Competition Commission of India to address what India views as a "winner takes all" market wherein a few large digital incumbents capture and control the entire market at the expense of smaller players.[85] In drafting the proposal, India's Committee on Digital Competition Law analysed digital competition-related laws across jurisdictions. These laws included the EU's DMA, as well as DMA-inspired rules in the United Kingdom, and Germany's Act Against Restraints of Competition (ARC) 1958, whose 11th Amendment facilitates the adoption of the DMA.[86] Furthermore, new enforcement tools for India's existing antitrust legislation were inspired by practices in the EU.

Turkey's Draft Amendment of the Turkish Competition Act was directly inspired by the EU's DMA and Germany's ARC, borrowing key definitions such as "gatekeeper" and "core platform service."[87] The Draft's preamble also makes explicit its criticism of traditional competition rules that apply ex post that, in its view, do not effectively correct digital market issues, making the need for ex ante rules.[88]

Indonesia is considering both a DSA and DMA framework, with the deputy minister of communication and digital affairs explicitly stating that Indonesia's Ministry thinks, "The Digital Services Act (DSA) and Digital Markets Act (DMA) are among the best frameworks."[89] The EU ambassador to Indonesia also affirmed that cooperation in digital affairs between the two could bring a myriad of benefits.[90] This cooperation suggests that an alignment of digital frameworks could enhance digital trade relations.

Finally, in addition, evidence shows that other Global South countries have either adopted, proposed, or considered DMA-style regulation, including Kazakhstan, Kenya, Malaysia, Mexico, Morocco, Nigeria, South Africa, Thailand, and Uzbekistan.[91]

These cases demonstrate the EU's regulatory influence abroad. This adoption is significant because such widespread adoption of a regulation that clearly operates against a dynamic view of competition and innovation impacts those markets, but the negative innovation effects are arguably felt more acutely in Global South countries.

In these economies, large technology companies serve a fundamentally different role than they do in mature Western markets, often acting as enablers of innovation to meet local needs, filling in critical infrastructure gaps, investing in research and development (R&D), and drawing talent into underdeveloped digital sectors.[92] For example, in 2022, Google Search, Ads, AdSense, Play, YouTube, and Cloud helped provide R$153 billion of economic activity for businesses in Brazil, as well as supported over 200,000 jobs within Google's Android ecosystem.[93] And Meta estimates that the metaverse, which it is developing, could impact Indonesia's economy by almost 2.5 percent of its gross domestic product (GDP).[94] Large technology firms play a central role in introducing and

diffusing advanced technologies across local economies. Their platforms provide foundational tools and services that allow domestic businesses—especially small and medium-sized enterprises—to grow and compete on a global scale.

This effect is especially clear in the digital platform economy, wherein global tech firms act as intermediaries, offering local sellers access to broader markets, cloud infrastructure, development tools, and jobs. More than 50 percent of goods sold on major e-commerce platforms now come from third-party sellers, while a global community of over 26 million software developers rely on these platforms for infrastructure and distribution of their apps.[95] Indeed, Amazon's entry into the South African market makes the current e-commerce system more competitive, leading to better access for locals to their own e-commerce sector with Amazon partnering with local businesses and suppliers.[96] Upon entry into the market, Amazon also put out adverts for jobs to sustain operations within the region.[97] Ecosystems facilitated by larger companies lower barriers to entry for smaller firms and foster local entrepreneurship, creating multiplier effects across sectors and communities. In countries with fragmented logistics systems or limited broadband infrastructure, large platforms often serve as the backbone of market access and digital enablement. Cloud providers such as Amazon Web Services (AWS) also create large positive externalities, supplying low-cost, scalable compute and developer tools that shrink the capital and engineering needed to build and scale data-intensive products. Cloud enables MSMEs and start-ups to adopt sophisticated digital services and create new products. In Malaysia, AWS anticipates over $12 billion in GDP contribution from its operations in the region, with an estimated 3,500 new jobs created annually between 2024 and 2038.[98]

Similarly, M-Pesa, a money transfer system operated by Kenya's largest cellular phone provider Safaricom, has brought mobile phone coverage to over 60 percent of Africans, increasing local economic activity by facilitating money transfers.[99] And Shopify—a global e-commerce platform—has removed barriers to business, with merchants able to spend their time more efficiently and with greater impact. As of 2019, Shopify has supported over 2.1 million full-time jobs, with over 7,500 partners operating in developing countries around the world.[100]

E-commerce has been particularly transformative for the Global South. The rise of mobile-first digital economies, coupled with an expanding middle class and accelerated digital adoption during the COVID-19 pandemic, has brought millions of new consumers online for the first time.[101] Large technology firms have facilitated this shift, helping to build out the digital infrastructure and services that underpin this growth. In many cases, their platforms are the first entry point into the digital economy for both buyers and sellers, enabling microbusinesses to reach new markets, fostering

financial inclusion, and bridging longstanding divides in access to technology, education, and opportunity.

DMA-like rules directly threaten this model. The DMA's prescriptive approach to platform regulation—focused on restricting the conduct of large digital gatekeepers—is ill-suited to the realities of emerging economies. By breaking the integrated services that underpin many platform ecosystems, limiting cross-service interoperability and imposing blanket obligations that disregard local contexts, the DMA undermines the very actors that support digital inclusion and technology diffusion in developing regions. For Global South countries that emulate the DMA, the result may not be more competition or innovation, but rather less access, fewer opportunities, and a slower path to digital development.

The Digital Services Act

The DSA regulates online services to limit the spread of illegal or harmful content online. It does this by tying obligations to different categories of service provider, with additional obligations on designated VLOPs or Very Large Online Search Engines (VLOSEs). To address systemic risks posed by VLOPs and VLOSEs, both need to address user privacy, protection of minors, content moderation, and transparency and accountability. Actions include stringent content moderation systems such as flagging, swift action against illegal content, and transparent appeals processes. Any failure to comply with these obligations would lead to substantial fines of up to 6 percent of global annual turnover.[102]

Unfortunately, the DSA's complex requirements both impact its enforceability and open liability to companies that deter them from operating within the EU market. They also take resources away from innovation activities such as R&D towards regulatory compliance, further impacting the role such companies play in contributing to a thriving innovation ecosystem in the EU.

In particular, the DSA negatively impacts innovative models such as decentralised online platforms because it treats all platforms the same. By requiring every online platform to maintain a formal point of contact and comply with complex, prescriptive obligations, the DSA assumes a centralised authority that decentralised services such as Mastodon simply do not have. These volunteer-run, nonprofit networks are designed to distribute responsibility among users rather than a single entity, making compliance burdensome or even impossible. Functionally, the DSA entrenches incumbents because the DSA "tends to be distortive of the other models and possibly even stops [emerging players] from coming about at all".[103]

Moreover, the DSA's notification mechanisms and takedown obligations unduly burden online services. The scope of the DSA extends well beyond social media platforms to intermediary services such as Internet service

providers, cloud service providers, online marketplaces, and any other service that hosts third-party content. Within this scope, intermediary services must implement a notification mechanism for its users that, when implemented, would consider those services to have actual knowledge of any potential illegal content hosted on their sites.[104] This provision opens up a huge amount of liability exposure for companies, for which actual knowledge is met with an obligation for removal of that content in a timely manner. Such requirements are less burdensome for larger companies than emerging players and firms with fewer resources. On the whole, however, the imposition of actual knowledge, timeliness, and proactive takedowns creates an environment that deters both operation and innovation within the EU.

Unfortunately, Global South countries continue to propose DSA-style rules, with some positing that non-EU governments would favour the DSA because it validates burgeoning efforts to bring the Internet under government control, with heavy fines on large cooperations for noncompliance.[105]

Brazil's proposed "Fake News Bill" (Bill 2630) offers a case in point, with references to the DSA in particular on intermediary liability and emergency government powers.[106] The legislation would require Internet companies, search engines, and messaging services to proactively detect and report illegal content, under threat of substantial fines for noncompliance. Critics of the bill argue that this preventative obligation—covering material deemed capable of encouraging certain crimes—grants the state broad discretion to suppress lawful expression.[107] The result risks a more closed Internet environment in which legitimate discourse is chilled and technology companies are compelled, by law, to act as enforcers of government speech controls, disincentivising their operation. Indeed, when Elon Musk initially refused to ban several profiles on the platform X that the Brazilian government deemed to be spreading misinformation about the 2022 Brazilian presidential election, Brazil's Supreme Court blocked access to the platform.[108] Only after X paid $5 million in fines and blocked those accounts did Brazil's Supreme Court lift the ban.

In September 2022, Nigeria's National Information Technology Development Agency's (NITDA)'s Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries came into force, with similar objectives to the DSA to require intermediaries to deliver prompt responses to legal notices and remove harmful or unlawful content within 48 hours.[109] Moreover, when required by NITDA, platforms would need to disclose content creators' identities, and for large service platforms, they would need to be incorporated in Nigeria with a physical contact address. Nigeria's Code directly borrows from the DSA's size-based enforcement, as well as creates a clear link between government involvement and platform censorship.

India published its Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules 2021, inspired by the then DSA proposal which introduces tiered, size-based enforcement, take-downs, content moderation, and intermediary liability.[110] However, India's rules go a step further to also bring in online news publishers, which has triggered constitutional challenges to the rules currently sitting with the Delhi High Court.[111]

The DSA allows government to play a stronger role in the regulation of online speech by regulating the intermediary platforms that host such speech. This effect is amplified in countries where there is little infrastructure to balance the spread of illegal content online, and the necessity for free speech. Coupled with issues that traditionally plague developing countries such as corruption, political instability, and a fragile independent press, the DSA legitimises censorship online that restricts innovation through access to services and the increased compliance burdens that act as a barrier to firms entering the market.

The Artificial Intelligence Act

The AIA is the world's first AI-specific legislation, designed to regulate the development, deployment, and use of AI across the bloc. Taking a risk-based approach, various obligations apply based on the risk category for the AI system, with extra transparency obligations on general purpose AI (GPAI) providers, and strict requirements on any providers of "high-risk" AI systems. The AIA imposes penalties for noncompliance, as well as establishes an AI Code of Practice which, if companies comply with it, presumes conformity with the AIA until the European Commission establishes harmonised standards. Compliance with the Code involves certain safety, security, and transparency obligations.

The AIA has come under heavy criticism, not least because it does not actually represent a risk-based regulation. Indeed, even the main author behind the AI Act considers the final text to be a failure, so much so that he resigned from the European Commission.[112] Whilst the underlying objective of the AIA is to strike a balance between innovation and the protection of fundamental values, the AIA's provisions do not follow a truly risk-based approach, which leads to overregulation.[113] In particular, the AIA lacks the necessary risk-benefit analysis to achieve the AIA's objectives, does not rely sufficiently on empirical evidence, and lacks a case-by-case risk classification to strike the right balance between prevention of risk and facilitation of innovation. As previously explained, the AIA has led to a real-time loss in technological innovation within Europe, with several GPAI providers delaying or limiting access to their AI services in the region.

Moreover, evidence shows that, similar to the GDPR, which pushed innovation such as life science innovation outside of Europe, the same is likely to happen under the AIA.[114] Both the AIA and GDPR lacked the precision needed to ensure a clear regulatory environment, the main

reason why life science innovation left Europe upon the introduction of the GDPR. With the AIA, organisations focused on speed and efficiency to commercialise AI-powered medical products face increased regulatory complexity from similar ambiguity, as well as additional regulatory hurdles that impact time to market, and budgets. Not only do these hurdles limit the number of accessible AI-powered services, but they also reduce the amount of investment into AI-powered medical R&D, contributing to overall less innovation in the European life sciences marketplace.

Adoption of these rules beyond the EU is likely to see similar effects in different regions and sectors, but positively, some Global South countries have pushed back on the idea of conformity. For example, both South Africa and India have opted to avoid AIA style rules, instead exploring sector-specific and preexisting rules to address any market failure.[115] And non-European policymakers generally favour a light touch, sector-specific approach to AI regulation, in part because conformity to the EU is no longer essential. There is little incentive to access a market with, according to Mario Draghi, limited innovation capacity, contingent on rules that in turn hinder domestic AI innovation when compared with more favourable international markets such as the United States or China.

Unfortunately, this pushback is by no means widespread, with several other Global South countries exploring AIA proposals.

Latin America has seen two AIA replications. In December 2024, the Brazilian Senate approved the Brazil AI Act (Bill No. 2338/2023), which mirrors the EU's risk-based framework and imposes similar obligations on AI providers and operators; it now awaits final approval from the lower house and the president.[116] Peru has gone further, enacting AI Law No. 31814 earlier in July 2023, which classifies AI systems by risk and mandates transparency, human oversight, and data governance in close alignment with the EU approach.[117]

Turkey has proposed its own draft AI Law to harmonise its regulations with international AI standards.[118] Particular attention was paid to the EU AIA in the drawing up of the draft, which is likely why it mirrors the EU's risk classification system. Research also suggests that Turkey will use complementary secondary legislation to harmonise the draft law to the EU AIA.[119]

This evidence indicates some level of influence over the structure of AI legislation beyond the EU. As many Global South countries become more export oriented, the pressure grows to align domestic rules with international ones, such as those defined by the EU AIA, despite its limited effectiveness in fostering AI innovation. This pressure often results in proposals that cherry-pick elements of the EU framework yet still embed its core risk-based model and, importantly, the precautionary principle that underpins it.

Table 1: Summary of third countries with adopted or proposed EU-style digital rules as of August 2025.

	GDPR[120]	DMA[121]	DSA[122]	AIA[123]
Argentina	✓			
Brazil	✓	✓	✓	✓
Egypt	✓			
Georgia	✓			
India	✓	✓	✓	
Indonesia	✓	✓	✓	
Kenya	✓	✓		
Kazakhstan		✓		
Malaysia		✓		
Mexico	✓	✓		
Morocco		✓		
Nigeria	✓	✓	✓	
Peru				✓
Rwanda	✓			
South Africa	✓	✓		
Sri Lanka	✓			
Thailand	✓	✓		
Turkey	✓	✓		✓
Uganda	✓			
Uzbekistan		✓		
Vietnam	✓			

Alignment with EU rules can disadvantage Global South economies for two main reasons. First, replicating EU legislation wholesale means adopting rules they had no role in shaping, sacrificing regulatory sovereignty in exchange for access to a large market. Second, even when countries try to adapt the framework to be more innovation friendly, the EU's underlying legislation is inherently ill-suited to fostering innovation, so its shortcomings persist even without direct, full-scale adoption.

Taken together, these points show that while the EU has every right to regulate its internal market, a lack of opportunity for input from those outside the bloc undermines the EU's ambition to set a global standard. The EU treats Global South countries less as equal trading partners with their own priorities and more as passive recipients of its regulatory model. The EU's GDPR adequacy system illustrates this dynamic.

Moreover, the EU's digital rulebook has created little incentive for reform within the bloc, as much of the economic burden falls on non-EU companies, especially those in emerging technology sectors. While the EU acknowledges a need for simplification, there is little sign of a fundamental overhaul of its approach. This lack of change from within makes it all the more important for Global South countries to develop an alternative regulatory model that reflects their shared but distinct interests and harnesses innovation to drive social and economic prosperity for those regions.

GLOBAL SOUTH COUNTRIES NEED ALTERNATIVES TO EU-STYLE HARMONISATION FOR AI

As AI governance frameworks proliferate globally, Global South countries face increasing pressure to align with EU-style regulatory models. Yet, strict harmonisation is neither necessary nor well-suited to many development contexts. Instead, a growing range of alternative approaches demonstrates how countries can pursue AI governance that supports innovation, regional integration, and economic growth, while preserving regulatory autonomy.

Reject Wholesale Adoption of EU-Style AI and Data Rules

Global South countries should not adopt EU-style AI rules and instead forge their own regulatory pathways. A global pushback against the Brussels Effect opens doors for Global South countries to move beyond binary choices between compliance and isolation. It enables them to select from multiple governance models or develop innovative hybrid approaches that combine regulatory elements specifically tailored to their unique development contexts and economic priorities. By doing so, these countries can prioritise economic complementarity and innovation potential over rigid regulatory harmonisation with Europe.

Indeed, the GDPR's restrictions on cross-border data flows limit the ability of third countries to collaborate regionally because of its strict

requirements, inflexible nature, and negative trade impact. These constraints can inhibit regional economic integration and collective AI development, particularly for countries without EU adequacy decisions.

Build Flexible, Interoperable, and Regionally Grounded Governance Models

Countries without EU adequacy decisions have successfully developed alternative frameworks to facilitate cross-border data flows through more flexible and interoperable approaches. These include interoperability agreements, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Enforcement Arrangement (CPEA), the EU's Cross-Border Privacy Rules (CBPR), the G7 Ministerial Declaration to operationalise Data Free Flow with Trust, and ASEAN Model Contractual Clauses.[124]

In contrast with the GDPR, more flexible rules relying on mutual collaboration—such as the OECD Privacy Guidelines and APEC's CBPR—operationalise both privacy protection and secure cross-border data transfers simultaneously. The OECD Privacy Guidelines, for example, presume the allowance of free transfers of personal data, subject to proportionate restrictions based on risk and the availability of equivalent safeguards. Importantly, this approach prioritises data transfers while relying on ex post accountability rather than rigid ex ante controls.

These mechanisms demonstrate that regulatory diversity can coexist with functional international commerce, offering Global South countries governance models that preserve national autonomy while supporting innovation and economic integration.

Strengthen Regional Cooperation to Shape AI Rules Collectively

Regional models offer Global South countries powerful alternatives that leverage local partnerships and regional alliances. Latin America has already demonstrated momentum towards regional cooperation through initiatives such as the Second Ministerial Summit on the Ethics of AI in Latin America and the Caribbean, the Montevideo Declaration on regional AI governance, and the Cartagena Declaration, which was signed by 17 countries.[125]

Elsewhere, observers note that uneven AI safety governance, limited future readiness, and a challenging international outlook underscore the need for deeper regional cooperation in Southeast Asia, particularly around catastrophic risk management.[126] Stronger cooperation could support a shared AI talent pool and improve collective international representation. Similarly, the Economic Community of West African States (ECOWAS) is leveraging its regional platform to advance a pact on ethical AI and digital education, aligned with the ECOWAS Digital Strategy 2024–2029.[127] Four years after adopting its Data Protection Act, Kenya is also considering accession to the Malabo Convention.

As Global South countries determine their preferred AI governance approaches, they should both prioritise frameworks that build trust among regional partners and facilitate AI development through collaboration rather than distant regulatory alignment. APEC's CPEA offers one such path forward.

CPEA shows how voluntary cooperation can achieve effective governance on data privacy without sacrificing national autonomy or innovation. The framework creates a structure for regional cooperation in enforcement while specifically aiming to facilitate information sharing and promote effective implementation across diverse regulatory environments.[128] Developed during a period of experimentation with privacy laws in the region, CPEA operates as a common foundation for addressing privacy issues and implementing basic privacy principles while explicitly permitting variation among different jurisdictions.[129]

The framework's core principles illustrate how flexible governance can maintain standards without rigidity. These principles include harm prevention, choice over data processing, access and correction rights, and accountability measures, providing sufficient structure for cooperation while allowing adaptation to local contexts. Membership remains voluntary, leaving participants the freedom to create or leverage domestic privacy measures that benefit cross-border information sharing and privacy protection, enabling each member to facilitate protection in line with their preexisting regulatory structures rather than adapting to a rigid, one-size-fits-all approach.

CPEA's practical advantages address common resource constraints faced by developing nations. The arrangement provides leeway for member data protection authorities to prioritise issues based on their specific circumstances, addressing possible resource or capacity constraints that typically challenge data protection authorities.[130] Moreover, built on the premise of cooperation, open dialogue, and consensus, CPEA provides a mechanism for members to request assistance from other member enforcement authorities, spreading the load of responsibility whilst keeping economies involved.[131]

Current participants in CPEA include authorities from Australia, Hong Kong, Japan, South Korea, Malaysia, Mexico, New Zealand, the Philippines, Singapore, Taiwan, and the United States, demonstrating the framework's appeal across diverse economic and regulatory contexts.[132]

The business-friendly CBPR complements CPEA by focusing on practical implementation. Designed for businesses engaged in data processing across APEC economies, the CBPR builds on a voluntary accountability scheme that many view as more conducive to business operations and therefore easier to follow and implement without impeding traditional commercial activities.[133] Indeed, the focus of CBPR differs from the

GDPR's primary objective of protection of personal data to instead view privacy protection as a factor in the facilitation of cross-border information flows.[134] Currently active within the United States, Mexico, Japan, Canada, Singapore, South Korea, Australia, Taiwan, and the Philippines, the system demonstrates how international cooperation can facilitate rather than hinder business development.[135]

APEC's data governance approach provides a blueprint for Global South AI governance strategies. It shows how countries can address legitimate concerns around AI safety and security while preserving the freedom to leverage the technology for their own economic and social priorities—offering a compelling alternative to the restrictive harmonisation traditionally demanded by the EU.

CONCLUSION

The Brussels Effect represents less a triumph of soft power than an exercise in regulatory imperialism, as the EU exports its regulatory model to countries with little say in the process. A large academic literature recognizes that nations should differ in regulatory stringency based on levels of economic development. Lower-income countries naturally adopt less-stringent regulations than higher-income ones.[136]

The adoption of EU rules across multiple sectors, including digital policy and chemicals regulation, imposes high compliance costs and constrains innovation in third countries, particularly in the Global South, where firms and governments possess limited institutional and financial capacity to absorb such burdens.[137]

As EU-style rules spread globally, regulatory convergence constrains economic growth in the Global South. Global South countries should therefore resist default alignment with EU-style regulation and instead pursue frameworks that reflect domestic developmental needs and innovation potential. Flexible and context-sensitive regulatory approaches, including in AI and digital governance, would preserve regulatory autonomy while enabling these countries to help shape a more open and dynamic global innovation landscape.

REFERENCES

1. Robert D. Atkinson, "Resisting Europe's Regulatory Imperialism," *Latin Trade,* May 13, 2020, https://globalsilicones.org/wp-content/uploads/2020/11/Resisting-Europes-Regulatory-Emperialism-Latin-Trade.pdf.
2. Ibid.
3. Mark Scott and Laurens Cerulus, "Europe's new data protection rules export privacy standards worldwide," *Politico.EU*, January 31, 2018, https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.
4. Graham Greenleaf, "'European' Data Privacy Standards Implemented in Laws Outside Europe," (2017) 149 Privacy Laws & Business International Report 21-23, UNSW Law Research paper No. 18-2, September 3, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3096314.
5. Atkinson, "Resisting Europe's Regulatory Imperialism."
6. Naja Bentzen, "Protecting, promoting and projecting Europe's values and interests in the world," European Parliament Research Service, September 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652061/EPRS_BRI(2020)652061_EN.pdf.
7. Scott and Cerulus, "Europe's new data protection rules export privacy standards worldwide."
8. Juan Fernando López Aguilar on behalf of the Committee on Civil Liberties, Justice and Home Affairs, "Motion for a Resolution on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application," European Parliament, May 17, 2021, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.html.
9. European Council Press Release, "Remarks by President Charles Michel at the Munich Security Conference," European Union, February 20, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/02/20/remarks-by-president-charles-michel-at-the-munich-security-conference/; Edoardo Bressanelli et al., "The European Council: Truly The Law-Maker-In-Chief?" Centre for European Policy Studies, March 2025, https://cdn.ceps.eu/wp-content/uploads/2025/04/2025-03_INST-EU-Council.pdf.
10. Hilal Aka, "EU Regulatory Actions Against US Tech Companies Are a De Facto Tariff System," Information Technology and Innovation Foundation, April 28, 2025, https://itif.org/publications/2025/04/28/de-facto-eu-tariff-system/.
11. "EU paid Airbus billions in illegal subsidies, WTO rules," BBC News, May 15, 2018; Seungjoo Lee, "High technology and economic statecraft: the emergence of techno-economic statecraft in South Korea," *Cambridge University Press*, February 15, 2024, https://www.cambridge.org/core/journals/business-and-politics/article/high-technology-and-economic-statecraft-the-emergence-of-technoeconomic-statecraft-in-south-korea/9CD4E7168C5451208D018061CE56A960; Seungjoo Lee, "U.S.-China Technology Competition and the Emergence of Techno-Economic

Statecraft in East Asia: High Technology and Economic-Security Nexus," *Journal of Chinese Political Science*, January 3, 2024, https://link.springer.com/article/10.1007/s11366-023-09878-8.

12. See art 3. GDPR.

13. Dan Cooper and Laura Somaini, "European Commission Retains Adequacy Decisions for Data Transfers to Eleven Countries," *Inside Privacy*, January 17, 2024, https://www.insideprivacy.com/cross-border-transfers/european-commission-retains-adequacy-decisions-for-data-transfers-to-eleven-countries/.

14. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC.

15. "United Kingdom," European Parliament, accessed July 31, 2025, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-kingdom_en.

16. The Conservative European Forum, House of Lords European Affairs Committee UK-EU data adequacy inquiry, written evidence, May 24, 2024, https://committees.parliament.uk/writtenevidence/130595/html/.

17. "Adequacy decisions," European Commission [Accessed July 31, 2025], https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

18. European Parliament recommendation of 29 April 2021 to the Council, the Commission and the Vice-President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy concerning EU-India relations (2021/2023(INI)), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2021_506_R_0018.

19. F Ferracane et al., "Digital Trade, Data Protection and EU Adequacy Decisions," CITP Working Paper 6, Centre for Inclusive Trade Policy, October 11, 2023, https://citp.ac.uk/publications/digital-trade-data-protection-and-eu-adequacy-decisions.

20. Kenya engaged with the EU Commission in November 2024 at the 46th Global Privacy Assembly to agree a mutual adequacy agreement; however, no further progress appears to have been made. If granted, Kenya would be the first African country to achieve EU data adequacy. Similarly, Brazil and the EU are close to reaching a mutual adequacy arrangement for data flows according to a senior European Commission official.

    "EU Commission and Kenya close to agreeing a mutual adequacy agreement," Privacy Laws & Business, November 4, 2024, https://www.privacylaws.com/news/eu-commission-and-kenya-close-to-agreeing-a-mutual-adequacy-agreement/; Matthew Newman, "Brazil, EU near agreement on mutual-adequacy deal, EU Commission official says," MLex, March 26, 2025, https://www.mlex.com/mlex/articles/2316142/brazil-eu-near-agreement-on-mutual-adequacy-deal-eu-commission-official-says.

21. Benedikt Erforth and Charles Martin-Shields, "Where Privacy Meets Politics,: EU-Kenya Cooperation in Data Protection," Africa-Europe Cooperation and

Digital Transformation, 142–155, November 2022, https://www.taylorfrancis.com/reader/download/214d2647-f901-471c-a99f-10d905ffdf18/chapter/pdf.

22. See art 1(2) DMA, and art 2(1) DSA.

23. Helena Drewes and Alexander Kirk, "Extraterritorial Effects of the Digital Markets Act – The 'Elusive Long Arm' of European Digital Regulation," April 13, 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4763361; European Commission, "Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines," press release, April 25, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.

24. European Council Press Release, "Remarks by President Charles Michel at the Munich Security Conference," European Union, February 20, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/02/20/remarks-by-president-charles-michel-at-the-munich-security-conference/.

25. Cara Mannion, "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets," *Vanderbilt Journal of Transnational Law*, March 2, 2020, https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1019&context=vjtl.

26. Directorate-General for International Partnerships, "Global Gateway: EU launches Digital Economy Package for Kenya to boost connectivity, skills and inclusive governance," European Commission News Announcement, October 5, 2023, https://international-partnerships.ec.europa.eu/news-and-events/news/global-gateway-eu-launches-digital-economy-package-kenya-boost-connectivity-skills-and-inclusive-2023-10-05_en.

27. "BELLA – Building the Europe Link to Latin America," European Commission, accessed July 30, 2025, https://international-partnerships.ec.europa.eu/policies/programming/programmes/bella-building-europe-link-latin-america_en.

28. Foreign Affairs Department, "Brazil, European Union strengthen cooperation in digital governance, reaffirm legal frameworks for digital area," Brazilian government press release, February 14, 2024, https://www.gov.br/secom/en/latest-news/2025/02/brazil-european-union-strengthen-cooperation-in-digital-governance-reaffirm-legal-frameworks-for-digital-area.

29. "Key outcomes of the second EU-India Trade and Technology Council," European Commission publication, February 28, 2025, https://digital-strategy.ec.europa.eu/en/news/key-outcomes-second-eu-india-trade-and-technology-council.

30. J López González and J. Ferencz, "Digital Trade and Market Openness," OECD Trade Policy Papers, No. 217, 2018, https://www.oecd.org/en/publications/digital-trade-and-market-openness_1bd89c9a-en.html.

31. "Cross-border data flows," OECD Policy sub-issue, accessed October 16, 2025, https://www.oecd.org/en/topics/sub-issues/cross-border-data-flows.html.

32. Ibid.

33. Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology and Innovation Foundation, July 19, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

34. Mannion, "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets."

35. Sabina Frizell, "How Kenya's New Data Privacy Bill Could hurt Its Economy," Council on Foreign Relations, November 8, 2018, https://www.cfr.org/blog/how-kenyas-new-data-privacy-bill-could-hurt-its-economy.

36. The Data Protection Act, 2019, https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2021/LN263_2021.pdf.

37. Mugambi Laibuta, "Two years on: the impact the GDPR has had on privacy and data protection in Kenya," Inform, June 18, 2020, https://inforrm.org/2020/06/18/two-years-on-the-impact-the-gdpr-has-had-on-privacy-and-data-protection-in-kenya-mugambi-laibuta/.

38. "Kenya's Open Government Partnership (OGP) 5th National Action Plan 2023-2027," Kenyan government, accessed October 16, 2025, https://www.opengovpartnership.org/wp-content/uploads/2024/01/Kenya_Action-Plan_2023-2027_December.pdf.

39. Zunaira Saieed, "Johor rejects nearly 30% of data centre applications to protect local resources," *The Straits Times*, November 19, 2024, https://www.straitstimes.com/asia/se-asia/johor-rejects-nearly-30-per-cent-of-data-centre-applications-to-protect-local-resources.

40. "ASEAN's data centres electricity demand keeps growing," Ember, accessed October 16, 2025, https://ember-energy.org/chapter/setting-the-scene.

41. Kholofelo Kugler, "The Impact of Data Localisation Laws on Trade in Africa," Mandela Institute, University of Witwatersrand, 2022, https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB%2008%20Data%20localisation%20laws%20and%20trade.pdf.

42. Thiago Lima, "Power struggle: will Brazil's booming datacentre industry leave ordinary people in the dark?" *The Guardian*, March 4, 2025, https://www.theguardian.com/global-development/2025/mar/04/brazil-power-electricity-energy-poverty-datacentre-boom.

43. Abhijith Balakrishnan, "Enforcement Gaps in India's DPDP Act and the case for decentralized data protection boards," *Express Computer*, July 4, 2025, https://www.expresscomputer.in/guest-blogs/enforcement-gaps-in-indias-dpdp-act-and-the-case-for-decentralized-data-protection-boards/126140.

44. Ibid.

45. Ayndri, "Extraterritorial Application in Data Privacy: Lessons for India's DPDP Act," CyberPeace, March 6, 2025, https://www.cyberpeace.org/resources/blogs/extraterritorial-application-in-data-privacy-lessons-for-indias-dpdp-act.

46. Mercy King'ori and Hunter Dorwart, "A Look into DPA Strategies in the African Continent," Future of Privacy Forum, May 2022, https://fpf.org/wp-content/uploads/2022/05/African-DPAs-Strategies-Report.pdf.

47. Ibid.

48. Ibid.

49. Adam Gillert and Claudia Chan, "The new UK BCRs and their impact in practice," Freshfields, accessed October 17, 2025, https://www.lexology.com/library/detail.aspx?g=206d2c07-c38b-4549-82f1-4015104cf86e.

50. Knut Blind et al., "The impact of the EU General data protection regulation on product innovation," Centre for European Economic Research, 2023, https://publica-rest.fraunhofer.de/server/api/core/bitstreams/fc8aa755-7b55-4284-9a5c-cb19aa375df9/content.

51. Francesca Casalini et al., "Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers," OECD Trade and Agriculture Directorate, May 2021, https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/05/mapping-commonalities-in-regulatory-approaches-to-cross-border-data-transfers_e66a8dc0/ca9f974e-en.pdf.

52. Mert Demirer et al., "Data, Privacy Laws and Firm Production: Evidence From The GDPR," National Bureau of Economic Research Working Paper Series, February 2024, https://www.nber.org/system/files/working_papers/w32146/revisions/w32146.rev0.pdf.

53. Benjamin Mueller, "A New Study Lays Bare the Cost of the GDPR to Europe's Economy: Will the AI Act Repeat History?" Center for Data Innovation, April 9, 2022, https://datainnovation.org/2022/04/a-new-study-lays-bare-the-cost-of-the-gdpr-to-europes-economy-will-the-ai-act-repeat-history/; Aryamala Prasad, "Unintended Consequences of GDPR," Regulatory Studies Center, September 3, 2020, https://regulatorystudies.columbian.gwu.edu/unintended-consequences-gdpr.

54. Dylan Walsh, "GDPR reduced firms' data and computation use," MIT Sloan, September 10, 2024, https://mitsloan.mit.edu/ideas-made-to-matter/gdpr-reduced-firms-data-and-computation-use.

55. Dr. Ayman ElTarabishy and Dr. Rico Baldegger, "Global Micro-, Small and Medium-Sized Enterprises Report," International Council for Small Business, June 27, 2024, https://www.un.org/sites/un2.un.org/files/globalmsmesreport2024.pdf.

56. Walsh, "GDPR reduced firms' data and computation use."

57. Knut Blind et al., "The impact of the EU General data protection regulation on product innovation," Centre for European Economic Research, 2023, https://publica-rest.fraunhofer.de/server/api/core/bitstreams/fc8aa755-7b55-4284-9a5c-cb19aa375df9/content.

58. Heike Baumuller and John Kieti, "Digital solutions are boosting agriculture in Kenya, but it's time to scale up. Here's how," *The Conversation*, November 1, 2022, https://theconversation.com/digital-solutions-are-boosting-agriculture-in-kenya-but-its-time-to-scale-up-heres-how-192422.

59. Ibid.

60. Ibid.

61. Renan Gadoni Canaan, “The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law,” *Internet Policy Review*, February 28, 2023, https://policyreview.info/articles/analysis/replicating-gdpr-into-brazilian-general-data-protection-law.

62. Mario Draghi, “The future of European competitiveness,” European Commission, September 2024, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059.

63. Ibid.

64. Ibid.

65. Ibid.

66. Josh Withrow, “Don’t stifle U.S. tech innovation with Europe’s rules,” *The Detroit News*, October 9, 2022.

67. Jian Jia et al., “The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment,” Marketing Science 40(4):661-684, March 1, 2021, https://pubsonline.informs.org/doi/10.1287/mksc.2020.1271; Luis Garicano, “Is GDPR undermining innovation in Europe?” Silicon Continent, September 11, 2024, https://www.siliconcontinent.com/p/is-gdpr-undermining-innovation-in.

68. Rebecaa Janßen et al., “GDPR and the Lost Generation of Innovative Apps,” National Bureau of Economic Research, May 2022, https://www.nber.org/papers/w30028.

69. Aurelien Portuese, “The Digital Markets Act: A Triumph of Regulation Over Innovation,” Information Technology and Innovation Foundation, August 2022, https://www2.itif.org/2022-digital-markets-act.pdf.

70. Aaron Tilley and Kim Mackrael, “Apple Says Regulatory Concerns Might Prevent Rollout of AI Features in Europe,” *The Wall Street Journal*, June 21, 2024, https://www.wsj.com/tech/ai/apple-says-regulatory-concerns-may-prevent-rollout-of-ai-features-in-europe-0b0aaf5e.

71. Fredrik Erixon, “‘Too Big to Care’ or ‘Too Big to Share’: The Digital Services Act and the Consequences of Reforming Intermediary Liability Rules,” European Centre for International Political Economy, April 2021, https://ecipe.org/publications/digital-services-act-reforming-intermediary-liability-rules/.

72. Fredrik Erixon et al., “After the DMA, the DSA and the New AI Regulation: Mapping the Economic Consequences of and Responses to New Digital Regulations in Europe,” European Centre for International Political Economy, March 2022, https://ecipe.org/wp-content/uploads/2022/04/ECI_22_OccPaper_DMA-DSA-AI_03_2022_LY03.pdf.

73. Nancy Jaiswal, “Elon Musk’s xAI to sign only safety chapter of EU AI code, slams rest as ‘detrimental to innovation’; details here,” *India Times*, July 31, 2025, https://www.indiatimes.com/trending/elon-musks-xai-to-sign-only-safety-chapter-of-eu-ai-code-slams-rest-as-detrimental-to-innovation-details-here-665504.html.

74. Kim Mackrael, “Meta to European Union: Your Tech Rules Threaten to Squelch the AI Boom,” *The Wall Street Journal*, September 19, 2024,

https://www.wsj.com/tech/ai/meta-to-european-union-your-tech-rules-threaten-to-squelch-ai-boom-35297c03.

75. Ram Iyer, "Meta refuses to sign EU's AI code of practice," *Tech Crunch*, July 18, 2025, https://techcrunch.com/2025/07/18/meta-refuses-to-sign-eus-ai-code-of-practice/.

76. Ross Kelly, "'Europe could do it, but it's chosen not to do it' Eric Schmidt thinks EU regulation will stifle AI innovation – but Britain has a huge opportunity," *IT Pro*, February 13, 2025, https://www.itpro.com/business/policy-and-legislation/eric-schmidt-eu-ai-regulation-uk.

77. Evelyne Hoffman, "From GDPR to AI: How the EU Rules Stifle Technological Innovation in 2025," WINSS, July 27, 2025, https://www.winssolutions.org/european-union-technological-innovation/.

78. Mohamed Moutii, "Europe's Precautionary Principle Is Killing the Next Big Thing," *The Daily Economy*, July 30, 2025, https://thedailyeconomy.org/article/europes-precautionary-principle-is-killing-the-next-big-thing/.

79. Ayesha Bhatti, "EU Competitiveness Hinges on Digital Adoption Not Digital Regulation," Center for Data Innovation, September 3, 2024, https://datainnovation.org/2024/09/eu-competitiveness-hinges-on-digital-adoption-not-digital-regulation/.

80. "About the Digital Markets Act," European Commission [accessed August 4, 2025], https://digital-markets-act.ec.europa.eu/about-dma_en#what-does-this-mean-for-gatekeepers.

81. Portuese, "The Digital Markets Act: A Triumph of Regulation Over Innovation"; Matthias Bauer et al., "EU Export of Regulatory Overreach: The Case of the Digital Markets Act (DMA)," European Centre for International Political Economy, April 2025, https://ecipe.org/publications/eu-export-of-regulatory-overreach-dma/.

82. Portuese, "The Digital Markets Act: European Precautionary Antitrust."

83. Dario Oliveira Neto, "Lessons from the UK for Brazil's Digital Market Strategy," *Truth on the Market*, July 22, 2025, https://truthonthemarket.com/2025/07/22/lessons-from-the-uk-for-brazils-digital-market-strategy/.

84. "Brazil's Digital Markets Act," Information Technology and Innovation Foundation, accessed August 8, 2025, https://itif.org/publications/2025/05/25/brazil-digital-markets-act/.

85. Sonam Mathur et al., "India: navigating digital markets through the proposed ex ante framework," *GCR*, October 2, 2024, https://globalcompetitionreview.com/guide/digital-markets-guide/fourth-edition/article/india-navigating-digital-markets-through-the-proposed-ex-ante-framework.

86. Ibid.

87. Bahadir Balki et al., "Türkiye: data commoditisation warrants updated regulatory framework," GCR, May 30, 2025, https://globalcompetitionreview.com/guide/data-antitrust-guide/second-edition/article/turkiye-data-commoditisation-warrants-updated-regulatory-framework.

88. Cihan Doğan, “Turkish DMA: What’s in the Package?” *Kluwer Competition Law Blog*, August 15, 2024, https://legalblogs.wolterskluwer.com/competition-blog/turkish-dma-whats-in-the-package/.

89. Rahmad Nasution and Farhan Kenzu, “Indonesia studies EU’s digital regulations for governance framework,” *Antara News*, April 28, 2025, https://en.antaranews.com/news/353173/indonesia-studies-eus-digital-regulations-for-governance-framework.

90. Ibid.

91. Ronan Murphy, “Mapping the Brussels Effect,” Centre for European Policy Analysis, March 19, 2025, https://cepa.org/comprehensive-reports/the-brussels-effect-goes-global/.

92. Matthias Bauer et al., “EU Export of Regulatory Overreach: The Case of the Digital Markets Act (DMA),” European Centre for International Political Economy, April 2025, https://ecipe.org/publications/eu-export-of-regulatory-overreach-dma/.

93. Access Partnership, “Google’s Economic Impact in Brazil,” Google, September 2023, https://accesspartnership.com/wp-content/uploads/2023/09/Googles-Economic-Impact-in-Brazil-EN-1.pdf.

94. Deloitte Center for the Edge, “The Potential Economic Impact of the Metaverse in Indonesia,” Meta, 2022; Sri Haryati et al., “Metaverse development to positively impact national economy: Minister,” *Antara News*, August 24, 2022, https://indonesia.fb.com/wp-content/uploads/sites/68/2023/05/The-Potential-Economic-Impact-of-the-Metaverse-in-Indonesia-2022.pdf.

95. Bauer et al., “EU Export of Regulatory Overreach: The Case of the Digital Markets Act (DMA).”

96. Amy-Leigh Lambert, “Amazon’s Quiet Move into South Africa,” RT7, October 11, 2024, https://rt7digital.com/blog/amazons-quiet-move-into-south-africa-2.

97. Phillip de Wet, “Amazon is hiring a whole bunch of South Africans again, some to work from home, with only matric,” *news24*, March 14, 2023, https://www.news24.com/business/companies/amazon-is-hiring-a-whole-bunch-of-south-africans-again-some-to-work-from-home-with-only-matric-20230314.

98. “AWS Investment In Malaysia: Economic Impact Study,” AWS, 2024, https://d1.awsstatic.com/onedam/marketing-channels/website/aws/en_US/events/approved/documents/malaysia-economic-impact-study.pdf.

99. Sebastian Edwards et al., “Mobile Banking: The Impact of M-Pesa in Kenya,” *African Successes, Volume III: Modernization and Development*, University of Chicago Press, September 2016, https://www.nber.org/system/files/chapters/c13367/c13367.pdf.

100. Anastasia Philopoulos, “Shopify’s Global Economic Impact Report: How Shopify Partners are Changing Commerce,” Shopify, October 30, 2019, https://www.shopify.com/partners/blog/shopify-global-economic-impact-report.

101. Filipe Nery, “The Rise of E-commerce in Emerging Markets: Opportunities and Challenges,” Lyzer, January 8, 2025, https://www.lyzer.tech/blog/rise-e-commerce-emerging-markets-opportunities-challenges.

102. “DSA: Very large online platforms and search engines,” European Commission [accessed August 6, 2025], https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.

103. Makenzie Holland, “Laws geared to big tech could harm decentralized platforms,” *Tech Target*, Mar 1, 2023, https://www.techtarget.com/searchcio/news/365531985/Laws-geared-to-big-tech-could-harm-decentralized-platforms.

104. Article 16, Digital Services Act.

105. Anpuam Chander, “When the Digital Services Act Goes Global,” *Berkeley Technology Law Review*, *Vol. 38, Issue 3,* 1067–1088, 2023, https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?params=/context/facpub/article/3566/&path_info=When_the_DSA_Goes_Global_final_Berkeley_Tech.pdf.

106. Joan Barata, “Regulating Online Platforms Beyond the Marco Civil in Brazil: The Controversial ‘Fake News Bill’,” *Tech Policy Press*, May 23, 2023, https://www.techpolicy.press/regulating-online-platforms-beyond-the-marco-civil-in-brazil-the-controversial-fake-news-bill/.

107. Wesley Oliveira, “Votação do PL das fake news provoca racha de forças políticas na Câmara dos Deputados,” *Gazeta Do Povo*, April 24, 2023, https://www.gazetadopovo.com.br/republica/votacao-do-pl-das-fake-news-provoca-racha-de-forcas-politica-na-camara-dos-deputados/.

108. Ben Derico and Ione Wells, “Brazil lifts ban on Musk’s X after it pays £5m fine,” BBC News, October 8, 2024, https://www.bbc.co.uk/news/articles/c5y06vzk3yjo.

109. Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries, National Information Technology Development Agency, accessed August 11, 2025, https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTIVE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf.

110. “India: Massive Overhaul of Digital Regulation, With Strict Rules For Take-Down Of Illegal Content And Automated Scanning Of Online Content,” Future of Privacy Forum, March 11, 2021, https://fpf.org/blog/india-massive-overhaul-of-digital-regulation-with-strict-rules-for-take-down-of-illegal-content-and-automated-scanning-of-online-content/.

111. Medha Garg, “Constitutional Challenges to the IT Rules, 2021: Arguments Set to Begin,” Internet Freedom Foundation, October 17, 2024, https://internetfreedom.in/dhc-it-rules-2021-hearing/.

112. Ruth Fulterer, “«Das Gegenteil von dem, was ich erreichen wollte»: Der Hauptautor des KI-Gesetzes der EU packt aus,” *NZZ*, September 12, 2025, https://www.nzz.ch/technologie/hauptautor-des-ki-gesetzes-der-eu-packt-aus-ld.1899070.

113. Martin Ebers, “Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU’s AI Act,” *European Journal of Risk Regulation* 16(2):684-703, November 6, 2024, https://www.cambridge.org/core/journals/european-journal-of-risk-

regulation/article/truly-riskbased-regulation-of-artificial-intelligence-how-to-implement-the-eus-ai-act/E526C1D0D7368F9691082220609D60F4.

114. Mike King and Alex Denoon, "The EU AI Act: will regulation drive life science innovation away from Europe?" European Pharmaceutical Review, November 28, 2024, https://www.europeanpharmaceuticalreview.com/article/238250/the-eu-ai-act-will-regulation-drive-life-science-innovation-away-from-europe/.

115. Dr. Nils Rauer and Andrew Attieh, "South Africa takes first steps towards AI regulation," Pinsent Masons, November 14, 2024, https://www.pinsentmasons.com/out-law/news/south-africa-takes-first-steps-towards-ai-regulation; Amlan Mohanty and Shatakratu Sahu, "India's Advance on AI Regulation," Carnegie India, November 21, 2024, https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en.

116. "Brazil AI Act," accessed August 11, 2025, https://artificialintelligenceact.com/brazil-ai-act/.

117. "Peru: AI landscape," Data Guidance, February 19, 2025, https://www.dataguidance.com/opinion/peru-ai-landscape.

118. Alican Babalioglu et al., "New Turkish AI Law on the horizon," CMA Law-Now, July 9, 2024, https://cms-lawnow.com/en/ealerts/2024/07/new-turkish-ai-law-on-the-horizon.

119. Ibid.

120. Murphy, "Mapping the Brussels Effect: The GDPR Goes Global."

121. Ibid.

122. See The Digital Services Act sub-section on page 18.

123. See The Artificial Intelligence Act sub-section on page 20.

124. Ministerial Declaration – The G7 Digital and Tech Ministers' Meeting, 2023, https://g7g20-documents.org/database/document/2023-g7-japan-ministerial-meetings-ict-ministers-ministers-language-ministerial-declaration-the-g7-digital-and-tech-ministers-meeting#section-2.

125. Carolina Aguerre, "Strategies, norms, cooperation: three approaches to AI governance in Latin America," KU Leuven, October 15, 2024, https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/strategies-norms-cooperation-three-approaches-to-ai-governance-in-latin-america; Maia Levy Daniel, "Regional cooperation crucial for AI safety and governance in Latin America," Brookings Institute, February 13, 2025, https://www.brookings.edu/articles/regional-cooperation-crucial-for-ai-safety-and-governance-in-latin-america/.

126. Lyantoniette Chua et al., "AI Safety Governance, The Southeast Asian Way," Center for Technology Innovation at Brookings, August 2025, https://www.brookings.edu/wp-content/uploads/2025/08/GS_08252025_AISA_report.pdf.

127. Ola Schad Akinocho, "ECOWAS Lawmakers Push for Regional Pact on Ethical AI and Digital Education," *We Are Tech.Africa*, July 3, 2025, https://www.wearetech.africa/en/fils-uk/news/tech/ecowas-lawmakers-push-for-regional-pact-on-ethical-ai-and-digital-education.

128. Asian-Pacific Economic Cooperation, "APEC Cross-border Privacy Enforcement Arrangement (CPEA)," February 2024, accessed September

12, 2025, https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group/cross-border-privacy-enforcement-arrangement.

129. Ellyce R Cooper and Alan Charles Raul, *The Privacy, Data Protection And Cybersecurity Law Review*, Chapter 3, The Law Reviews, 5th Edition, October 2018, https://datamatters.sidley.com/wp-content/uploads/sites/2/2018/11/APEC-Overview.pdf.

130. APEC Cooperation Arrangement for Cross-Border Privacy Enforcement, accessed September 12, 2025, https://www.apec.org/docs/default-source/groups/ecsg/cbpr/cpea-2019.pdf?sfvrsn=f1643e20_1.

131. Cooper and Raul, *The Privacy, Data Protection And Cybersecurity Law Review*.

132. "APEC Cross-border Privacy Enforcement Arrangement (CPEA)," Asian-Pacific Economic Cooperation, February 2024, accessed September 12, 2025, https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group/cross-border-privacy-enforcement-arrangement.

133. Clare Sullivan, "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era," Computer Law & Security Review, Volume 35, Issue 4, August 2019, 380–397.

134. Ibid.

135. "What is the APEC CBPR?" NCC Group, July 20, 2023, https://www.nccgroup.com/what-is-the-apec-cbpr/.

136. Gene M. Grossman and Alan B. Krueger, "Economic Growth and the Environment," *Quarterly Journal of Economics 110, no. 2* (May 1995): 353–377, https://www.jstor.org/stable/2118443.

137. Atkinson, "Resisting Europe's Regulatory Imperialism."

ABOUT THE AUTHOR

Ayesha Bhatti is an AI governance advisor based in London. Previously, she was head of digital policy for the United Kingdom and EU at ITIF's Center for Data Innovation. Prior to joining ITIF, she worked as a data scientist at a technology consulting firm in London. She has an LLB from the University of Nottingham and an MSc in Computer Science from Birkbeck, University of London. She is also a licensed attorney in the state of New York.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation studies the intersection of data, technology, and public policy. With staff in Washington, London, and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the Information Technology and Innovation Foundation (ITIF), a nonprofit, nonpartisan think tank.

Contact: info@datainnovation.org

datainnovation.org