

How Leaders in the Global South Can Devise AI Regulation That Enables Innovation: *Annex*

IMPACT ASSESSMENT FOR POSSIBLE AI REGULATORY INTERVENTIONS

The impact assessment presented in this table is not exhaustive. We recommend that countries use it to identify their own regulatory priorities, context and mechanisms (per steps one to three of our five-step process). They should then conduct a detailed assessment of the potential impact of regulatory interventions across the four dimensions of the AI lifecycle on the AI Regulation Wheel while designing their approach.

Figure 1 – Impact Assessment Framework

⊕ Positive impact ⊖ Negative impact ⊕/⊖ Mixed impact, where the effect can vary depending on context or implementation

AI LIFECYCLE COMPONENTS	PRIORITIES & MECHANISMS	ECONOMIC GROWTH	LABOUR MARKET	NATIONAL SECURITY	CONSUMER PROTECTION & CONFIDENCE	TRADE & OPENNESS	CLIMATE
Input (data & feedstocks)	Transparent use of data	⊕/⊖ Compliance costs but increases competition and innovation	⊕ Preserves some jobs	⊕ Reduces misuse	⊕ Prevents harmful developments	⊖ Restricts data flow	⊕/⊖ Better reporting on environmental impact or increases energy consumption
	Protect copyright and IP	⊖ Increased cost of data	⊕ Preserves some jobs	⊖ Less effective tool	⊖ Limits consumer choice and increases prices in short term	⊖ Makes operating in country more difficult	⊕/⊖ Fosters more efficient data usage or leads to less-effective tools
	Data accuracy and lawfulness	⊕/⊖ Compliance costs, but makes better models	⊕/⊖ Creates new jobs, or limits others	⊕ Creates more accurate tools, which decreases misuse	⊕ Improves accuracy of outputs and reduces risk of harms	⊖ Makes operating in country more difficult	⊕ Fosters more efficient data usage
	Promote data diversity and prevent bias	⊕/⊖ Compliance costs or may make better models	⊕ Prevents job discrimination	⊕ Creates more accurate tools, which decreases misuse	⊕ Prevents discriminatory outcomes	⊖ Makes operating in-country more difficult	⊖ Increased energy use and infrastructure requirements
Development (training & testing)	Mandate safety testing and risk standards	⊕/⊖ Keeps some models from reaching market, or models may be more effective	⊕/⊖ Prevents AI encroaching on more professions or increases demand for new specialised jobs	⊕ Prevents dangerous AI developments	⊕ Prevents harmful effects for consumers	⊖ Less friendly investment environment	⊕/⊖ Initial higher energy usage or fewer failings requiring fixes
	Provide technical transparency and user-friendly explanations	⊕/⊖ Compliance costs or supports innovation	⊕/⊖ Creates new jobs or increases demand for others	⊕ Prevents dangerous AI developments	⊕ Increases public understanding of AI	⊖ Less friendly investment environment	⊕/⊖ More efficient models or increases energy and storage

⊕ Positive impact ⊖ Negative impact ⊕/⊖ Mixed impact, where the effect can vary depending on context or implementation

AI LIFECYCLE COMPONENTS	PRIORITIES & MECHANISMS	ECONOMIC GROWTH	LABOUR MARKET	NATIONAL SECURITY	CONSUMER PROTECTION & CONFIDENCE	TRADE & OPENNESS	CLIMATE
	Mandate central algorithm registry	⊖ Compliance costs	⊕ Creates new specialised roles	⊕ Prevents dangerous AI developments	⊕ Fewer unknowns and boosts consumer trust	⊖ Less friendly investment environment	⊕/⊖ Increased energy consumption and greater infrastructure requirements or leads to better resource allocation
	Regulate foreign use of domestic service providers to train AI	⊖ Retaliatory laws and decreases country's competitiveness	⊕ Helps protect labour force	⊕/⊖ Prevents misuse of AI and safeguards strategic resources, or damages international relations	⊕/⊖ Increases consumer confidence through enhanced privacy and transparency, or reduces consumer choice, or increases costs	⊖ Retaliatory laws from foreign countries and isolates domestic industries	⊕/⊖ Infrastructure duplication or drives investment in local energy infrastructure
	Impose data-centre energy limits	⊕/⊖ Impedes model development but avoids resource drain from other industries	⊕/⊖ Creates new jobs or limits others	⊖ Impedes model development	⊕/⊖ Increased transparency around energy or may create barriers for entry	⊖ Less friendly investment environment	⊕ Limits emissions
Output (AI applications)	Mandate high-risk AI-systems compliance	⊖ Stifles innovation, increased compliance costs, reduced competitiveness	⊕ Increased demand for compliance specialists	⊕ Controls AI systems, which poses greatest potential risk to national security	⊕ Increased consumer safety and reduced risk	⊖ Regulatory divergence/non-tariff trade barriers	⊖ Potential to slow down the development of innovative AI solutions
	Require human oversight	⊖ Increased costs and potential drag on profitability	⊕ Creation of new roles in AI-oversight ethics and compliance	⊕/⊖ Enhanced reliability and improved safeguards or impacts supply chain and ability to compete	⊕ Clearer lines of responsibility and stronger safeguards for the consumer	⊖ Risk of barriers to trade	⊕ Improved reliability and verification
	Require transparency when AI is used	⊖ Compliance costs, market consolidation and slow consumer adoption of AI solutions	⊕ Creation of new roles in AI R&D leads to sector's growth	⊕ Provides more visibility and strengthened security defences	⊕ Increased consumer trust and adoption	⊖ Risk of access to market	⊕/⊖ Increases energy usage or identifies energy inefficiencies
	Regulate AI-driven recommendations	⊖ Compliance costs and inhibits algorithm design	⊕ Protection for workers and increased transparency	⊕ Increased control overflow of information	⊕ Increased trust and user engagement	⊖ Restricts data flows and digital trade	⊕/⊖ Increases processing power or leads to efficient content delivery
	Require independent evaluation and reporting	⊖ Compliance costs and market concentration	⊕ Increased demand for ethics/compliance professionals	⊕ Secure and reliable defence systems	⊕ Enhanced quality and trust	⊕/⊖ Trade barriers or increased appeal through trustworthiness	⊕ Additional infrastructure to optimise systems

Economic growth: Influence on GDP, innovation, business competitiveness and market expansion

Labour market: Effects on job creation, skills demand and workforce displacement

National security: Implications for safeguarding sensitive data, preventing misuse and maintaining sovereignty

Consumer protection & confidence: Impact on consumer trust, safety and adoption of AI technologies

Trade & openness: Effects on international trade, regulatory harmonisation and market accessibility

Climate: Environmental considerations, including energy consumption and carbon footprint

⊕ Positive impact ⊖ Negative impact ⊕/⊖ Mixed impact, where the effect can vary depending on context or implementation

AI LIFECYCLE COMPONENTS	PRIORITIES & MECHANISMS	ECONOMIC GROWTH	LABOUR MARKET	NATIONAL SECURITY	CONSUMER PROTECTION & CONFIDENCE	TRADE & OPENNESS	CLIMATE
Feedback loop	Require post-market monitoring by AI developers and deployers	⊕/⊖ Compliance costs, or rapid identification of issues and improvements could mean more business	⊕ Increased demand for compliance specialists	⊖ Tension between transparency and confidentiality for national security	⊕ Enhanced product safety/issue resolution	⊖ Restricts market access and clashes with desire to protect IP	⊕/⊖ Higher energy consumption initially, but optimisation over time
	Establish AI Office	⊕/⊖ Additional layer of government bureaucracy or ensures horizontal consistency of standards and regulations	⊖ Stifles innovation in favour of protecting current labour market	⊕/⊖ Enhanced collective efforts, but limits individual states' autonomy	⊕ Faster and more reliable compliance with AI regulations and enhanced recalls/updates on identified issues	⊕/⊖ Promote global standards or creates regulatory divergence	⊕ Pushes climate agenda forward through greater coordination
	Require reporting of serious incidents	⊕/⊖ Short-term disruption or improved long-term stability	⊕ Increased demand for compliance specialists	⊕ Enhanced identification of vulnerabilities and resilience	⊕ Enhanced trust and product safety/issue resolution	⊕/⊖ Trade delays and restricted market access or greater trade long term	⊕/⊖ Increased computational resources or earlier detection of energy-wasteful malfunctions
	Mandate quality-management systems	⊖ Compliance costs	⊕ Increased demand for specialists	⊕ Enhanced control to prevent negative outcomes	⊕ Increased transparency/protection from harms	⊖ Increased operational costs for trade	⊕/⊖ Require additional infrastructure requirements or leads to more efficient resource utilisation
	Identify derived data (open data/data-sharing standards)	⊕ Innovation in data quality and increased productivity	⊕ Increased demand for technical experts	⊕ Reliable systems	⊕ Increased consumer trust	⊕ New global benchmarks for data practices	⊕/⊖ Increased infrastructure demand or efficient allocation

Economic growth: Influence on GDP, innovation, business competitiveness and market expansion

Labour market: Effects on job creation, skills demand and workforce displacement

National security: Implications for safeguarding sensitive data, preventing misuse and maintaining sovereignty

Consumer protection & confidence: Impact on consumer trust, safety and adoption of AI technologies

Trade & openness: Effects on international trade, regulatory harmonisation and market accessibility

Climate: Environmental considerations, including energy consumption and carbon footprint

AI USE: RISKS, SUB-RISKS AND IMPACT

A classification system, such as the one included in the International Scientific Report on the Safety of Advanced AI,¹ offers a useful starting point for understanding the risks and sub-risks associated with AI use. Figure 2 outlines these classifications and provides a non-exhaustive overview, supported by real-world examples.

Figure 2 – AI-related risks associated with the use of advanced AI systems

RISK	DEFINITION	SUB-RISK	EXAMPLE	IMPACT
Malicious use	The intentional use of AI technologies for harmful purposes	Harm to individuals through fake content	AI systems leveraged by criminals to attack individuals ²	Increased personal security risk, erodes trust
		Disinformation and manipulation of public opinion	AI-generated fake news inciting violence ³	Destabilises societies, erodes trust
		Cyber offence	AI systems hacked to manipulate national infrastructure ⁴	Threatens national security
		Dual-use science risk	AI systems could accelerate scientific advances but also pose dual-use risks by potentially enabling malicious applications ⁵	Privacy risks, erodes trusts
Risk from malfunction	Risks that arise from unintended failures or errors in AI systems	Risk from product functionality issues	Determining fault/legal liability in autonomous-vehicle accidents ⁶	Legal uncertainty, consumer harm
		Risk from bias and underrepresentation	Facial recognition misidentifying people of colour ⁷	Reinforces systemic inequalities
		Loss of control	AI surpassing human intelligence and operating beyond human ability to control, govern or restrain. ⁸	Destabilises world order









Systemic risks	Risks with broader societal and economic impacts	Labour-market disruption	AI-driven automation leading to significant job losses ⁹	Economic inequality, social unrest
		Global AI divide	Content moderators in low-income countries facing psychological harm ¹⁰	Human-rights violations
		Market concentration and single points of failure	AI technologies become concentrated in a few large companies ¹¹	Reduced competition and innovation
		Environmental risk	High energy and water consumption of AI data centres ¹²	Environmental degradation
		Privacy risk	AI chatbots leaking sensitive user information ¹³	Erodes consumer trust, legal risk, identity theft
		Copyright infringement	AI system generates content after being trained on dataset of copyrighted books, without obtaining proper licences or permissions from the copyright holders ¹⁴	Legal uncertainty and challenges for creative community
Cross-cutting risks	Risks amplified by technical/societal factors	Difficult to assure trustworthiness	Difficulty in proving trust across all use cases due to the general-purpose nature of AI	Outputs that are contextually unsafe despite prior testing
		Immature risk-assessment models	Current evaluation methods for AI systems are underdeveloped and resource intensive	Limited ability to predict or mitigate AI failures at scale
		Increasing autonomy	Autonomous systems reduce human oversight, increasing risks of accidents and malicious use	Autonomous systems acting without accountability
		Competitive pressures	Market competition incentivises speed over safety, increasing risk of insufficient safeguards	Race-to-the-bottom for deploying less-tested AI
		Regulatory lag	Regulations struggle to keep pace with rapid AI advancements	Outdated legal frameworks unable to address emerging risks

Source: International Scientific Report on the Safety of Advanced AI

THE AI LIFECYCLE: REGULATION AND RISK MITIGATION

Figure 3 summarises the components of the AI lifecycle, the importance of regulation in that part of the AI lifecycle and examples of current regulations that are relevant to the components of the AI Regulation Wheel.

Figure 3 – Components of the AI Lifecycle and Associated Risks

COMPONENTS OF THE AI LIFECYCLE	IMPORTANCE FOR REGULATION	INNOVATION PROMOTION	RISK MITIGATION
Input: Gathering and preparing the data that feeds AI systems	High-quality, secure data is the foundation; regulations ensure ethical sourcing, privacy and IP rights to foster unbiased AI	India's National Digital Health Mission 	Brazil's data protection law (LGPD) 
Development: Building and refining AI models through training and testing	Ethical, transparent development is key; regulations set standards for fairness and responsibility in model creation	Canada's Artificial Intelligence and Data Act 	Mexico's proposed Federal AI Regulation 
Output: Deploying AI solutions/models into real-world applications	Safe, reliable AI outputs are crucial; regulations prevent harm and ensure responsible use in critical sectors	UAE's Dubai Financial Services Authority 	EU's Product Liability Directive 
Feedback loop: Monitoring and upgrading the AI systems by taking user feedback as new data input	Ongoing oversight is vital; regulations support compliance and adaptability as technology and risks evolve	Brazil's Data Protection Impact Assessments 	US's proposed Algorithmic Accountability Act 

Footnotes

- 1 <https://www.gov.uk/government/publications/international-scientific-report-on-the-safety-of-advanced-ai>
- 2 <https://www.europol.europa.eu/media-press/newsroom/news/new-report-finds-criminals-leverage-ai-for-malicious-use-%e2%80%93-and-it-%e2%80%99s-not-just-deep-fakes#:~:text=For%20example%2C%20AI%20could%20be%20used%20to%20support%3A,pollution%2C%20by%20identifying%20blind%20spots%20in%20detection%20rules>
- 3 <https://www.bloomberg.com/news/articles/2024-08-07/suspected-foreign-agitators-boost-uk-extremists-to-inflame-riots>
- 4 <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>
- 5 <https://openai.com/index/openai-o1-system-card/>
- 6 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3816158
- 7 <http://gendershades.org/overview.html#>
- 9 <https://futurism.com/the-byte/ai-safety-expert-warning-loss-control>
- 10 <https://www.theguardian.com/technology/2023/aug/02/ai-chatbot-training-human-toll-content-moderator-meta-openai>
- 11 https://www.lemonde.fr/en/economy/article/2024/09/25/ai-is-the-first-technology-to-be-dominated-by-major-players-from-the-outset_6727252_19.html
- 12 <https://www.ft.com/content/b7570359-f809-49ce-8cd5-9166d36a057b>
- 13 <https://www.wired.com/story/openai-custom-chatbots-gpts-prompt-injection-attacks/>
- 14 <https://www.reuters.com/legal/litigation/meta-hit-with-new-author-copyright-lawsuit-over-ai-training-2024-10-02/>