# International Law and Artificial Intelligence: A Structural Readiness Assessment.


## Abstract

Artificial intelligence (AI) has rapidly become embedded in core domains of international concern, from autonomous weapons and cyber operations to biometric border control, digital trade, and financial regulation. While existing debates in international law tend to focus on discrete questions—such as the legality of lethal autonomous weapons or the human-rights implications of algorithmic surveillance—much less attention has been paid to whether the international legal system, as a structure, is ready to govern AI as a cross-cutting phenomenon. This article offers a structural readiness assessment of international law for artificial intelligence. It develops a three-part framework centred on normative coverage (the extent to which existing rules and principles apply to AI-mediated conduct), institutional capacity (the ability of international bodies to interpret, monitor, and enforce those norms), and adaptive flexibility (the system's capacity to adjust to rapid technological change without constant crisis-driven reform). Drawing on doctrinal analysis and case studies relating to autonomous weapons, AI-enabled surveillance, and cross-border algorithmic regulation, the article argues that international law is normatively rich but institutionally thin and procedurally slow in AI-sensitive areas, producing fragmented, reactive, and often ad hoc responses. It concludes that meaningful readiness for AI will depend less on drafting entirely new "AI treaties" and more on clarifying responsibility for AI-mediated harm, strengthening oversight mandates of existing institutions, and developing interpretive principles tailored to algorithmic opacity, explainability, and systemic risk.




## 1. Introduction

The international legal order was not designed with artificial intelligence in mind. The UN Charter, the Geneva Conventions, core human-rights treaties, and the multilateral trade regime emerged in an era when decisions of international significance were taken primarily by human actors, relying on human judgment and responsibility. Today, however, AI systems participate in or shape decisions across a spectrum of activities of direct concern to international law. Militaries experiment with autonomous weapons and AI-assisted targeting; intelligence services and law-enforcement agencies rely on algorithmic analysis for surveillance, risk-assessment, and predictive policing; border authorities deploy biometric and AI-driven systems to manage migration; and economic regulators and private actors use algorithms in high-frequency trading, credit-scoring, and cross-border digital services.

These developments raise familiar doctrinal questions in new guises. Can autonomous weapons comply with the principles of distinction and proportionality in international humanitarian law (IHL)? Are mass algorithmic surveillance programmes compatible with the rights to privacy, freedom of expression, and non-discrimination under international human rights law? How do AI-enabled digital services interact with commitments on data flows, market access, and non-discrimination under trade and investment agreements? And how should responsibility be allocated when AI-mediated conduct causes cross-border harm? A growing body of scholarship and institutional practice addresses these questions within individual regimes. Yet, as with earlier phases of technological disruption, the risk is that international law responds in a piecemeal fashion, treating each issue in isolation and neglecting the structural implications for the system as a whole.

Against this background, the present article asks a different, more systemic question: *is the structure of public international law ready for artificial intelligence?* Instead of focusing exclusively on whether specific AI applications are lawful, it examines whether the combination of norms, institutions, and processes that make up the international legal order is capable of governing AI as a transversal phenomenon. The analysis is guided by a three-part notion of structural readiness: normative coverage, institutional capacity, and adaptive flexibility.

The article does not claim that AI renders existing international law obsolete, nor does it assume that new, AI-specific treaties are always necessary. Its central argument is more nuanced. It contends that international law possesses considerable normative resources to regulate AI-mediated activities but that structural weaknesses in institutional capacity and adaptive flexibility threaten to undermine effective governance, particularly where AI systems are opaque, rapidly evolving, and dominated by private actors. By situating concrete case studies within this broader framework, the article seeks to illuminate not only doctrinal issues but also deeper questions about authority, legitimacy, and accountability in a digitised world.

The article is structured as follows. Section 2 introduces the “diaspora” of AI governance across multiple regimes and institutions, tracing the historical evolution and current landscape of international initiatives on AI. Section 3 outlines the research methodology, combining doctrinal and structural analysis with targeted case studies. Section 4 sets out the theoretical framework, defining structural readiness and linking it to debates on regime complexity and technology governance. Section 5 formulates the research questions. Section 6 reviews the literature on AI and international law, highlighting the need for a structural perspective. Section 7 presents the core analysis of normative coverage, institutional capacity, and adaptive flexibility. Section 8 examines three case studies—autonomous weapons, AI-enabled surveillance, and algorithmic regulation in cross-border economic activity—as concrete sites where these structural issues manifest. Section 9 discusses the broader impact of the identified legal challenges on the

legitimacy and effectiveness of international law. Section 10 concludes with reflections on the conditions under which international law can achieve meaningful readiness for AI.

## 2. Diaspora and Its Background

### 2.1. The dispersed landscape of AI governance

Unlike traditional arms-control treaties or specialised environmental regimes, there is no single, unified "AI convention" that concentrates international legal authority over artificial intelligence. Instead, AI-relevant norms and processes form a dispersed landscape, or diaspora, stretching across different branches of international law and involving a wide range of institutions and actors. This dispersion is partly the product of historical path-dependence: rules dealing with technological issues have accumulated over decades in separate domains such as telecommunications, cybercrime, data protection, trade in services, and human rights.

The emergence of AI as a distinct policy concern has not displaced these pre-existing regimes. Rather, AI has layered itself onto them, accentuating tensions and creating new interdependencies. For example, AI-enabled cyber operations touch on both the law of state responsibility and emerging cyber norms; biometric identification at borders implicates human rights, refugee law, and data-protection principles; and AI in digital trade raises questions about market access, regulatory autonomy, and cross-border data flows under trade agreements. The result is that AI governance at the international level does not start from a blank slate; it is superimposed on a complex architecture of overlapping and sometimes competing rules.

### 2.2. From early tech governance to AI-specific initiatives

International law's engagement with technology predates AI. The early twentieth century saw treaties on telegraphy, radio communications, and aviation; the Cold War era produced nuclear arms-control agreements and regimes governing outer space; the late twentieth century added data-protection instruments such as Council of Europe Convention 108, the Budapest Convention on Cybercrime, and various frameworks on e-commerce and electronic signatures. These instruments established important precedents: they showed that technology-neutral principles could be applied to new tools, but also that specialised regimes might be necessary where risks were acute.

AI entered this picture gradually. Initially, many of its legal implications were treated as extensions of existing debates: autonomous weapons in the context of IHL, AI-driven surveillance in privacy and data-protection law, and algorithmic trading within financial regulation. Over time, however, AI's distinctive features—opacity, autonomy, scalability, and reliance on large data sets—prompted calls for more explicit governance frameworks. This has led to a proliferation of soft-law instruments and emerging treaty processes.

The OECD's 2019 AI Principles were among the first globally endorsed normative statements on AI, articulating values such as human-centred and trustworthy AI, transparency, robustness, and accountability. UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence added a broad, human-rights-oriented framework, covering issues from non-discrimination to environmental impacts. The Council of Europe has since negotiated a Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, which, once in force, will become the first binding international treaty specifically focused on AI. At the same time, the European Union has elaborated the AI Act, a sophisticated risk-based regulatory model with extraterritorial implications that, while not a treaty, will significantly shape cross-border AI governance.

In parallel, UN organs have begun to address AI in various ways. The UN Secretary-General has issued policy briefs on AI and global governance; UN human-rights mechanisms have produced thematic reports on AI and human rights; and debates on autonomous weapons continue under the framework of the Convention on Certain Conventional Weapons (CCW). However, these developments remain fragmented: they occur in different fora, with different memberships, mandates, and procedural rules.

### 2.3. Actors and asymmetries in the AI governance diaspora

The diaspora of AI governance involves an unusually wide array of actors. States are central, but international and regional organisations (UN, Council of Europe, OECD, UNESCO, EU, African Union, among others), technical standard-setting bodies (ISO, IEC, IEEE), and private corporations all participate in norm-creation. Large technology companies and research labs, in particular, exert de facto regulatory influence through their control of infrastructure, algorithms, and data, as well as through corporate codes of conduct and participation in multi-stakeholder initiatives.

This pluralism has both advantages and drawbacks. On the one hand, multiple fora allow experimentation and innovation; different institutions can address different aspects of AI (e.g. ethics, human rights, trade, security). On the other hand, dispersion risks incoherence, duplication, and conflict. It also exacerbates inequalities of participation: states and organisations with greater technical and diplomatic capacity can navigate and shape the emerging landscape more effectively, while others struggle to have their perspectives heard. These asymmetries matter because they influence whose values and interests are embedded in global AI governance.

The dispersed character of AI governance thus forms a crucial background for assessing international law's structural readiness. Any evaluation of normative coverage, institutional capacity, and adaptive flexibility must take into account that AI is regulated not in a single venue but across a constellation of regimes and institutions that interact in complex ways.

## 3. Research Methodology

This article employs a qualitative methodology combining doctrinal legal analysis with structural and institutional assessment, supported by targeted case studies. The aim is not to test hypotheses in a statistical sense but to understand and systematise how international law, as a normative and institutional system, engages with AI-mediated activities.

First, doctrinal analysis focuses on primary sources of international law relevant to AI. These include the UN Charter (particularly provisions on peace and security), the Geneva Conventions and Additional Protocols, core human-rights instruments (such as the ICCPR and ECHR), multilateral and regional trade agreements, and soft-law instruments such as the OECD AI Principles, the UNESCO Recommendation on AI, and the emerging Council of Europe AI Convention. The analysis also considers decisions and opinions of human-rights courts and treaty bodies, as well as relevant reports and resolutions adopted by UN organs and specialised agencies. The doctrinal method is used to identify applicable norms, interpret their scope and content, and evaluate their suitability for regulating AI-mediated conduct.

Second, the study performs a structural and institutional analysis, examining the mandates, procedures, and practices of key international bodies involved in AI-related issues. These include, inter alia, the CCW framework and its Group of Governmental Experts on lethal autonomous weapons systems, UN human-rights mechanisms (treaty bodies, special rapporteurs, and regional courts), economic and technical organisations (such as the WTO, OECD, and ITU where relevant), and emerging AI-specific forums. The analysis assesses their capacity to interpret and enforce norms in AI-sensitive contexts, taking into account jurisdictional limits, resource constraints, expertise, and political dynamics.

Third, the article uses illustrative case studies to ground the structural analysis in concrete practice. The chosen case studies—autonomous weapons and IHL, AI-enabled surveillance and human rights, and algorithmic regulation in cross-border economic activity—were selected based on three criteria: (1) each involves salient AI applications with clear international-law implications; (2) each has generated a significant body of legal and policy debate; and (3) together they span the three broad domains of security, human rights, and economic regulation. The case studies are not intended to be exhaustive; rather, they serve as focal points for exploring how the dimensions of structural readiness play out in practice.

The research also draws extensively on secondary sources, including academic literature on AI and international law, reports by international organisations and expert groups, NGO analyses, and policy briefs. These materials provide context, document institutional practice, and articulate critiques and reform proposals that are relevant to the structural assessment.

Certain limitations should be acknowledged. The rapid pace of AI development and regulation means that the legal and institutional landscape is in flux; new instruments and initiatives may emerge after this article's completion. The focus on global and European practice inevitably under-represents developments in other regions, although the analysis emphasises the importance of broad participation in AI governance. Lastly, the structural emphasis, while essential for the article's aims, leaves less room for detailed exploration of technical AI design choices, which are themselves crucial for effective regulation. Nonetheless, the chosen methodology offers a robust foundation for evaluating international law's readiness for AI in a systematic and conceptually grounded way.

## 4. Theoretical Framework

The theoretical framework of this article is built around the concept of structural readiness. Rather than evaluating individual AI applications solely in terms of compliance with specific rules, structural readiness assesses whether the overall configuration of norms, institutions, and processes in international law is capable of governing AI in a coherent and legitimate manner.

The framework comprises three interrelated components: **normative coverage, institutional capacity,** and **adaptive flexibility.**

Normative coverage refers to the extent to which existing rules and principles of international law apply to AI-mediated activities, and whether they can do so effectively. Many fundamental norms are drafted in technology-neutral terms. The prohibition of the threat or use of force, the principles of distinction, proportionality, and precaution in IHL, and human-rights guarantees of privacy, non-discrimination, and procedural fairness do not depend on the specific tools used. Likewise, trade and investment rules often speak broadly of services, measures, and treatment without differentiating between AI-enabled and traditional activities. From this perspective, AI does not create a legal vacuum. However, AI's distinctive features—such as opacity of decision-making, the speed and scale of automated actions, reliance on large and sometimes biased datasets, and the centrality of private developers and platforms—place stress on existing norms. Questions arise about how to apply due diligence standards to AI-mediated risk, how to assess foreseeability and control when systems learn and adapt, and how to ensure meaningful accountability when harms are distributed across complex socio-technical systems. Normative coverage thus concerns not only whether rules formally apply, but whether they are substantively adequate to address AI's challenges.

Institutional capacity concerns the ability of international institutions to interpret, monitor, and enforce the norms relevant to AI. This includes formal attributes such as jurisdiction, competence, and enforcement powers, as well as practical factors like expertise, resources, and

access to information. For example, the CCW framework has taken up the issue of lethal autonomous weapons systems but remains divided on whether to prohibit, regulate, or merely monitor their development. Human-rights courts and treaty bodies have begun to address AI-related surveillance and profiling, but face difficulties in obtaining evidence about proprietary systems and in crafting general standards. Economic and technical organisations grapple with AI in the context of digital trade and standards, yet often lack explicit human-rights mandates. Institutional capacity also involves the ability to coordinate across regimes and to engage with non-state actors who control much of the relevant technology. Weak or fragmented institutional capacity can leave even well-formulated norms under-enforced.

Adaptive flexibility captures the system's capacity to respond to rapidly evolving technologies without requiring constant formal treaty amendment. In practice, much adaptation occurs through interpretive evolution, soft-law instruments, expert guidelines, and multi-stakeholder processes. Soft law has been particularly prominent in AI governance, as seen in the OECD AI Principles, the UNESCO Recommendation, and various policy frameworks issued by international organisations and regional bodies. These instruments can be adopted relatively quickly and updated as practice develops, but they lack the binding force and institutionalised enforcement mechanisms of treaties. Adaptive flexibility thus involves a trade-off between speed and legal solidity. A system with high adaptive flexibility will generate timely, coherent guidance that shapes behaviour and can be integrated into formal law over time; a system with low flexibility will respond slowly and inconsistently, leaving gaps and uncertainties that actors may exploit.

This framework is informed by debates on regime complexity and fragmentation, which describe how international governance often takes place in regime complexes—sets of partially overlapping and non-hierarchical regimes. AI governance exemplifies this phenomenon: security, human-rights, trade, data-protection, and technical-standardisation regimes all claim some jurisdiction over AI-related issues. This can lead to both innovation and conflict. The notion of structural readiness is therefore relational; it is concerned with how these regimes interact and whether, taken together, they can provide coherent and legitimate governance.

Finally, the framework engages with scholarship on emerging technology governance, which emphasises anticipatory regulation, precaution, and polycentric governance structures. AI challenges traditional assumptions about agency, foreseeability, and control—elements that underpin legal concepts such as fault, intent, and due diligence. Ideas like "meaningful human control" over autonomous systems, "human-rights impact assessments" for AI deployments, and requirements of transparency and explainability can be seen as early attempts by law and policy to internalise AI-specific concerns. By analysing how and where such concepts are

emerging, the article assesses whether international law is evolving towards a more AI-sensitive mode of operation.

In the sections that follow, this theoretical framework underpins both the statement of research questions and the analysis of law and practice in the selected case studies.

## 5. Research Questions

The present study is structured around a primary research question and three interrelated sub-questions, each corresponding to a component of the structural readiness framework developed above. Together, they seek to move beyond isolated doctrinal debates and to produce a more integrated assessment of international law's capacity to govern artificial intelligence.

The **core research question** that guides the analysis is: *To what extent is the current structure of public international law—its norms, institutions, and adaptive processes—capable of governing AI-mediated activities across security, human rights, and economic domains in a coherent, effective, and legitimate manner?* This question is deliberately systemic. It does not ask whether international law is "for" or "against" AI, nor whether a particular application is lawful. Rather, it interrogates the underlying architecture of international law in an era where algorithmic decision-making increasingly shapes decisions of international concern.

From this core inquiry, three **sub-questions** emerge. The first concerns **normative coverage**: *How far do existing rules and general principles of international law already extend to the design, deployment, and effects of AI-driven systems in key domains such as armed conflict, surveillance and border control, and cross-border economic regulation, and where do significant normative gaps or ambiguities arise?* This sub-question examines whether technology-neutral norms—such as due diligence, proportionality, non-discrimination, and procedural fairness—are sufficient, or whether AI's distinct features demand further specification or novel legal concepts.

The second sub-question relates to **institutional capacity**: *Are existing international institutions—security and disarmament fora, human rights courts and treaty bodies, economic and technical organisations, and emerging AI-specific initiatives—equipped, in terms of mandate, expertise, procedure, and enforcement powers, to interpret and implement international norms in relation to AI-mediated activities?* Here the focus is not only on formal jurisdiction but also on practical ability: access to technical knowledge, capacity to compel cooperation, and willingness to confront powerful state and non-state actors.

The third sub-question addresses **adaptive flexibility**: *Through which mechanisms, and with what degree of agility and coherence, does international law adapt to the rapid evolution of AI*

*technologies, and what structural factors facilitate or impede such adaptation?* This inquiry looks at interpretive developments, soft-law instruments, multi-stakeholder processes, and cross-regime coordination as expressions of the system's ability to respond to AI-related challenges without constant formal treaty revision.

These questions are not posed in the abstract. They are operationalised through detailed examination of legal texts, institutional practice, and case studies in subsequent sections. By answering them, the article seeks to illuminate whether international law is merely coping with AI on an ad hoc basis or whether it possess, or can develop, the structural readiness required for long-term governance.

## 6. Literature Review

Scholarship on artificial intelligence and international law is still relatively young, but it has expanded rapidly in recent years. For analytical purposes, it can be divided into several overlapping strands: work on autonomous weapons and the law of armed conflict; analyses of AI-mediated surveillance and human rights; studies of AI, digital trade, and economic regulation; and examinations of global AI governance initiatives and soft law. While each strand is rich in its own right, they tend to proceed in parallel, leaving the structural questions that motivate this article only partially addressed.

A first major strand concerns **autonomous weapons and IHL**. Since the early 2010s, discussions under the Convention on Certain Conventional Weapons (CCW) have focused on whether lethal autonomous weapons systems (LAWS) should be prohibited or regulated, and what "meaningful human control" over targeting decisions should entail. International and regional organisations, including the ICRC and various UN special rapporteurs, have produced influential reports warning that fully autonomous weapons could challenge compliance with the principles of distinction, proportionality, and precaution, as well as undermine meaningful accountability. Academic writers mirror these concerns, debating whether existing IHL is sufficient or whether specific treaty-based bans are necessary. This literature offers valuable insights into how AI might disrupt core security norms but generally stops short of assessing broader institutional and adaptive capacities.

A second corpus addresses **AI-enabled surveillance, profiling, and human rights.** UN human-rights mechanisms and the Council of Europe have warned that AI-driven facial recognition, predictive policing, and biometric border systems risk entrenching discrimination, enabling pervasive surveillance, and eroding due-process guarantees. Reports by the UN High Commissioner for Human Rights have called for moratoria or strict regulation of certain uses of AI that are incompatible with privacy and equality rights, while regional courts have begun to consider cases involving digital surveillance and algorithmic decision-making. Scholars analyse

these developments through the lenses of privacy, non-discrimination, freedom of expression, and access to remedies, often drawing analogies with earlier jurisprudence on mass surveillance and data-retention. Yet, here too, attention tends to remain within the human-rights silo, with less emphasis on how these issues intersect with trade, security, or technical standard-setting.

A growing third strand explores **AI, digital trade, and economic regulation.** WTO-related literature has examined how rules on services, data flows, and non-discrimination apply to AI-enabled platforms, algorithmic services, and cross-border data-intensive business models. Regional trade agreements, particularly those involving digital chapters, increasingly address issues such as source-code disclosure, data localisation, and algorithmic regulation, raising questions about regulatory autonomy and the ability of states to impose transparency or human-rights-oriented requirements on AI-driven services. Scholarship in this area demonstrates that AI does not fit neatly within existing trade categories, but it rarely connects these concerns with parallel debates in security and human-rights regimes.

A fourth body of work deals with **global AI governance and soft-law instruments**. Analyses of the OECD AI Principles, UNESCO's Recommendation, the EU's AI Act, and the Council of Europe's AI convention process highlight emergent consensus around certain values—such as transparency, accountability, and human-centric design—as well as persistent tensions between innovation, regulation, and geopolitical competition. This literature emphasises the role of multi-stakeholder processes, private governance by big technology companies, and the increasing weight of technical standards bodies. It also raises concerns about fragmentation, duplication, and possible "forum-shopping" by states seeking favourable regulatory environments.

Finally, there is an emerging but still thin strand that explicitly contemplates **AI and the structure of international law**. Some authors discuss AI in relation to general principles such as state responsibility and due diligence, or in connection with the concept of jus cogens and peremptory norms, especially in the context of lethal autonomous weapons and systemic surveillance. Others allude to regime complexity and the risk of "siloed" governance, but few attempt a systematic evaluation of normative coverage, institutional capacity, and adaptive flexibility across multiple regimes.

In sum, existing literature offers rich doctrinal and policy analysis of AI within specific legal fields but tends to overlook the cross-cutting structural questions that this article seeks to address. There is a clear need for a study that synthesises insights across these strands and evaluates international law's readiness for AI as a systemic issue, rather than as a series of isolated challenges.

## 7. Analysis

This section applies the structural readiness framework to three key dimensions of international law's engagement with AI: normative coverage, institutional capacity, and adaptive flexibility. It draws on doctrinal material, institutional practice, and the case studies developed in the next section to provide an integrated assessment.

### 7.1. Normative coverage: technology-neutral rules and AI-specific pressures

At first glance, international law appears well-equipped to address AI-mediated activities. Core norms are formulated in broad, technology-neutral terms and apply irrespective of the tools used. The prohibition of the threat or use of force, the principles of distinction and proportionality in IHL, human-rights guarantees of privacy, non-discrimination, and fair trial, and trade rules on services and non-discrimination all cover conduct carried out through AI systems as much as through traditional means. States remain responsible under existing doctrines when they deploy AI in ways that breach these obligations, just as they would be for violations committed with conventional tools.

However, the appearance of sufficiency masks deeper tensions. AI systems introduce new modalities of risk and harm that strain traditional concepts. Opacity, often described as the "black box" problem, can make it difficult to ascertain how an AI system arrived at a particular output, complicating assessments of intent, foreseeability, and negligence. Machine-learning models may evolve in deployment, creating a moving target for regulation. When AI systems interact in complex digital environments, chains of causation become diffuse: harms may emerge from a combination of design choices, training data, deployment contexts, and user behaviour. Existing doctrines of state responsibility and due diligence must therefore operate in a context where attribution of specific decisions to individual human agents is less straightforward, and where control is shared between states and private developers or platforms.

In the security domain, debates on lethal autonomous weapons highlight these concerns. While IHL principles remain applicable, serious doubts exist about whether autonomous systems can reliably distinguish combatants from civilians, assess proportionality, or react appropriately to dynamic battlefield conditions without human judgment. The very notion of "meaningful human control" is contested, and existing treaty language does not specify the degree or quality of human involvement required. In human-rights law, AI-driven surveillance and profiling raise questions about what constitutes "arbitrary" or "unlawful" interference with privacy when data collection and analysis become ubiquitous and continuous.
Non-discrimination norms must grapple with algorithmic bias embedded in training data and

model design, often in ways that evade traditional categories of direct or indirect discrimination.

In economic law, AI-enabled services complicate the application of definitions and commitments negotiated before such technologies existed. The classification of AI-driven platforms and services for purposes of market-access commitments, the treatment of algorithmic transparency requirements as potential trade barriers, and the interaction between data-localisation rules and AI's data needs all expose grey areas in trade and investment law.

Overall, normative coverage is substantial but incomplete. International law has the conceptual tools to address AI in many areas, yet the specificity and clarity of those tools may be insufficient for consistent application. Emerging soft-law instruments and interpretive efforts can be seen as attempts to fill this gap, signalling an evolving, but still uneven, normative landscape.

### 7.2. Institutional capacity: mandates, expertise, and enforcement

Even where norms exist, the capacity of institutions to apply and enforce them in AI-related contexts is uneven. The CCW's Group of Governmental Experts on lethal autonomous weapons has, over several years, produced guiding principles and ongoing discussions but has not yet agreed on a legally binding outcome, reflecting deep divisions among states about the desirability and feasibility of a prohibition or strict regulation. Its mandate, the need for consensus, and the complexity of technical issues limit its ability to move from general principles to concrete, enforceable rules.

Human-rights institutions have been more active in addressing AI. UN special rapporteurs and the Office of the High Commissioner for Human Rights have issued detailed reports on AI and human rights, calling for moratoria on certain uses and for robust safeguards in others. Regional courts and treaty bodies have begun to interpret existing rights in light of digital surveillance and algorithmic decision-making, sometimes grounding their reasoning in broader principles of the rule of law and democratic oversight. Nonetheless, they often face evidentiary challenges when dealing with proprietary AI systems, lack direct access to technical expertise, and rely heavily on submissions from states and civil society for information about system design and impact. Their decisions may have strong persuasive authority but limited direct enforcement power, especially beyond their regional scope.

Economic and technical organisations occupy a more ambiguous position. Bodies involved in trade, standards, and telecommunications have significant influence over the conditions under which AI systems are designed and deployed, but their mandates frequently emphasise efficiency, interoperability, and trade facilitation rather than human-rights or security concerns. Coordination between these institutions and human-rights or security bodies is limited and

often informal. Emerging AI-specific forums and initiatives—whether under the OECD, UNESCO, or ad hoc multi-stakeholder platforms—can develop sophisticated guidance but lack the authority to impose binding obligations.

Institutional capacity is thus characterised by fragmentation and asymmetry. Some institutions are norm-rich but enforcement-poor; others have technical influence but weak human-rights mandates. Few possess a combination of strong jurisdiction, robust enforcement mechanisms, and deep technical expertise oriented explicitly toward AI governance. This structural weakness risks leaving AI-mediated harms inadequately addressed, particularly where powerful states or corporations are involved.

### 7.3. Adaptive flexibility: soft law, experimentation, and inertia

With respect to adaptive flexibility, the picture is mixed. On the one hand, international law has seen a proliferation of soft-law instruments, guidelines, and principles that address AI more rapidly than formal treaties could. The OECD AI Principles, the UNESCO Recommendation, and numerous policy frameworks at regional level demonstrate a willingness to engage with AI in a forward-looking manner. These instruments can be updated over time, serve as references for domestic legislation, and influence corporate practices, especially where they are backed by major economies and institutions.

On the other hand, the reliance on soft law and interpretive evolution creates risks of fragmentation and variable implementation. Without binding force or strong monitoring mechanisms, adherence to AI principles can be uneven, and their integration into hard law is neither automatic nor guaranteed. Moreover, formal treaty-making on AI—such as the Council of Europe's AI convention—proceeds slowly and may be limited in geographic reach. Security-related processes, such as those concerning autonomous weapons, struggle to keep pace with technological developments, leading to a sense that "law always arrives late" in the face of emerging capabilities.

Institutional inertia, geopolitical rivalry, and the complexity of AI itself all constrain adaptive flexibility. States may be reluctant to agree to stringent international standards that they fear could limit their strategic or economic advantages. Multi-stakeholder processes can include diverse perspectives but sometimes lack clear decision-making authority. Technical expertise, while increasingly integrated into governance discussions, remains unevenly distributed and is often concentrated in the private sector.

Taken together, these factors suggest that international law's adaptive flexibility in relation to AI is present but fragile. The system can generate soft-law responses and interpretive developments, but structural obstacles may prevent these from coalescing into a coherent and sufficiently robust governance framework. The following case studies illustrate how these

dynamics play out in practice, and how legal challenges in specific domains reflect the broader structural issues identified in this section.

## 8. Case Studies

This section examines three illustrative case studies that bring into focus the dynamics of normative coverage, institutional capacity, and adaptive flexibility discussed above. They are not exhaustive of all AI-related challenges in international law, but they represent key domains—security, human rights, and economic regulation—where structural tensions are particularly visible.

### 8.1. Autonomous weapons and the law of armed conflict

Debates on lethal autonomous weapons systems (LAWS) have become one of the most prominent intersections between AI and international law. LAWS are generally understood as weapons systems that, once activated, can select and engage targets without further human intervention. The prospect of delegating life-and-death decisions to machines has triggered intense legal, ethical, and political controversy.

From a normative coverage perspective, IHL applies fully to the use of LAWS. Parties to armed conflict remain bound by the principles of distinction, proportionality, and precaution, as well as by customary rules governing weapons that are indiscriminate or cause unnecessary suffering. States deploying LAWS would be responsible for ensuring that such systems can comply with these obligations in practice. Article 36 of Additional Protocol I requires legal reviews of new weapons to determine their compatibility with international law, a provision that applies equally to AI-enabled systems.

Nevertheless, the application of these norms is contested. Critics argue that current or foreseeable AI technology cannot reliably distinguish combatants from civilians in complex environments, particularly where civilians and fighters intermingle or where contextual judgment is required. They question whether autonomous systems can make proportionality assessments that require qualitative evaluation of expected military advantage versus collateral harm, or adequately interpret dynamic battlefield signals indicating surrender or incapacitation. Proponents contend that, in some contexts, autonomous systems might be more precise than humans, reducing error and emotional bias. The lack of explicit AI-specific rules in IHL leaves considerable discretion to states in interpreting their obligations.

As to institutional capacity, the CCW framework and its Group of Governmental Experts (GGE) have become the primary forum for multilateral discussion. The GGE has agreed on guiding principles, including that IHL continues to apply to all weapons systems and that humans remain responsible for decisions on the use of force. However, it has not reached consensus on a legally

binding instrument prohibiting or strictly regulating LAWS. A number of states and civil-society coalitions advocate for a pre-emptive ban, while others favour continued monitoring, arguing that existing law suffices. The CCW's consensus-based decision-making and its limited enforcement mechanisms constrain its ability to produce strong, binding outcomes. The ICRC and UN officials have urged states to adopt clear constraints on autonomy in weapons systems, but these recommendations lack direct legal effect.

Regarding adaptive flexibility, the LAWS debate demonstrates both innovation and inertia. On the one hand, the very existence of the GGE and the rapid development of normative concepts such as "meaningful human control" show that states and institutions can respond proactively to emerging technologies. On the other hand, the slow progress toward binding rules, despite years of discussion and accelerating technological development, exemplifies the problem of law lagging behind technological change. The absence of clear global standards risks a scenario in which some states unilaterally develop and deploy increasingly autonomous weapons, creating pressure on others to follow and making future regulation harder.

Overall, the LAWS case reveals substantial normative coverage but contested interpretation, limited institutional capacity to translate debates into binding rules, and only partial adaptive flexibility in the face of rapid technological advancement.

### 8.2. AI-enabled surveillance and international human rights law

The second case study concerns AI-driven surveillance, profiling, and decision-making in areas such as law enforcement, border control, and social-media monitoring. States and private actors increasingly deploy facial-recognition systems, predictive policing tools, and algorithmic analysis of online content. These practices raise core human-rights issues, particularly regarding privacy, non-discrimination, freedom of expression, and access to effective remedies.

In terms of normative coverage, international human-rights treaties already provide robust protection against arbitrary or unlawful interference with privacy, discriminatory treatment, and unjustified restrictions on expression and movement. The ICCPR, for example, protects the right to privacy and family life and prohibits discrimination on various grounds. Regional instruments, such as the European Convention on Human Rights, contain analogous protections and have generated extensive jurisprudence on surveillance, data retention, and secret-service activities. These norms apply irrespective of whether surveillance is conducted through human agents or AI-enabled systems.

However, AI-enabled surveillance introduces new forms of risk. Large-scale facial-recognition systems can track individuals across multiple contexts and datasets, creating pervasive, continuous monitoring. Predictive policing tools trained on historical crime data may reproduce and reinforce existing biases, disproportionately targeting certain communities. Algorithmic

content moderation and recommender systems can shape access to information and public discourse in opaque ways. Traditional human-rights tests—such as whether an interference is lawful, pursues a legitimate aim, and is necessary and proportionate—must now be applied to complex socio-technical systems whose functioning is not easily understandable.

With respect to institutional capacity, human-rights mechanisms have begun to respond. UN special rapporteurs have issued reports expressing concern about AI-driven surveillance, recommending moratoria on certain uses, and calling for strict safeguards and human-rights impact assessments. Regional courts have extended existing surveillance jurisprudence to digital contexts, emphasising the need for clear legal bases, independent oversight, and effective remedies. Yet, many of these bodies face practical limitations: they depend on information provided by states and civil-society organisations, may lack in-house technical expertise, and cannot directly compel disclosure of proprietary algorithms or training data. Remedies are often individual and retroactive, whereas AI-enabled surveillance is systemic and ongoing.

The adaptive flexibility of human-rights law in this area is both promising and incomplete. On the one hand, interpretive developments—such as recognition of the chilling effect of mass surveillance on expression and association, and acknowledgment of algorithmic bias as a form of discrimination—show that human-rights bodies can adapt existing norms to new technologies. On the other hand, the absence of binding, AI-specific human-rights instruments and the reliance on case-by-case adjudication may lead to uneven standards and enforcement. Some states embrace robust safeguards; others use AI tools in ways that evade scrutiny or rely on opaque security justifications.

Thus, while human-rights law offers strong normative foundations, institutional capacity and adaptive mechanisms are still catching up with the scale and complexity of AI-enabled surveillance.

### 8.3. AI, algorithms, and cross-border economic regulation

The third case study explores AI's role in cross-border economic activity, particularly digital trade, algorithmic decision-making in services, and data-driven business models. AI is now integral to e-commerce platforms, cloud-based services, algorithmic trading, and personalised advertising, all of which operate across borders and fall within the ambit of trade and investment rules.

From a normative coverage standpoint, WTO agreements and regional trade treaties regulate trade in goods and services, intellectual property, and related aspects of digital commerce. However, most of these instruments were negotiated before AI became central to digital services. Commitments on services often refer to modes of supply without distinguishing

between human-provided and algorithmically delivered services. Provisions on non-discrimination, market access, and domestic regulation apply, but their interaction with AI-specific measures is not always clear. For example, requirements that firms disclose information about their algorithms, ensure explainability, or maintain certain data within national borders may be characterised as barriers to trade or investment, even when motivated by human-rights or security concerns.

In terms of institutional capacity, economic tribunals and dispute-settlement bodies have not yet developed a substantial body of case law on AI-specific measures. Nonetheless, emerging disputes over data localisation, access to source code, and cross-border digital services suggest that such cases are likely. Technical standard-setting bodies (such as ISO and IEC) and economic organisations (like the OECD and WTO) influence the conditions under which AI systems operate through standards, guidelines, and trade rules, yet their mandates typically prioritise trade facilitation and interoperability over human-rights or security considerations. Coordination with human-rights or security bodies is limited, raising the risk that AI-relevant trade rules may conflict with other international obligations or hinder domestic regulation aimed at ensuring trustworthy AI.

Regarding adaptive flexibility, digital trade negotiations and plurilateral initiatives on e-commerce have begun to include provisions on source-code and algorithmic disclosure, data flows, and localisation. Some of these proposals seek to restrict states' ability to demand access to algorithms or to impose data-localisation requirements, reflecting concern about protectionism but potentially constraining regulatory space for AI oversight. Soft-law frameworks on trustworthy AI from economic organisations can encourage good practices but lack binding force. The absence of a clear, integrated approach to AI in trade and investment law underscores the structural challenge: economic rules are adapting to digitalisation, but not always in ways that account for the broader governance needs of AI.

This case study thus illustrates how AI interacts with economic regimes that were not designed with such technologies in mind, raising questions about normative coherence, institutional role allocation, and the balance between trade facilitation and regulatory autonomy.

## 9. Impact of Legal Challenges

The legal challenges identified in the preceding analysis and case studies have significant implications for the legitimacy, effectiveness, and coherence of international law in the age of AI. They also affect how states, individuals, and private actors perceive and engage with the international legal order.

### 9.1. Legitimacy and trust in international institutions

Structural shortcomings in normative clarity, institutional capacity, and adaptive flexibility can erode the perceived legitimacy of international law. When autonomous weapons debates stall despite widespread ethical concern, when AI-enabled surveillance appears to outpace human-rights oversight, or when trade rules seem to constrain legitimate regulation of AI, affected communities may question whether international institutions are capable of protecting fundamental values in a digitised world.

This legitimacy deficit can have self-reinforcing effects. States may become less willing to accept international scrutiny or to invest in strengthening institutions they perceive as ineffective. Individuals and civil-society organisations may turn to domestic courts or political advocacy rather than international mechanisms. Private actors, particularly large technology companies, may fill governance gaps through self-regulation, further privatising normative choices that ought to be subject to public oversight.

### 9.2. Accountability gaps and unequal protection

AI's deployment in security, surveillance, and economic systems can exacerbate existing accountability gaps. If international law struggles to attribute responsibility for AI-mediated harm—because of diffuse causal chains, shared control between states and private entities, or limited access to technical evidence—victims may find it difficult to obtain remedies at national or international levels.

Moreover, structural inequalities in participation and capacity mean that not all states are equally able to shape AI governance or to protect their populations from harmful uses. Wealthier states and corporations often lead in AI development and standard-setting, while many developing countries must accept imported technologies and governance frameworks with limited influence over their design. This can entrench imbalances in power and protection, with residents of some regions more likely to be subjected to unregulated surveillance, experimental systems, or exploitative economic models.

If left unaddressed, these accountability and equity concerns risk undermining the universality and fairness that international law claims as core attributes.

### 9.3. Fragmentation, forum-shopping, and regulatory arbitrage

The dispersed nature of AI governance and the uneven development of norms and institutions create opportunities for fragmentation and strategic behaviour. States and private actors may engage in forum-shopping, selecting the most favourable venue or regime for advancing their interests—whether in trade negotiations, technical standard-setting, or security forums.

Regulatory arbitrage becomes easier when there is no clear, coherent framework for AI across regimes. Companies may locate data or operations in jurisdictions with weaker oversight, while still benefiting from cross-border markets. States may invoke security or trade justifications selectively to resist human-rights-oriented constraints. Such behaviour can further erode coherence and undercut efforts by more ambitious regulators to enforce higher standards.

### 9.4. Prospects for structural reform

At the same time, the challenges highlighted in this article create pressure for structural reform. Calls for clearer allocation of responsibility in AI-related harms, stronger human-rights mandates for technical and economic bodies, more robust oversight mechanisms for AI deployment in security and surveillance, and better coordination across regimes reflect a growing awareness that fragmented governance is inadequate.

Efforts such as the Council of Europe's AI convention, ongoing debates under the CCW, and the integration of AI considerations into human-rights and trade bodies illustrate attempts to move toward more coherent frameworks. Whether these initiatives will coalesce into a genuinely structural response depends on political will, the willingness of states to accept constraints on strategic and commercial interests, and the capacity of international institutions to integrate technical expertise and diverse perspectives.

## 10. Conclusion

Artificial intelligence does not confront international law with an entirely new universe; rather, it amplifies and accelerates existing tensions about authority, accountability, and the relationship between technology and human dignity. This article has offered a structural readiness assessment of international law for AI, focusing on three dimensions: normative coverage, institutional capacity, and adaptive flexibility.

The analysis suggests that international law is normatively rich: core principles in IHL, human-rights law, and economic law already apply to many AI-mediated activities and provide meaningful constraints in theory. However, AI's distinctive characteristics—opacity, complexity, speed, and reliance on private actors—strain the application of these norms and expose areas where greater specificity or new interpretive tools are needed.

Institutional capacity is more uneven and fragile. Security fora, human-rights bodies, economic organisations, and technical standard-setters all play roles in AI governance but often operate with limited mandates, incomplete expertise, and modest enforcement powers. Coordination across regimes remains ad hoc. As a result, even where norms exist, their implementation and enforcement in AI-related contexts can be inconsistent and incomplete.

Adaptive flexibility, finally, is present but constrained. Soft-law instruments, expert guidelines, and interpretive developments show that international law can respond to AI more quickly than formal treaty-making would allow. Yet, structural obstacles—including consensus-based procedures, geopolitical competition, and institutional inertia—limit the speed and coherence of this adaptation.

The case studies on autonomous weapons, AI-enabled surveillance, and cross-border economic regulation illustrate these dynamics in concrete settings. They reveal persistent accountability gaps, legitimacy concerns, and risks of fragmentation, but also sites of innovation where new concepts and processes are emerging.

The article therefore concludes that international law is neither obsolete in the face of AI nor fully prepared. Its structural readiness is a moving target. To improve it, states and international institutions should prioritise:

- Clarifying responsibility for AI-mediated harm, including the duties of states to regulate private developers and platforms.
- Strengthening the mandates, resources, and technical expertise of existing bodies that oversee AI-relevant norms, particularly in human-rights and security contexts.
- Developing cross-cutting interpretive principles—such as transparency, explainability, human-rights impact assessment, and meaningful human control—that can be integrated into multiple regimes.
- Enhancing coordination between security, human-rights, trade, and technical-standards bodies to reduce fragmentation and regulatory arbitrage.

Ultimately, whether international law becomes genuinely ready for artificial intelligence will depend on political choices. AI can either reinforce an international order marked by inequality, opacity, and contestation, or it can act as a catalyst for renewing commitments to human rights, the rule of law, and shared responsibility in a technologically complex world.

## 11. References


1. OECD. (2019). *OECD Principles on Artificial Intelligence*. OECD Publishing. https://www.oecd.org/sti/artificial-intelligence/policies/oecd-principles-on-artificial-intelligence.htm
2. UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000380455

3. Council of Europe. (2024). *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. Council of Europe Treaty Series No. 235. https://www.coe.int/en/web/artificial-intelligence/cai-convention
4. Office of the United Nations High Commissioner for Human Rights (OHCHR). (2021). *The Right to Privacy in the Digital Age: Report of the Special Rapporteur on the Right to Privacy*. A/HRC/48/31. https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-report-special-rapporteur-right-privacy-right-privacy-digital-age
5. International Committee of the Red Cross (ICRC). (2018). *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*. ICRC Report. https://www.icrc.org/en/document/autonomous-weapon-systems-implications-increasing-autonomy-critical-functions-weapons
6. United Nations. (1969). *Vienna Convention on the Law of Treaties*. United Nations Treaty Series, vol. 1155, p. 331. https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf
7. International Committee of the Red Cross (ICRC). (2005). *Measures to Implement Article 36 of Additional Protocol I of 1977*. ICRC Expert Meeting Report. https://international-review.icrc.org/sites/default/files/irrc_864_11.pdf
8. Cortright, D., & Lopez, G. A. (2000). *The Sanctions Decade: Assessing UN Strategies in the 1990s*. Lynne Rienner Publishers.
9. Farrall, J. M. (2007). *United Nations Sanctions and the Rule of Law*. Cambridge University Press.
10. Hovell, D. (2016). *The Power of Process: The Value of Due Process in Security Council Sanctions Decision-Making*. Oxford University Press.
11. Reinisch, A. (2001). "Securing the Effects of Security Council Sanctions: The Need for a Full Judicial Review." *European Journal of International Law*, 12(4), 795–819.
12. Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*. W.W. Norton & Company.
13. Yeung, K., & Lodge, M. (2019). "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance*, 12(4), 505–523.
14. United Nations Secretary-General. (2021). *Our Common Agenda: Report of the Secretary-General*. A/75/982. https://www.un.org/en/content/common-agenda-report/
15. International Committee of the Red Cross (ICRC). (2017). *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects*. ICRC Expert Meeting Report. https://www.icrc.org/en/document/autonomous-weapon-systems-technical-military-legal-and-humanitarian-aspects
16. European Court of Human Rights. (2020). *Big Brother Watch and Others v. United Kingdom* (Application nos. 58170/13, 62322/14 and 24960/15). Judgment.
17. United Nations General Assembly. (2023). *Resolution on Human Rights and Artificial Intelligence*. A/RES/78/XXX (forthcoming or related resolutions).

18. World Trade Organization. (2021). *Digital Trade Developments*. WTO Report. https://www.wto.org/english/res_e/booksp_e/digital_trade_2021_e.pdf
19. Alter, K. J., & Raustiala, K. (2018). "The Rise of International Regime Complexes." *American Journal of International Law*, 112(3), 417–464.
20. Drezner, D. W. (2011). "Sanctions Sometimes Smart: Targeted Sanctions in Theory and Practice." *International Studies Review*, 13(1), 96–108.