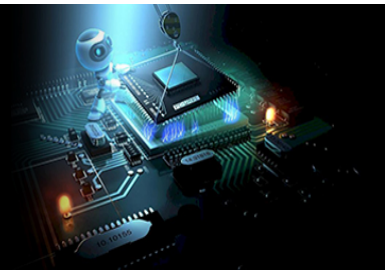
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
Impact Factor (RJIF): 5.52
www.computersciencejournals.com/ijecs
IJECS 2026; 8(2): 38-47
Received: 12-02-2026
Accepted: 14-03-2026

Sandeep Kumar Nayak
Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, Uttar Pradesh India

Corresponding Author:
Sandeep Kumar Nayak
Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, Uttar Pradesh India

The evolving frontier of national and international cyber law (2020–2026)

Sandeep Kumar Nayak

DOI: https://www.doi.org/10.33545/26633582.2026.v8.i2a.275

Abstract
Between 2020 and 2026, the landscape of cyber law underwent a fundamental paradigm shift, transitioning from fragmented national policies toward integrated, legally binding international frameworks. Driven by the COVID-19 pandemic's digital acceleration and the emergence of generative Artificial Intelligence (AI), this period witnessed the adoption of the first United Nations Cybercrime Convention and a decisive global move toward "digital sovereignty." Drawing on a cross-jurisdictional analysis of the European Union, the United States, and the United Kingdom, this paper examines critical legislative milestones including the EU Cyber Solidarity Act, the US NIST Cybersecurity Framework (CSF) 2.0, and South Africa's Cybercrimes Act alongside persistent challenges such as jurisdictional creep, the privacy-security paradox, and AI governance gaps. The paper argues that while international legal coordination has advanced significantly, the tension between national sovereignty and the borderless nature of cyber threats remains the central challenge for the next decade of digital law.

Keywords: Cyber law, Artificial Intelligence (AI) governance, privacy-security balance, jurisdictional creep, digital sovereignty

1. Introduction
The early 2020s marked a decisive turning point for global digital governance. The COVID-19 pandemic forced a rapid migration of critical infrastructure, government services, and corporate operations to digital environments, fundamentally reshaping the threat landscape. By 2022, organizations worldwide experienced a substantial year-on-year increase in cyberattacks, with ransomware attacks alone rising by over 40% in the same period [1, 4]. Remote work arrangements, accelerated cloud adoption, and the exponential expansion of Internet of Things (IoT) devices dramatically expanded the attack surface, creating vulnerabilities that malicious actors were quick to exploit [3].

As Chawki observes, this surge necessitated more robust legal responses to address both "cyber-dependent" crimes such as ransomware, malware, and denial-of-service attacks and "cyber-enabled" crimes, including financial fraud, identity theft, and phishing schemes. Traditional legal frameworks, largely designed for a pre-digital era, proved ill-equipped to handle the scale, speed, and cross-border nature of contemporary cyber threats. The Budapest Convention on Cybercrime (2001), while influential as the first multilateral treaty addressing cybercrime, suffered from limited membership and lacked universal ratification, leaving significant gaps in global legal cooperation [2].

Yet the challenge extends beyond mere threat proliferation. As Chawki [2] frames it, the central dilemma of contemporary cybersecurity governance lies in reconciling national security imperatives with individual privacy rights a tension that has intensified with the deployment of AI in surveillance, threat detection, and automated decision-making. Governments increasingly invoke national security justifications to expand surveillance powers, mandate data retention, and compel private sector cooperation. Simultaneously, citizens and civil society organizations demand stronger privacy protections, transparency, and accountability mechanisms. This friction has generated numerous legal challenges, including high-profile court cases such as Schrems II (2020), which invalidated the EU-US Privacy Shield, and ongoing debates over mass surveillance programs under the USA PATRIOT Act and Foreign Intelligence Surveillance Act (FISA) amendments.

The period 2020–2026 also witnessed the emergence of transformative technologies that

Outpaced existing regulatory frameworks. Generative AI, particularly Large Language Models (LLMs), became widely accessible, raising novel questions about data provenance, algorithmic bias, misinformation, and liability for AI-generated content. Nation-state actors and cybercriminal organizations began leveraging AI to automate phishing campaigns, generate deepfakes, and evade traditional detection systems. In response, regulators scrambled to develop governance frameworks from the EU's AI Act to sector-specific guidelines in healthcare, finance, and critical infrastructure.

This paper explores how national and international legal frameworks evolved between 2020 and 2026 to address four critical questions, originally articulated by Chawki [2] but contextualized within this specific timeframe: (R1) how can national security imperatives be effectively balanced with the right to individual privacy in the context of cybersecurity governance? (R2) Do existing legal frameworks sufficiently regulate the use of artificial intelligence and data-sharing practices to protect personal privacy, particularly in light of rapid technological advancement? (R3) What is the role of public-private partnerships in building cybersecurity resilience, and how can accountability be achieved in such partnerships without eroding privacy protections? (R4) How can artificial intelligence technologies be leveraged to protect digital infrastructures and detect threats without infringing upon individual rights and fundamental freedoms?

To answer these questions, this paper adopts a qualitative, interdisciplinary legal-tech methodology grounded in comparative analysis. It examines three primary jurisdictions the European Union, the United States, and the United Kingdom each representing distinct regulatory philosophies: the EU's rights-based, supranational approach under the General Data Protection Regulation (GDPR); the US's security-oriented, sectoral model; and the UK's hybrid framework balancing intelligence imperatives with procedural safeguards. The analysis draws on peer-reviewed academic literature, legislative instruments, regulatory enforcement actions, judicial decisions, and policy white papers published between 2013 and 2025, as well as specific legal milestones enacted between 2020 and 2026.

The remainder of this paper is structured as follows. Section 2 examines international frameworks, focusing on the UN Convention against Cybercrime (2024) and EU solidarity mechanisms. Section 3 analyzes national legislative trends across selected jurisdictions, highlighting the tension between digital sovereignty and cross-border interoperability. Section 4 addresses emerging challenges, including AI governance, the privacy paradox in information sharing, and jurisdictional creep. Section 5 presents case studies of effective and ineffective information-sharing practices. Section 6 outlines recommended legal frameworks for equitable cybersecurity governance. Section 7 concludes with implications for future research and policy development.

2. International Frameworks: A Move toward Multilateralism

The most significant development in international law during the period 2020–2026 was the transition from voluntary, non-binding norms toward legally binding treaties and enforceable regional mechanisms. Prior to this period, international cybersecurity governance relied primarily on soft-law instruments, bilateral agreements, and sector-specific guidelines that suffered from inconsistent adoption and weak enforcement. The Budapest Convention on Cybercrime (2001), while influential as the first multilateral treaty addressing cybercrime, counted only 66 state parties by 2020 and faced criticism for excluding meaningful participation from developing nations, particularly from Africa, Asia, and South America [2, 12].

The years 2020–2026 witnessed a decisive shift toward what Chawki [2] terms a "regime complex" a collection of partially overlapping norms and institutions functioning across multiple levels of authority, from international treaties to technical protocol standards. This section examines three interconnected developments: (1) the United Nations Convention against Cybercrime (2024), representing the first universal cybercrime treaty; (2) the European Union's emerging solidarity and resilience framework, including the Cyber Solidarity Act and Cyber Resilience Act; and (3) the reaffirmation and application of existing international law to the cyber domain.

2.1 UN Convention against Cybercrime (2024)

2.1.1 Historical Context and Negotiation Process

The United Nations Convention against Cybercrime, adopted on December 24, 2024, represents a landmark achievement in international digital governance [5]. Negotiations began under the auspices of the UN Ad Hoc Committee on Cybercrime, which convened seven substantive sessions between January 2022 and March 2024. Unlike the Budapest Convention, which was drafted primarily by Western industrialized nations, the UN Convention emerged from a more inclusive process that explicitly sought input from developing countries, civil society organizations, and private sector stakeholders.

The convention addresses a long-standing criticism of previous international instruments: the absence of universal participation. As Sharma [6] observes, the UN framework deliberately incorporates provisions for technical assistance, capacity building, and resource sharing to enable developing nations to implement effective cybercrime legislation and enforcement mechanisms. This represents a recognition that cybercrime is a global problem requiring genuinely global solutions, and that legal harmonization cannot succeed without corresponding investment in institutional capacity.

2.1.2 Key Provisions and Mechanisms

The UN Convention against Cybercrime establishes several innovative mechanisms that distinguish it from previous international instruments.

24/7 Network for Mutual Legal Assistance: The convention mandates that each state party establish a point of contact available twenty-four hours a day, seven days a week, to facilitate expedited cooperation in cybercrime investigations. This network enables rapid preservation of electronic evidence, emergency mutual legal assistance requests, and real-time information sharing across jurisdictions. Unlike traditional mutual legal assistance processes, which often take months or years, the 24/7 network is designed to operate on timescales relevant to cybercrime investigations typically hours or days.

Criminalization Framework: The convention requires state parties to criminalize a comprehensive range of cyber-

dependent and cyber-enabled offenses, including: illegal access to computer systems; illegal interception of non-public data transmissions; system interference (including the deliberate introduction of malware); data interference (alteration, damage, or suppression of data); misuse of devices (including passwords and other access credentials); computer-related forgery and fraud; and offenses related to child sexual exploitation material. Additionally, the convention addresses ransomware attacks explicitly, recognizing them as a distinct and particularly harmful category of cybercrime requiring specific legal responses.

Jurisdictional Provisions: The convention establishes multiple bases for jurisdiction, including territoriality (offenses committed within a state's territory), active personality (offenses committed by a state's nationals), and passive personality (offenses committed against a state's nationals) the latter being a controversial provision discussed further in Section 4.3. The convention also includes provisions for extraterritorial jurisdiction in cases where the offense affects a state's essential security interests [11].

Electronic Evidence Provisions: Recognizing the volatility of electronic evidence, the convention authorizes expedited preservation of stored computer data, expedited disclosure of traffic data, and production orders requiring the submission of subscriber information. These provisions balance law enforcement needs with privacy protections by requiring judicial authorization for more intrusive measures and limiting mandatory data retention to specified categories.

2.1.3 Ratification Status and Implementation Challenges

As of early 2026, the convention had garnered over 80 signatories, with ratification progressing most rapidly among African, Asian, and Latin American nations precisely the regions least represented under the Budapest regime. However, implementation challenges remain substantial. As Chawki [2] notes, the gap between normative commitments and enforcement capacity is particularly acute in developing nations, where cybersecurity agencies may lack technical expertise, forensic capabilities, and legal infrastructure necessary to comply with convention obligations.

Kumar [7] highlights three persistent challenges: (1) diverging domestic legal frameworks regarding evidentiary standards, privacy protections, and due process rights; (2) insufficient technical capacity for digital forensics and cross-border evidence exchange in many state parties; and (3) political disagreements regarding the scope of lawful surveillance and data retention obligations. These challenges suggest that while the convention represents a milestone in norm-setting, its practical effectiveness will depend on sustained investment in capacity building and technical assistance.

2.2 European Union: Solidarity and Resilience

Alongside the UN process, the European Union emerged as a particularly influential actor in cybersecurity governance, leveraging its regulatory authority to establish binding frameworks that transcend the voluntary nature of many international instruments. As Chawki [2] observes, the European model grounds regulation in human dignity and proportionality principles, conceptualizing privacy and cybersecurity as extensions of individual personality under the Charter of Fundamental Rights. This normative orientation, combined with robust enforcement mechanisms including independent Data Protection Authorities and the Court of Justice of the European Union enables the EU to impose meaningful consequences for non-compliance [12].

2.2.1 The Cyber Solidarity Act (Regulation 2025/38)

The Cyber Solidarity Act, formally adopted in early 2025, establishes a supranational mechanism for detecting, preparing for, and responding to large-scale cyber threats [7]. The regulation creates three interconnected pillars.

European Cyber Shield: This pillar establishes a network of national and cross-border Security Operations Centers (SOCs) across all member states. These SOCs employ advanced AI and machine learning technologies to detect cyber threats in near real-time, share threat intelligence across national borders, and coordinate incident response. The Shield builds upon existing initiatives such as the Cybersecurity Act (2019) and the Network and Information Security (NIS2) Directive but ads dedicated funding and mandatory participation requirements.

Cyber Emergency Mechanism: The regulation establishes a standby response capacity comprising private sector incident response teams that can be deployed at the request of any member state experiencing a significant cyber incident. The mechanism is financed through the EU budget, with contributions from participating member states, and includes provisions for coordinated procurement of cybersecurity services and technologies.

European Cybersecurity Incident Review Mechanism: Following major incidents, the regulation mandates independent reviews to identify root causes, extract lessons learned, and issue recommendations for improving EU-wide cybersecurity posture. These reviews are conducted by the European Union Agency for Cybersecurity (ENISA) in coordination with affected member states and relevant private sector entities.

As Cambridge Core [7] notes, the Cyber Solidarity Act represents a significant shift from voluntary cooperation to legally binding solidarity obligations among member states. However, the regulation has attracted criticism regarding data sharing and privacy, as cross-border threat intelligence exchange necessarily involves processing potentially sensitive information.

2.2.2 The Cyber Resilience Act (Regulation 2024/2847)

Adopted in late 2024, the Cyber Resilience Act imposes mandatory cybersecurity requirements for all products with digital elements encompassing everything from smart home devices and wearable technology to industrial control systems and medical devices. The regulation represents the first horizontal cybersecurity requirement framework for hardware and software products placed on the EU market.

Essential Requirements: Manufacturers must ensure that products with digital elements are designed, developed, and produced in accordance with state-of-the-art cybersecurity practices. Requirements include: security by design and by default principles; protection against unauthorized access and modification; limited attack surfaces; secure default

configurations; timely security updates; and vulnerability disclosure mechanisms.

Conformity Assessment: Products must undergo conformity assessment procedures before being placed on the EU market. For higher-risk products (categories determined by function, use of personal data, or criticality), this requires involvement of independent third-party conformity assessment bodies (notified bodies). For lower-risk products, manufacturers may self-certify compliance.

Vulnerability Handling: Manufacturers must establish vulnerability handling processes, including: a single point of contact for vulnerability reporting; timely receipt, analysis, and remediation of reported vulnerabilities; coordinated disclosure mechanisms; and free security updates for a defined support period.

The Cyber Resilience Act complements the GDPR by addressing security issues such as insecure default configurations and lack of security updates that the GDPR does not directly regulate. However, Chawki [2] notes that compliance burdens may disproportionately affect small and medium-sized enterprises, which lack resources for conformity assessment procedures and ongoing vulnerability management.

2.2.3 Relationship to the NIS2 Directive and EU AI Act

The Cyber Solidarity Act and Cyber Resilience Act operate within a broader EU cybersecurity ecosystem that includes the NIS2 Directive (Directive 2022/2555), which establishes baseline security requirements for essential and important entities across critical sectors, and the EU AI Act (Regulation 2024/1689), which imposes risk-based requirements for AI systems. As Chawki [2] observes, these instruments collectively create a multi-layered governance architecture that addresses cybersecurity from device-level requirements (Cyber Resilience Act) to network-level detection and response (Cyber Solidarity Act) to sector-specific resilience (NIS2 Directive) to AI-specific risk management (AI Act).

This architecture exemplifies the EU's distinctive regulatory philosophy: privacy and cybersecurity are not merely policy preferences subject to political negotiation but fundamental rights enforceable through judicial proceedings and administrative sanctions. The GDPR's enforcement record including the €1.2 billion fine imposed on Meta in 2023 for unlawful transatlantic data transfers demonstrates the EU's willingness to impose meaningful consequences for non-compliance, even on the world's largest technology companies [2].

2.3 Application of Existing International Law to the Cyber Domain

Throughout the period 2020–2026, international bodies and state coalitions reaffirmed that existing international law applies to state behavior in cyberspace, even in the absence of cyber-specific treaties. As H. Moynihan [6] observe, NATO, the G7, and the UN Group of Governmental Experts have consistently articulated that the UN Charter's principles including sovereignty, non-intervention, prohibition on the use of force, and peaceful settlement of disputes apply with equal force to cyber operations as to conventional military actions.

2.3.1 Sovereignty and Non-Intervention

The principle of sovereignty prohibits states from conducting cyber operations that violate another state's territorial integrity or political independence. This includes: cyber operations targeting critical infrastructure located in another state's territory; cyber theft of intellectual property or state secrets through remote access; cyber operations supporting secessionist movements in another state; and cyber operations interfering with another state's electoral processes or governmental functions.

However, Chawki [2] cautions that states remain reluctant to state definitive opinions on legal issues, often resorting to ambiguous concepts such as "norms" without specifying interpretations or enforcement mechanisms. The lack of binding dispute resolution mechanisms for cyber operations means that even clear violations of sovereignty often go unaddressed, as states lack practical remedies beyond diplomatic protest or retaliatory cyber operations.

2.3.2 Prohibition on the Use of Force (Article 2(4))

Article 2(4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any state. The International Court of Justice, in the *Nicaragua* case (1986), established that the prohibition applies regardless of the means employed to deliver force whether conventional weapons or other methods. By extension, cyber operations that cause effects equivalent to armed force such as destruction of critical infrastructure, loss of human life, or significant economic harm may violate the prohibition.

The Tallinn Manual 2.0 (2017), prepared by an international group of legal experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence, provides a non-binding but influential assessment of how international law applies to cyber operations. The manual concludes that cyber operations qualify as a use of force when their scale and effects are comparable to non-cyber operations that would be considered uses of force.

2.3.3 Gaps and Criticisms

Despite these affirmations, significant gaps remain. Chawki [2] identifies three persistent weaknesses in the application of existing international law to cyberspace:

Attribution challenges: International law state responsibility principles require that wrongful acts be attributable to a state. However, cyber operations are frequently conducted through intermediary systems, using stolen credentials, or from infrastructure located in third states. Proving state attribution with the degree of certainty required for international legal proceedings remains technically and politically challenging.

Threshold ambiguity: The distinction between prohibited uses of force (violations of Article 2(4)) and lawful cyber operations short of force remains contested. States disagree on what level of harm economic, physical, or functional triggers the prohibition. This ambiguity creates space for grey-zone operations that cause significant harm while arguably remaining below the force threshold.

Limited enforcement mechanisms: Even when a violation of international law is established, states have limited options for peaceful dispute resolution. The International

Court of Justice requires both states' consent to jurisdiction, and many states have entered reservations excluding certain categories of disputes. The UN Security Council, which could authorize collective responses, remains subject to veto politics that often paralyze action against permanent members.

3. National Legislative Trends: Sovereignty vs. Interoperability

National laws enacted between 2020 and 2026 reflect a growing emphasis on digital sovereignty the state's asserted right to control digital infrastructure, data flows, and cybersecurity governance within its territorial boundaries. As Chawki [2] observes, digital sovereignty represents a reaction against the borderless, multi-stakeholder governance model that characterized early internet governance, instead asserting that states retain primary authority over digital spaces, just as they do over physical territories [12].

However, digital sovereignty stands in tension with interoperability the practical necessity of cross-border data flows, international threat intelligence sharing, and harmonized legal frameworks to address cyber threats that inherently transcend national boundaries. This section analyzes how major jurisdictions navigated this tension between 2020 and 2026.

3.1 Comparative Jurisdictional Framework

Chawki's [2] comparative analysis of the European Union, United States, and United Kingdom reveals three distinct normative orientations that continue to shape national cyber legislation through 2026:

European Union (Rights-Based Model): The EU regards privacy as a fundamental right rooted in human dignity, enshrined in the Charter of Fundamental Rights (Articles 7 and 8). This orientation produces legislation that prioritizes individual rights protections, even at the cost of limiting data-driven security measures. The GDPR and the AI Act exemplify this approach, imposing strict conditions on data processing and automated decision-making.

United States (Security-Oriented Model): The United States views privacy as a policy value important but subordinate to national security imperatives and market efficiency. This orientation produces sectoral legislation (e.g., Health Insurance Portability and Accountability Act [HIPAA] for healthcare, Gramm-Leach-Bliley Act [GLBA] for finance) rather than comprehensive privacy frameworks, with national security carve-outs that permit extensive surveillance under statutes such as the USA PATRIOT Act and FISA amendments [14].

United Kingdom (Procedural Equilibrium Model): The United Kingdom seeks balance through procedural regulation rather than immutable rights. The Investigatory Powers Act (2016, updated 2022) confers extensive surveillance authority but subjects it to judicial warrants, parliamentary oversight, and Investigatory Powers Tribunal review. This model aims to achieve substantive protections through procedural mechanisms rather than absolute prohibitions.

These divergent orientations produce different legislative outcomes, as illustrated in Table 1 (Chawki, Putter [9], S. Azzahro and Aminullah) [2, 9, 10].

Table 1: Comparative National Cyber Legislation (2020–2026)

Country	Major Legislation (Year)	Key Features	Regulatory Philosophy	Privacy-Security Balance
European Union	GDPR (2018, rev. 2024)	Data protection rights; consent requirements; cross-border transfer restrictions	Rights-based	Strong privacy protection; security limited by due process
European Union	NIS2 Directive (2022)	Security requirements for essential entities; incident reporting; supply chain security	Risk-based	Balanced; sector-specific requirements
European Union	AI Act (2024)	Risk-based AI regulation; prohibited AI practices; conformity assessment	Risk-based	Privacy prioritized for high-risk systems
United States	NIST CSF 2.0 (2024)	Governance-focused framework; supply chain risk management	Voluntary/Advisory	Security prioritized; privacy secondary
United States	SEC Cybersecurity Rule (2023)	Four-day incident disclosure; governance requirements	Mandatory/Disclosure	Transparency prioritized
United States	FISMA 2023 (2023)	Federal agency cybersecurity; CISA oversight; incident reporting	Mandatory/Compliance	Security prioritized
United Kingdom	Investigatory Powers Act Update (2022)	Bulk surveillance powers; judicial warrants; double-lock authorization	Procedural	Equilibrium through oversight
United Kingdom	Data Protection and Digital Information Bill (2023)	GDPR replacement framework; streamlined data sharing	Rights-reduced	Reduced privacy protections post-Brexit
South Africa	Cybercrimes Act (No. 19 of 2020)	Ransomware criminalization; interception offenses; evidence provisions	Criminal enforcement	Security prioritized; limited privacy safeguards [7]
Indonesia	Law No. 27 of 2022 (PDP Law)	Personal data protection; data localization; state control over data flows	Sovereignty-focused	State security prioritized; limited individual rights [8]
China	Data Security Law (2021) & Personal Information Protection Law (2021)	Data localization; state access requirements; cross-border transfer restrictions	State-controlled	State security absolutely prioritized

3.2 European Union: Deepening the Rights-Based Framework

The European Union continued to develop its distinctive rights-based approach to cybersecurity governance between 2020 and 2026. Three major legislative developments warrant detailed examination. [12]

3.2.1 NIS2 Directive (Directive 2022/2555)

Adopted in December 2022, the NIS2 Directive substantially expands the scope and requirements of the original NIS Directive. Key provisions include:

- **Expanded Scope:** The directive now covers 18 sectors (increased from 7), including energy, transport, banking, health, digital infrastructure, public administration, and space. Estimates suggest NIS2 covers approximately 160,000 entities across the EU.
- **Risk Management Obligations:** Covered entities must implement proportionate technical, operational, and organizational measures, including risk analysis, incident handling, business continuity, supply chain security, and cybersecurity training.
- **Incident Reporting:** Entities must report significant cyber incidents within 24 hours (early warning), 72 hours (notification), and 30 days (final report).
- **Enforcement and Penalties:** Fines up to €10 million or 2% of global annual turnover for essential entities.
- **Management Liability:** Management bodies are held accountable for compliance, extending to personal liability for intentional or grossly negligent violations.

3.2.2 EU AI Act (Regulation 2024/1689)

Adopted in May 2024, the EU AI Act establishes the world's first comprehensive horizontal legal framework for AI. The Act's risk-based classification system is central to its regulatory approach:

- **Unacceptable Risk (Prohibited):** Social scoring by governments, real-time remote biometric identification in public spaces (with narrow exceptions), and AI exploiting vulnerable populations.
- **High Risk (Regulated):** AI used in critical infrastructure, education, employment, law enforcement, and migration management. Requires conformity assessment, risk management, and human oversight.
- **Limited Risk (Transparency Obligations):** Chatbots and deepfakes must disclose their AI nature.
- **Minimal Risk (Unregulated):** AI-enabled spam filters, video games, and recommendation engines.

AI systems deployed for cybersecurity purposes in critical infrastructure sectors qualify as high risk, creating a recursive governance challenge: cybersecurity AI systems must themselves meet cybersecurity requirements.

3.3 United States: Sectoral, Security-Oriented, and Increasingly Proactive

The United States continued its distinctive sectoral approach, with no comprehensive federal privacy law but significant regulatory developments across multiple sectors.

3.3.1 NIST Cybersecurity Framework 2.0 (2024)

NIST released CSF 2.0 in February 2024 [11]. Key innovations include:

- **Governance as a Core Function:** The original five functions (Identify, Protect, Detect, Respond, Recover) were supplemented with a sixth function: Govern.
- **Supply Chain Risk Management:** Substantially expanded guidance reflecting lessons from the SolarWinds breach (2020).
- **Implementation Examples:** Concrete examples for each subcategory to aid smaller organizations.

3.3.2 SEC Cybersecurity Disclosure Rule (2023)

The SEC adopted final rules mandating cybersecurity disclosure for public companies, effective September 2023 [2]. Registrants must disclose material cybersecurity incidents on Form 8-K within four business days of determining materiality. Annual reports must describe risk management processes, management's role, and board oversight.

3.3.3 Federal Information Security Modernization Act (FISMA) 2023

Enacted in December 2024, FISMA 2023 represents the first comprehensive update to federal agency cybersecurity since 2014 [2]. Key provisions include expanded CISA authority, incident reporting within 24 hours, AI-specific provisions (algorithmic impact assessments, audit trails), and contractor oversight.

3.4 United Kingdom: Post-Brexit Realignment

Following Brexit (effective 2020), the United Kingdom pursued an independent data protection and cybersecurity policy.

3.4.1 Investigatory Powers Act Update (2022)

The IPA was updated to address technological changes and judicial criticism. Key provisions include bulk surveillance powers subject to judicial warrants, "double-lock" authorization (Judicial Commissioner approval and Secretary of State Signature), and privacy protections for privileged communications and journalistic sources.

3.4.2 Data Protection and Digital Information Bill (2023–2024)

The UK government proposed replacing GDPR-UK with a streamlined domestic framework. Key proposed changes include reduced record-keeping, relaxed cookie consent requirements, broader research exemptions for AI training, and an independent UK adequacy framework. The bill's outcome will significantly affect the UK's GDPR adequacy status.

3.5 Emerging Economies: Digital Sovereignty in Practice

Beyond Western jurisdictions, emerging economies increasingly assert digital sovereignty through legislation prioritizing state control over data.

South Africa (Cybercrimes Act, No. 19 of 2020): Criminalizes ransomware, unlawful interception, and cyber fraud; asserts extraterritorial jurisdiction; implementation hampered by insufficient technical training and delayed officer appointments [7].

Indonesia (PDP Law, Law No. 27 of 2022): Requires data

localization; establishes executive-branch supervisory authority; criminal penalties up to 6 years imprisonment; became fully effective in October 2024 [8].

China (Data Security Law and Personal Information Protection Law, 2021): Requires data classification by national security impact; cross-border transfers require CAC security assessment; state access requirements for security and law enforcement.

4. Emerging Challenges: AI, Jurisdictional Creep, and the Privacy Paradox

As national and international cyber legal frameworks evolved between 2020 and 2026, three interconnected challenges emerged that existing regulatory architectures struggled to address adequately.

4.1 Artificial Intelligence Governance

By 2025, the proliferation of LLMs, generative AI systems, and AI-enabled cybersecurity tools triggered an urgent wave of regulatory challenges [12, 13, 14]. As Chawki [2] emphasizes, AI cannot be treated as a monolithic technology for legal purposes. Figure 1 illustrates the framework for regulating and overseeing AI systems.

Fig 1: AI Governance

4.1.1 Disaggregating AI Systems

Chawki [2] identifies four categories of AI systems with distinct governance problems:

- **Large Language Models (LLMs) and Generative AI:** Data provenance, misinformation, model inversion, and liability concerns.
- **Predictive Policing and Risk Assessment Systems:** Proportionality, discrimination, and procedural fairness concerns.
- **Biometric Surveillance Systems:** Covert operation, difficulty of avoidance, and mass surveillance capabilities.
- **Anomaly Detection and Threat Identification Systems:** Explainability, false positives, and opacity ("black box") concerns.

4.1.2 Diverging International Approaches

The EU's comprehensive rights-based approach contrasts sharply with other jurisdictions. The United States has no comprehensive federal AI legislation, relying on sectoral guidelines and executive orders. China prioritizes state control and social stability, with AI systems serving party-state objectives. The UK emphasizes voluntary compliance, regulatory sandboxes, and sector-specific guidance. The ASEAN Guide on AI Governance (2026) reflects regional harmonization efforts but lacks binding enforcement mechanisms [8].

4.1.3 AI-Specific Cyber Threats

AI systems introduce novel cyber threats: adversarial machine learning (crafted inputs causing misclassification), model inversion and extraction (recovering training data), prompt injection and LLM vulnerabilities, and automated attack scaling. Legal frameworks must address these emerging vulnerability classes [16]

4.2 Jurisdictional Creep: The Expansion of Passive Personality Jurisdiction

One of the most controversial aspects of the 2024 UN Convention is its provision for passive personality jurisdiction the assertion of jurisdiction over crimes committed anywhere in the world where the victim is a national of the prosecuting state [11]. Figure 2 shows the expansion of legal jurisdiction across borders.

Fig 2: Jurisdictional Creep

4.2.1 Risks of Jurisdictional Creep

Scher-Zagier [11] identifies several risks: conflicting national claims (multiple states asserting jurisdiction over the same incident), sovereignty concerns (policing conduct within another state's territory), human rights implications (prosecution in countries with weaker due process), and enforcement disparities (wealthy states overreaching while developing states lack capacity).

4.2.2 Mitigation Strategies

Proposed safeguards include subsidiarity principles (deferring to territorial states), double criminality requirements, proportionality limitations, consultation and cooperation mechanisms, and human rights guarantees [2, 11].

4.3 The Privacy Paradox in Cybersecurity Information Sharing

The "privacy paradox" refers to the discrepancy between individuals' stated intentions to protect their privacy and their actual information-sharing behavior [2]. This paradox manifests across individual, organizational, and public-private information-sharing contexts. Figure 3 illustrates the privacy security trade off.

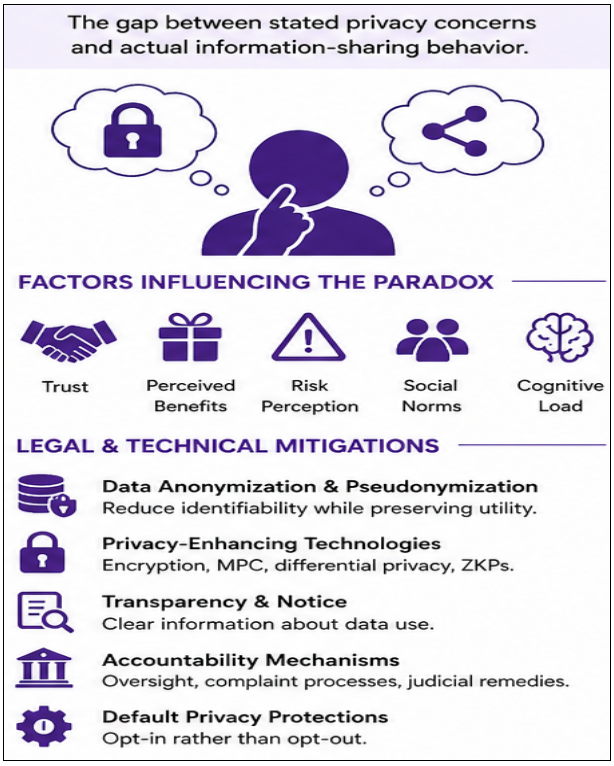


Fig 3: The Privacy Paradox

4.3.1 Factors Influencing the Privacy Paradox
Chawki [2] identifies several mediating variables: trust in the recipient organization, perceived benefits versus costs, risk perception (systematic misperception of privacy and security risks), social norms and observability, and cognitive load and decision fatigue.

4.3.2 Legal and Technical Mitigations
Mitigations include data anonymization and pseudonymization, privacy-enhancing technologies (encryption, secure multi-party computation, differential privacy, zero-knowledge proofs), transparency and notice, accountability mechanisms (internal complaint processes, regulatory oversight, judicial remedies), and default privacy protections (opt-in rather than opt-out).

The Department of Homeland Security's Automated Indicator Sharing (AIS) initiative illustrates the privacy paradox at an institutional level: stated support for collective cybersecurity coexists with persistent behavioral reluctance to share [2].

5. Case Studies in Information Sharing Effectiveness
Chawki [2] provides two instructive case studies that remain highly relevant to the 2020–2026 period.

Mayo Clinic (Effective): The Mayo Clinic exemplifies successful integration of clinical collaboration with robust cybersecurity governance. By implementing rigorous access controls, encryption, role-based privileges, and continuous penetration testing, the Clinic aligns with GDPR and HIPAA standards while maintaining patient trust. This demonstrates that standardized information sharing, coupled with a collaborative mindset, can transform institutional practice without sacrificing privacy [12].

US Intelligence Pre-9/11 (Ineffective): The September 11 attacks illustrate catastrophic national security failure resulting from insufficient information sharing. Institutional silos, a "need-to-know" culture, and legal barriers under FISA obstructed intelligence integration. Post-9/11 reforms including the USA PATRIOT Act and the creation of the Director of National Intelligence sought to address these deficiencies, yet cultural inertia persists, underscoring that institutional culture may be as pivotal as the rule of law in determining security outcomes [2, 14].

6. Recommended Legal Frameworks for Equitable Cybersecurity
Drawing on multi-level governance analysis [2, 17, 18], several legal mechanisms are proposed to balance privacy and security:

- **Accountability mechanisms:** Independent auditing and judicial supervision to prevent misuse of surveillance powers.
- **Data minimization:** Collecting and retaining only the minimum necessary information, for the shortest possible period.
- **Transparency obligations:** Clear disclosure of data management practices to build public trust.
- **Public-private partnerships with enforceable accountability:** Moving beyond voluntary information-sharing to frameworks with clear liability and oversight provisions.
- **Adaptive, risk-based regulation:** Moving from static rules to frameworks that can evolve with technological change, as exemplified by the EU AI Act's risk-based approach.
- These recommendations align with the broader trend identified in the literature: the transition from reactive measures to proactive, systemic governance [15].

7. Conclusion
The frontier of cyber law between 2020 and 2026 evolved from fragmented, reactive measures toward more integrated, proactive governance architectures. The United Nations Convention against Cybercrime marks an important step in international cooperation, although the balance between national security and privacy remains dynamic in a rapidly changing technological landscape. Key insights include the value of integrating legal principles with enforcement actions such as those under the General Data Protection Regulation and rulings like Schrems II along with a shift toward hybrid governance models and more targeted regulation of different AI systems. However, the tension between national sovereignty and borderless digital threats continues to be the central challenge, with future cybersecurity shaped by legal, ethical, and institutional decisions as much as by technological progress.

References
1. Oyadeyi B. Funding crime online: Cybercrime and its links to organised crime in the Caribbean. London: Commonwealth Secretariat; 2023.
2. Chawki M. Legal foundations and future directions of AI-enabled cybersecurity: A cross-jurisdictional analysis. Cogent Social Sciences. 2026;12(1):2614015. doi:10.1080/23311886.2026.2614015
3. Sahu VK, Pandey D, Khan RA, Khan MW, Pandey V. An enhanced layered IoT architecture for IoT applications against cyber-attacks. In: Recent advances in computational intelligence and cyber security. 1st ed. Boca Raton: CRC Press, Taylor and Francis Group; 2024.
4. Shabbir M, Yadav RK, Khan MW, Singh H. Empirical analysis of computationally intelligent technique for software risk prediction. Journal of Cybersecurity and Information Management. 2026;17(2):200-209.
5. Kumar R. United Nations cybercrime convention: A milestone in digital governance? IDSA Issue Brief. 2025:1-10.
6. Sharma RK. The UN cybercrime convention: Key features and global stances. IDSA Issue Brief. 2025:1-9.
7. Villani S. The cyber solidarity act: Framework and perspectives for the new EU-wide cybersecurity solidarity mechanism under the EU legal system. European Journal of Risk Regulation. 2025;16(2).
8. Moynihan H. The vital role of international law in the framework for responsible state behaviour in cyberspace. Journal of Cyber Policy. 2020;6(3).
9. Putter LF, Johnson R, Mans-Kemp N. Exploring cybersecurity disclosure in South Africa. South African Journal of Economic and Management Sciences. 2026.
10. Azzahro S, Aminullah. Comparison of Indonesian and Philippine public administration regulations in dealing with AI disruption in ASEAN. International Journal of Multidisciplinary Research. 2026;2(1):168-177.
11. National Institute of Standards and Technology. Cybersecurity framework 2.0 resource center. Gaithersburg (MD): National Institute of Standards and

Technology; 2024.
12. Ong JCL, Chang SY, William W, Butte AJ, Shah NH, Chew LST, *et al*. Ethical and regulatory challenges of large language models in medicine. Lancet Digital Health. 2024;6(6):e428-e432. doi:10.1016/S2589-7500(24)00061-X
13. Scher-Zagier E. Jurisdictional creep: The UN cybercrime convention and the expansion of passive personality jurisdiction. Yale Journal of Law and Technology. 2025;27(1):327-389.
14. Pandey K, Tripathi AK, Kapil G, Singh V, Khan MW, Agrawal A, *et al*. Current challenges of digital forensics in cyber security. In: Critical concepts, standards, and techniques in cyber forensics. Hershey (PA): IGI Global; 2020. p.31-46.
15. Khan RA, Khan MW. Cyber security's influence on smart cities: Challenges and solutions. In: Contemporary innovations in engineering and management. AIP Publishing; 2023. p.040033-1–040033-12.
16. Joshi M, Pandey D, Pandey V, Khan MW. A fusion framework for Hinglish cyberbullying detection using mBERT and FastText. International Journal of Engineering in Computer Science. 2025;6(1):7-14.
17. Khan RA, Farooqui MF, Khan MW. A comprehensive assessment of the existing literature on the challenges and solutions related to cyber security in smart cities. In: Advances in science, engineering and technology. 1st ed. Boca Raton: CRC Press, Taylor and Francis Group; 2025.
18. Adeel N, Kumar R, Akella KNS, Manickam V, Khan MW, Nandury SV. Measuring the implications of email viruses through a unified model of cyber security. In: Proceedings of the 6th International Conference on Contemporary Computing and Informatics (IC3I); 2023; Gautam Buddha Nagar, India. p.614-621.