ProSafeNet

International Journal of Disaster Risk Management • Vol. 8. No. 1 • https://doi.org/10.66050/5jedtn66

Publisher: Scientific-Professional Society for Disaster Risk Management

International Journal of Disaster Risk Management

Review article

Regulating Emerging Technologies in Disaster Management: A Comparative Analysis of Security Governance and Legal Liability in India and Serbia

Manindra Singh Hanspal[1], Vladimir M. Cvetković[1,2,3,4,5], Milan Lipovac[2], Dejana Jovanović Popović[2]

[1] Presidency University, School of Law, Bengaluru Itgalpura, Rajanukunte, Yelahanka, Bengaluru, Karnataka 560064, India.

[2] Department of Disaster Management and Environmental Security, Faculty of Security Studies, University of Belgrade, Gospodara Vucica 50, 11040 Belgrade, Serbia; vmc@fb.bg.ac.rs; vladimir.cvetkovic@unileoben.ac.at (V.M.C); dejana@fb.bg.ac.rs (D.J.P.)

[3] Safety and Disaster Studies, Chair of Thermal Processing Technology, Department of Environmental and Energy Process Engineering, Montanuniversität, Leoben, Austria.

[4] Scientific-Professional Society for Disaster Risk Management, Dimitrija Tucovića 121, 11040 Belgrade, Serbia.

[5] International Institute for Disaster Research, Dimitrija Tucovića 121, 11040 Belgrade, Serbia.

[6] ProSafeNet, the Global Hub for Safety, Security, Risk, Emergency Professionals, and Scientists, 11040 Belgrade, Serbia.

Correspondence: mhanspal21@gmail.com.

Received: 25 December 2025; Revised: 25 January 2026; Accepted: 10 February 2026; Published: 5 March 2026.

ABSTRACT

The integration of emerging technologies such as artificial intelligence (AI), drones, IoT sensors, big data, and blockchain is revolutionizing disaster management by enhancing response speed and effectiveness. However, these advancements introduce significant challenges in security governance and legal liability, particularly around accountability, data protection, algorithmic bias, and the resilience of critical infrastructure. This comparative study examines how India and Serbia regulate the use of these technologies in disaster management, incorporating legal analysis, policy review, and expert insights. The findings highlight that while India focuses on national frameworks, particularly through the National Disaster Management Authority (NDMA), Serbia aligns its disaster management approach with European Union standards and emphasizes regional cooperation. Both countries face common challenges, including the attribution of liability for autonomous decision-making, cybersecurity risks, and cross-border coordination. To address these issues, the study proposes a hybrid governance model that combines adaptive regulation, multi-stakeholder partnerships, liability-sharing mechanisms, and technology-neutral legal frameworks. The research argues that effective regulation must balance operational efficiency with security, legitimacy, and human rights protection, ultimately fostering public trust and enhancing disaster resilience.

KEYWORDS

Disaster management, emerging technologies, security governance, legal liability, cybersecurity, critical infrastructure

Academic Editor:
Prof. Dr. Neda Nikolić

e-ISSN2620-2786

Hanspal, M. S., Cvetković, V. M., Lipovac, M., & Popović, D. J. (2026). Regulating Emerging Technologies in Disaster Management: A Comparative Analysis of Security Governance and Legal Liability in India and Serbia, 8(1), 147-162.

1. Introduction

The contemporary security landscape in disaster management has been fundamentally transformed by the proliferation of emerging technologies, including artificial intelligence (AI), unmanned aerial vehicles (UAVs), Internet of Things (IoT) sensors, and blockchain systems (Mandloi, Arya, & Verma, 2024). These technologies offer unprecedented capabilities for early warning systems, real-time monitoring, resource allocation, and post-disaster recovery coordination (Kordi & Ertz, 2025; Leong, 2025; Milenković, Cvetković, Ivanov, & Renner, 2024; Vidović, Beriša, & Cvetković, 2024). However, their integration into national disaster management frameworks raises critical questions about security governance, legal liability, and regulatory adequacy that traditional legal systems struggle to address (Mustafa et al., 2025). This is especially relevant in countries with varied landscapes and dense populations, like India, where advanced tools such as AI, GIS, mobile communication systems, and drones have significant potential to improve disaster response and reduce negative impacts (Hanspal & Behera, 2024). The challenge of governing emerging technologies in disaster management contexts is particularly acute in developing and transitional economies, where regulatory frameworks often lag behind technological adoption (Lescrauwaet et al., 2022). This regulatory gap creates vulnerabilities in critical infrastructure, unclear liability attribution for automated decision-making, and potential security risks that could compromise the effectiveness of disaster response (Riggs et al., 2023).

The increasing frequency and intensity of global disasters necessitate robust disaster risk management strategies, highlighting the critical role of emerging technologies in mitigating their impact (Cvetković, 2024). In particular, India's diverse topography and dense population, coupled with Serbia's susceptibility to natural and socio-economic pressures, underscore the urgent need for technologically advanced disaster management frameworks (Cvetković, 2024; Hanspal & Behera, 2024). India and Serbia represent compelling case studies for comparative analysis due to their distinct regulatory approaches, geographical vulnerabilities, and varying patterns of technological adoption. India has faced a range of climate-related disasters and has invested heavily in technology-driven disaster management (Charak, Ravi, & Verma, 2024). Serbia has aligned its disaster management framework with European Union standards and developed cooperation mechanisms with neighbouring countries (Tanasic & Vladimir, 2024). This research addresses the gap in examining the legal liability implications of emerging technologies in disaster management contexts by providing a comprehensive comparative analysis of security governance models and their effectiveness in managing technological risks while maintaining operational capabilities.

This comparative approach aims to highlight best practices and pinpoint areas needing improvement in both national and international disaster response protocols. It supports the development of more resilient, legally robust frameworks for incorporating technology (Hanspal & Behera, 2024). Ultimately, the goal is to deepen understanding of how different disaster management strategies can enhance resilience, lower vulnerabilities, and improve coordination at national and regional levels (Beli, Renner, Cvetković, Ivanov, & Gačić, 2025). In this paper, "emerging technologies" refers to digital and cyber-physical systems that directly impact disaster-related decision-making, sensing and monitoring, warning dissemination, logistics, and coordination. The analysis looks at four main groups: AI-enabled decision support, UAV-based data collection and delivery, IoT sensor networks for early warning and infrastructure monitoring, and distributed digital platforms that support data sharing and identity or benefit management. Technologies used only for internal administration, such as generic office software, are not included unless they have a significant effect on emergency operations or public safety.

2. Literature review

2.1. Disaster risk governance: concepts and global policy anchors

Disaster risk governance encompasses the frameworks and processes through which various actors manage and mitigate disaster risks at multiple levels of society (Ikeda & Nagasaka, 2011). Ef-

fective disaster governance requires robust institutional, policy, and legal frameworks that facilitate collaboration among various stakeholders (Dai & Azhar, 2024). The adaptive governance model emphasizes communities' capacity to adapt to uncertainties, promoting a learning-centred, collaborative approach to disaster risks (Mitchell, 2022). The Sendai Framework for Disaster Risk Reduction (2015–2030) places governance, laws, institutions, and accountability at the core of risk reduction, calling for "risk-informed" decision-making, stronger legal frameworks, and multi-stakeholder coordination across sectors and scales. It explicitly links early warning, information sharing, and preparedness with regulatory capacity and public trust, framing technology as an enabler that must be embedded in governance systems rather than adopted in isolation (UNISDR, 2015). The integration of innovative technologies in governance can enhance risk anticipation and response capabilities (Klinke & Renn, 2012). However, challenges such as political inertia and resource allocation issues hinder the implementation of effective strategies that are vital to enhancing resilience against future disasters (Uddin et al., 2021).

2.2. Technology in disaster management: capabilities and constraints

The integration of technology in disaster management (DM) has transformed how societies prepare for, respond to, and recover from disasters. Technologies like big data, AI, drones, and IoT enhance predictive capabilities, real-time monitoring, and resource allocation during crises (Kirpalani, 2024; Pandey et al., 2025; Khan et al., 2022). However, challenges such as high implementation costs, skill gaps, and the need for seamless integration can hinder effective utilization (Krichen et al., 2024; Johnson et al., 2023). While technology offers significant advantages, its reliance may lead to complacency in traditional preparedness methods, which remain crucial in disaster resilience. Over the last decade, AI, remote sensing, and IoT have transitioned from experimental pilots to operational tools for hazard detection and situational awareness (Ahmad, 2024). However, challenges remain in model bias, explainability, data quality constraints, regulatory approval, and privacy issues (Rane et al., 2025; Lyu et al., 2023; Lone et al., 2023).

2.3. Cybersecurity as disaster-risk: cascading and compound threats

Modern cyber threats can trigger cascading and compound disasters, where a single incident or interconnected vulnerabilities lead to widespread, multi-domain impacts. Cyber-physical systems are particularly vulnerable to these dynamics, as failures can escalate from the digital to the physical domain, leading to large-scale systemic disruptions (He et al., 2024). Recent research emphasizes embedding cybersecurity into all-hazards disaster resilience planning, which includes multi-risk assessments and advanced modelling tools to anticipate cascading effects (Alakbarli, 2025). Proactive approaches, such as integrating cyber threat intelligence, implementing layered defense, and maintaining continuous adaptation, are essential for mitigating immediate and evolving threats (Dine, 2024).

The digitalization of emergency management has created new vulnerabilities. Ransomware and AI-enabled cyberattacks increasingly threaten critical infrastructure, with cascading impacts across various sectors (George et al., 2024). Incidents affecting healthcare, water systems, and transportation have shown that cyber disruptions can have humanitarian consequences comparable to those of natural disasters (Okolo et al., 2021). Recent ransomware attacks on emergency booking systems for paratransit services underscore the direct connection between cyber risk and disaster risk management (Kalinaki, 2024). Intelligence community reports further reveal intrusions against industrial control systems across the water, food, and port sectors, highlighting the need to treat cyber incidents as disaster-like events within all-hazards governance (Schlegelmilch, 2020).

2.4. Ethical and safety governance for AI in emergencies

The rapid adoption of artificial intelligence (AI) in emergency management and healthcare offers significant opportunities to improve crisis response, but it also raises complex ethical and safety concerns (Visave, 2024). Effective governance is essential to ensure AI systems are trustworthy, fair, and safe, particularly in high-stakes environments where decisions can have profound consequences (Ottun & Flores, 2025). Bias, fairness, transparency, and explainability are central challenges, as AI systems can unintentionally reinforce existing biases or make opaque decisions that undermine trust and accountability (Alabi, 2024; Patidar et al., 2024). Addressing these challenges requires robust mitigation strategies, continuous monitoring, and transparency in AI decision-making. Privacy and data security are additional concerns, as emergency AI systems often handle sensitive personal information, necessitating robust protections to prevent breaches and maintain public trust (Baladari, 2020).

Governance frameworks integrate ethical principles, regulatory measures, and operational practices to ensure effective AI management. Key principles include autonomy, beneficence, justice, and professional oversight (Subash & Whig, 2025). The GREAT PLEA framework emphasizes accountability, privacy, lawfulness, and autonomy to guide AI development in emergency contexts (Oniani et al., 2023). However, many global guidelines remain non-binding and lack enforceable mechanisms. Effective operationalization requires translating these ethical principles into actionable guidelines and risk management systems (Tariq et al., 2025). Global guidance now converges on the risk-based, context-sensitive governance of AI in public safety, with the WHO recommending human oversight and accountability safeguards (WHO, 2024). The EU Artificial Intelligence Act (2024) establishes a risk-tiered regime for "high-risk" systems, setting strict obligations for documentation, conformity assessments, and post-market monitoring (Du, 2025).

2.5. India: Disaster Law, Technology governance, and AI Regulation

India's disaster management system has evolved from a reactive model to a proactive, resilience-based framework, anchored in the Disaster Management Act of 2005, which established key institutions such as the National Disaster Management Authority (NDMA) and State/District Disaster Management Authorities (Hanspal & Behera, 2024). Despite this transformation, gaps persist in areas such as early warning systems, fund utilization, and institutional accountability, which were particularly evident during the Uttarakhand and Kerala floods. India has also integrated technology governance by incorporating ICT, big data, and remote sensing into national strategies, aligning with the Sendai Framework's emphasis on technology-driven approaches (Grembergen, 2004; Hanspal & Behera, 2024a). However, the rapid adoption of digital tools raises governance challenges related to data protection, interoperability, and ethical use, particularly amid emerging cyber threats and the Digital India initiative (Hanspal, 2024).

The increasing use of artificial intelligence (AI) and machine learning for predictive analytics and early warning has raised new concerns about liability, transparency, and human oversight, highlighting regulatory gaps and ethical dilemmas in AI-driven decision-making (Ahmed, 2025). India's disaster management regime, while maturing, requires greater legal clarity, stronger accountability mechanisms, and safeguards for emerging technologies to ensure technological advancements strengthen resilience without undermining rights or ethical standards. With the implementation of the Digital Personal Data Protection Act (2023), India now has a comprehensive data protection statute, introducing implications for consent, purpose limitation, user rights, and breach reporting in emergency contexts involving AI and UAVs (Malhotra & Malhotra, 2024).

2.6. Serbia: Disaster Law, Technology Governance, and AI Alignment with the EU

The basic legal instrument for this sector is the Law on Disaster Risk Reduction and Emergency Management. This legislation fundamentally redefined the national approach by prioritizing pre-

vention and preparedness over traditional response-only strategies (Cvetković, 2024; Cvetković & Miljković, 2024). Under Article 11 of this law, disaster risk reduction is explicitly defined as a set of measures intended to lessen harmful consequences and ensure an efficient response through enhanced preparedness (Cvetković & Miljković, 2024). The law also establishes a multi-sectoral system involving the police, the Serbian Army, fire and rescue services, and specialized associations, such as the Mountain Rescue Service, to ensure a coordinated response (Cvetković & Miljković, 2024). National resilience is defined within this system as the capacity of communities to recover while maintaining essential functions (Milenković, 2025).

The newly adopted AI Strategy (2025–2030) builds on previous efforts, conforming with global AI governance standards and concentrating on safety, accountability, and data governance, all critical to emergency management and defending infrastructure (Government of the Republic of Serbia, 2025). Serbia's data-protection framework is consistent with GDPR principles, imposing strict safeguards on the processing of personal and geospatial data in emergencies (Popović, 2023). These reforms illustrate Serbia's trajectory toward EU integration, strengthening organizational accountability, liability rules, and cross-border cooperation under the EU Civil Protection Mechanism (Corbane et al., 2024).

Serbia has increasingly integrated technology into its security and defense curricula, utilizing simulation centers to prepare for complex disaster scenarios (Roković & Stanojević, 2024). Governance in this area is guided by the Strategy for the Development of the Information Society and Information Security (2021–2026), which identifies information security as a prerequisite for a strong public administration and economy (Milenković, Cvetković, Ivanov, & Renner, 2024). Furthermore, the National Security Strategy officially recognized cyberspace and hybrid threats as essential factors influencing national security, mandating the protection of databases and critical infrastructure from unauthorized access and disinformation (Milenković, Cvetković, Ivanov, & Renner, 2024).

Serbia is presenting itself as a regional leader in AI regulation in the Western Balkans, having established a dedicated working group to prepare a national AI Act aligned with the EU's regulatory framework (Dejanović & Kriviņš, 2025; Krivokapić, Živković, & Nikolić, 2022). The AI Strategy (2025–2030) builds on earlier digital transformation efforts, focusing specifically on safety, accountability, and the classification of AI systems (Dejanović & Kriviņš, 2025). In the context of disaster management, this alignment is vital, as the EU AI Act classifies certain AI systems used in crisis response as "high-risk," requiring rigorous conformity assessments and human oversight (Commission, 2025). Serbia's approach aligns with these requirements, emphasizing that AI-powered tools must operate within clear moral boundaries to foster community confidence (Dejanović & Kriviņš, 2025; Krivokapić, Živković, & Nikolić, 2022).

The governance of emerging technologies in Serbian disaster management is heavily influenced by the GDPR-aligned data protection framework, which applies strict safeguards on the processing of personal and geospatial data (Krivokapić, Živković, & Nikolić, 2022). This alignment itself is essential for Serbia's participation in the EU Civil Protection Mechanism, which facilitates cross-border cooperation and standardized emergency response guidelines (Beli, Renner, Cvetković, Ivanov, & Gačić, 2025). Despite these advancements, difficulties persist in building comprehensive geospatial risk maps and in streamlining resource allocation between national and local government levels (Beli, Renner, Cvetković, Ivanov, & Gačić, 2025). Strengthened organizational accountability and liability rules are currently being developed to address the legal challenges posed by AI-induced harm, ensuring that liability for technological failures during emergencies is clearly defined in accordance with emerging EU standards (Havu et al., 2024; Vidović, Beriša, & Cvetković, 2024). This forward-looking legislative stance aims to preempt legal vagueness and to support a robust framework for accountability in the rapidly evolving landscape of AI applications in disaster management.

3. Methods

In this study, we have employed a qualitative comparative legal and policy analysis to examine the governance of emerging technologies in disaster risk management (DRM), with particular at-

tention to accountability and liability. Based on their characteristics, India and Serbia are selected for comparison due to their high disaster exposure and rapidly expanding technology ecosystems. Also, we have chosen them because of their contrasting regulatory architectures and institutional arrangements. Our analysis draws on a range of primary legal and policy documents, including national and regional strategies, disaster management laws, data protection regulations, network security frameworks, and official guidance. All documents are relevant to artificial intelligence, drones (UAVs), Internet of Things (IoT) systems, and digital applications used in emergency contexts. In the selection process, we have used three criteria: direct relevance to disaster preparedness or response, explicit reference to technology-enabled systems or data governance, and enforceability or operational applicability. Of course, to ensure comparability, an organized framework is applied to code each instrument according to the scope of technology coverage, assignment of responsibilities among actors, liability triggers and standards of care, disclosure and supervisory mechanisms, data protection and cybersecurity obligations, and enforcement tools and remedies. The aim of this study is to identify governance gaps and practical consequences for DRM operations. Aware of these facts, our study is limited to formal instruments and publicly available sources, and does not assess real-world compliance or implementation performance, which may vary across jurisdictions and agencies.

4. Regulatory architecture comparison

India has adopted a centralized model anchored by the National Disaster Management Authority (NDMA), coordinating technology integration across federal and state levels (Hanspal & Behera, 2024a). Serbia aligns its disaster management approach with European Union standards, integrating EU directives on critical infrastructure protection and cybersecurity into its legal framework (Murić et al., 2013).

Table 1. Comparative Regulatory Architecture.

Aspect	India	Serbia
DRM Law	Disaster Management Act, 2005	Law on Disaster Risk Reduction (2018)
Tech-Specific Regs	IT Act, Draft AI Policy	AI Strategy (2020), Cybersecurity Law, GDPR
Liability	State + product liability, weak AI liability	EU-influenced liability norms
Security Focus	Data protection gaps, fragmented governance	Strong cybersecurity integration
Emerging Gaps	Privacy, AI bias, corporate liability	Enforcement capacity, innovation adoption

4.1. Synthesis and gaps

The literature suggests that while technologies improve preparedness and response, risk governance determines their net value. Three key gaps stand out for India and Serbia:

- Operational oversight for high-risk AI (aligned with EU AI Act and WHO guidance).
- Privacy-by-design safeguards for aerial and sensor data under DPDP (India) and GDPR-aligned frameworks (Serbia).
- Cyber-resilience of emergency systems, including mandatory reporting, drills, and incident response protocols.

This study offers a comparative legal analysis of India and Serbia, identifying opportunities for convergence in technology governanceand liability frameworks. Table 1 illustrates the key structural differences between the two countries' regulatory architectures.

Table 2. Legal and Governance Frameworks for Disaster Tech.

Aspect	India	Serbia
Legal Framework	Disaster Management Act 2005, IT Act	Law on Disaster Risk Reduction (2018), Cybersecurity Law
International Alignment	SENDAI Framework, bilateral agreements	EU directives, regional cooperation
Key Focus	Technology-driven approaches, ICT integration	AI strategy, data governance

4.2. Legal Liability Attribution

Legal liability for failures in emerging technologies in disaster management presents a challenge for both India and Serbia. India's legal framework relies on traditional tort law, with the Supreme Court's decision in M.C. Mehta v. Union of India (1987) establishing strict liability for hazardous activities (Sharma, 2012). However, modern AI and autonomous systems complicate liability attribution, especially when multiple automated systems interact in complex disaster scenarios. Serbia has integrated EU liability frameworks through the implementation of the Product Liability Directive and has clarified liability through mandatory certification processes for critical technologies and public-private partnerships (Nuredin, 2022).

4.3. Security Governance Structures

Security governance in both countries operates through multi-layered frameworks, with India focusing on the National Critical Information Infrastructure Protection Centre (NCIIPC) to oversee security for critical sectors, including disaster management systems (Hanspal, 2024). Serbia's security governance aligns with NATO and EU standards, emphasizing threat assessment and real-time monitoring through the Unified Information System for Emergency Management (Cvetković et al., 2024).

4.4. Cross-border Cooperation Mechanisms

India's disaster management cooperation focuses primarily on regional frameworks in South Asia, though technology sharing remains limited due to security concerns and system compatibility issues (Bishwakarma & Hu, 2022). Serbia leverages the EU Civil Protection Mechanism, enabling technology interoperability and shared response capabilities, though this creates dependencies on external systems and standards (Kešetović & Samardžija, 2014).

Table 3. Cross-border Cooperation Frameworks.

Aspect	India	Serbia
Primary Mechanisms	SAARC, bilateral agreements	EU Civil Protection, DPPI SEE
Technology Sharing	Limited	Extensive through EU frameworks
Legal Harmonization	Minimal convergence	EU directive compliance

4.5. Implementation Challenges

Both countries face common implementation challenges, including lengthy procurement processes, skills gaps, and funding constraints. India struggles with federal-state coordination and im-

plementation across diverse contexts, while Serbia faces challenges with EU compliance timelines and balancing national sovereignty with regional integration (Petrović, 2019).

5. Comparative Analysis: India and Serbia

5.1. Disaster Governance and Institutional Frameworks

India and Serbia have both established legal frameworks for disaster risk governance, but their institutional structures differ. India's Disaster Management Act (2005) created a multi-tiered framework with the National Disaster Management Authority (NDMA) coordinating across federal and state levels (NDMA, 2019). In contrast, Serbia consolidated its governance under the Law on Disaster Risk Reduction and Emergency Management (2018), emphasizing institutional integration and alignment with EU directives (Beli et al., 2024). While India's federal structure allows for regional diversity, Serbia pursues legal uniformity in line with European standards.

5.2. Artificial Intelligence and Emerging Technologies in Disaster Management

Both countries recognize the potential of AI and emerging technologies, but are at different stages. India's adoption is still in the experimental phase, with pilot projects in flood forecasting, drone surveillance, and COVID-19 contact tracing (Hanspal & Behera, 2024). Oversight remains fragmented, as AI use is regulated by data protection law and sectoral guidelines. Serbia, on the other hand, has articulated a structured vision through its AI Strategy (2020–2025), which integrates disaster management and public safety, heavily influenced by the EU Artificial Intelligence Act (2024), which categorizes disaster-management AI as a "high-risk" system subject to oversight (Rajlic et al., 2025). This positions Serbia ahead of India in embedding accountability into AI-driven disaster response.

5.3. Drone and Remote Sensing Governance

India has liberalized drone regulation under the Drone Rules, 2021, easing permissions for UAV deployment in disaster response and logistics (Gupta et al., 2025). However, oversight around data security and civilian privacy remains limited, raising concerns over surveillance and liability. Serbia does not yet have a stand-alone UAV law; drone operations are regulated under civil aviation safety rules, which are integrated into disaster management protocols. While the lack of a dedicated UAV law may slow deployment, it ensures alignment with European safety and liability standards.

5.4. Data Protection and Privacy in Emergencies

India's Digital Personal Data Protection Act (2023) introduces significant privacy safeguards, including consent-based data collection and penalties for breaches (Sonkar, 2025). However, emergency provisions allow broad state discretion, raising concerns about the proportionality of surveillance during crises. Serbia applies a GDPR-harmonized data protection regime, ensuring stricter rules for lawful processing and transparency, even during emergencies. While this offers stronger individual protections, critics note that GDPR's rigidity may delay urgent data flows in crises (Tanasić & Vladimir, 2024).

5.5. Legal Liability and Accountability Mechanisms

India and Serbia differ significantly in their legal frameworks for liability for technological failures in disaster management. India relies on a mix of product liability, consumer protection law, and

judicial interpretations (Singh, 2017), though its jurisprudence on emerging technologies remains underdeveloped. In contrast, Serbia's EU-based liability regime emphasizes proportionality, strict product liability, and accountability for data protection breaches (Muftić, 2025), offering greater transparency and accountability for AI and drone failures. Serbia also mandates independent oversight bodies, while India depends on executive agencies and courts for enforcement.

5.6. Convergences and Divergences

Both India and Serbia recognize technology as key to disaster resilience, but differ in legal sophistication:

- Convergences: Adoption of AI and drones in disaster contexts, recognition of privacy risks, and a policy focus on resilience.
- Divergences: Serbia's EU-aligned frameworks provide stricter liability and oversight, whereas India's more flexible frameworks are still evolving, with less emphasis on rights protection.

India benefits from flexibility and rapid innovation, while Serbia's model highlights the importance of embedding accountability and ethical safeguards. A hybrid approach, combining India's innovation with Serbia's regulatory rigour, could offer a balanced solution for other countries facing similar challenges.

Table 4. Comparative Dimensions of India and Serbia's Technology Governance in Disaster Management.

Dimension	India	Serbia
Anchor Disaster Law	Disaster Management Act, 2005	Law on Disaster Risk Reduction and Emergency Management, 2018
AI Governance	Emerging (DPDP Act 2023; sectoral guidelines)	AI Strategy (2020–2025); EU-aligned data-protection regime
Drone/UAV Regulation	Drone Rules, 2021 (liberalized but consent-based)	No stand-alone law; integrated via aviation safety & disaster response
Data Protection	Digital Personal Data Protection Act, 2023	GDPR-aligned Data Protection Act
Liability & Accountability	Evolving jurisprudence on product liability and privacy in tech use	Stronger EU-derived liability norms; emphasis on proportionality
Regional/Global Alignment	Domestic focus with partial convergence (e.g., AI Act debates)	Strong EU alignment; candidate for EU accession

6. Discussion and policy implications

The comparative analysis reveals a trade-off between India's flexible, decentralized disaster governance and Serbia's EU-aligned model that emphasizes legal certainty. India's system promotes innovation but lacks a harmonized liability framework, leading to uncertainty, particularly regarding privacy, drone accidents, and AI errors. In contrast, Serbia's EU-derived framework ensures accountability through strict product liability and GDPR safeguards, though it can slow innovation due to compliance costs and procedural delays.

Policy implication: A hybrid approach that combines India's flexibility with Serbia's accountability could strengthen disaster governance while avoiding delays in innovation.

Both case studies show that emerging technologies like AI, drones, and geospatial tools are increasingly used in disaster governance, raising complex liability and ethical concerns. For example, AI can improve flood forecasting but may introduce bias if datasets underrepresent vulnerable groups. Similarly, drones accelerate search-and-rescue efforts but can infringe on privacy if not prop-

erly regulated. Serbia's approach, guided by the EU AI Act, ensures risk classification and human oversight for AI systems, while India prioritizes rapid adoption with less emphasis on safeguards.

Policy implication: Disaster governance frameworks should embed technology-specific liability standards to ensure transparency in liability allocation, particularly for AI and drones.

Data protection is a key divergence between India and Serbia. India's Digital Personal Data Protection Act (2023) provides a foundation for regulating disaster-related data, but its broad emergency exemptions could undermine rights during crises. Serbia's GDPR-aligned framework places stricter limits, though it may slow critical data flows in emergencies.

Policy implication: A middle ground is needed—allowing temporary derogations in emergencies but requiring ex post independent audits to prevent abuse. Embedding sunset clauses and proportionality checks would strengthen both resilience and legitimacy.

In India, the absence of a comprehensive liability regime forces victims of technological failures to rely on tort law or consumer protection law, often resulting in lengthy delays and inconsistent remedies. Serbia's EU-inspired strict liability model ensures predictable outcomes but may discourage smaller innovators due to high compliance risks.

Policy implication: A tiered liability regime may offer a balanced approach: strict liability for manufacturers and vendors of high-risk technologies, such as AI systems and drones; shared responsibility between state agencies and private operators during deployment; insurance mechanisms to spread risk while encouraging innovation.

The India–Serbia comparison offers broader lessons for global disaster governance:

- Developing states may benefit from India's flexible approach, but should introduce accountability mechanisms over time.
- GDPR-aligned frameworks, like Serbia's, emphasize rights protection even in emergencies, though expedited processing is necessary.
- General data-protection or liability laws are insufficient; specific provisions for AI and drones are required.
- Independent oversight bodies should be introduced in emerging economies to enhance accountability without politicization.
- International organizations like UNDRR and the Sendai Framework can foster harmonization of technology governance principles to ensure interoperability and ethical standards in cross-border disaster response.

7. Conclusion

This comparative study of security governance and Legal liability in disaster management highlights the challenges and opportunities involved in regulating emerging technologies. Analyzing the approaches of India and Serbia shows that, although both countries are updating their regulatory frameworks to keep pace with technological advancements, there are still notable gaps—especially in assigning liability, ensuring security, and facilitating cross-border cooperation. The study indicates that both centralized and networked governance models involve trade-offs among security, efficiency, and flexibility. India's hierarchical system offers unified standards but faces implementation hurdles, while Serbia's networked approach provides integration benefits yet grapples with sovereignty concerns and dependency issues.

Key insights include: (1) traditional legal liability frameworks are insufficient for managing risks from new technologies, necessitating specialized laws and judicial adaptation; (2) security governance must strike a balance between protective measures and operational effectiveness through risk-based strategies and flexible regulation; (3) cross-border efforts should find a middle ground between sovereignty and effectiveness, using graduated levels of integration; and (4) effective governance depends on capacity building and involving multiple stakeholders to address complex technological challenges.

This study enriches the academic understanding of how technology is governed in disaster situations and offers practical guidance for policy development. The proposed hybrid governance model provides a flexible framework to tackle shared challenges while respecting each country's unique context. Future research should focus on how these recommendations are implemented and on the governance hurdles posed by emerging technologies in disaster management. As new innovations continue to reshape security landscapes, adaptable governance systems that balance innovation with protection will be vital for maintaining societal resilience and security.

Author Contributions: M.S.H. and V.M.C. conceived the original idea for this study and led the study design and overall methodological approach. V.M.C. coordinated the research process and manuscript development. M.S.H. and V.M.C. developed the indicator framework, collected, processed, and curated the data, and compiled the final dataset. M.S.H. conducted the primary analyses and produced the initial results and figures, while V.M.C. performed additional analyses, verified and validated the results, and refined the methodological and interpretation sections. V.M.C. drafted and substantially expanded the manuscript and led the revision and editing process, with input from M.S.H. M.L. contributed domain-specific input and critical review, providing comments and minor revisions. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Scientific–Professional Society for Disaster Risk Management, Belgrade (https://spsdrm.com/, accessed on 18 February 2026), International Institute for Disaster Research (https://idr.edu.rs/, accessed 18 February 2026), Belgrade, Serbia, and ProSafeNet - The Global Hub for Safety, Security, Risk & Emergency Professionals & Scientists (https://prosafenet.com/, accessed 18 February 2026).

Acknowledgements: This study was supported by the Scientific-Professional Society for Disaster Risk Management and ProSafeNet – The Global Hub for Safety, Security, Risk & Emergency Professionals and Scientists (https://prosafenet.com/). The authors acknowledge the use of Grammarly Premium and ChatGPT 5.2 to improve the English in this manuscript. The AI tools were used to assist with language enhancement, but were not involved in developing the scientific content. The authors take full responsibility for the originality, validity, and integrity of the manuscript.

8. References

1. Ahmad, R. (2024). Smart remote sensing network for disaster management: An overview. Telecommunication Systems, 87(1), 213–237.
2. Ahmed, I. (2025). Navigating ethics and risk in artificial intelligence applications within information technology: A systematic review. American Journal of Advanced Technology and Engineering Solutions, 1(1), 579–601.
3. Alabi, M. (2024, November). Ethical implications of AI: Bias, fairness, and transparency [Unpublished manuscript]. Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
4. Alakbarli, E. (2025). Risk assessment from multiple hazards in underground systems (Doctoral dissertation, Sapienza University of Rome). CERN Document Server (CERN-THESIS-2025-013). Retrieved from https://cds.cern.ch/record/2924681
5. Baladari, V. (2020). Adaptive cybersecurity strategies: Mitigating cyber threats and protecting data privacy. Journal of Scientific and Engineering Research, 7(8), 279–288.
6. Beli, A., Renner, R., Cvetković, V. M., Ivanov, A., & Gačić, J. (2025). A Cross-National Study of Disaster Risk Management: Strengths and Weaknesses in Bulgaria, Romania, and Albania with Reflections on Serbia. International Journal of Disaster Risk Management, 7(1), 431. https://doi.org/10.18485/ijdrm.2025.7.1.25
7. Bishwakarma, J. K., & Hu, Z. (2022). Problems and prospects for the South Asian Association for Regional Cooperation (SAARC). Politics & Policy, 50(1), 154–179.
8. Charak, A., Ravi, K., & Verma, A. (2024). Review of various climate change exacerbated natural hazards in India and consequential socioeconomic vulnerabilities. Journal of Integrated Disaster Risk Management, 13(2), 142–177.

9. Commission, S. A. M. to the E. (2025). Artificial Intelligence in Emergency and Crisis Management: Rapid Evidence Review Report. In Zenodo (CERN European Organization for Nuclear Research). European Organization for Nuclear Research. https://doi.org/10.5281/zenodo.17737962
10. Corbane, C., Eklund, G., Gyenes, Z., Lentini, A., San-Miguel, J., Durrant, T., ... Salari, S. (2024). Cross-border and emerging risks in Europe: Overview of state of science, knowledge and capacity (EUR 31944 EN; JRC137818). Luxembourg: Publications Office of the European Union.
11. Cvetković, V. M. (2024). In-Depth Analysis of Disaster (Risk) Management System in Serbia: A Critical Examination of Systemic Strengths and Weaknesses. Preprints.Org. https://doi.org/10.20944/preprints202405.0762.v1
12. Cvetković, V. M. (2024). In-Depth Analysis of Disaster (Risk) Management System in Serbia: A Critical Examination of Systemic Strengths and Weaknesses. Preprints.Org. https://doi.org/10.20944/preprints202405.0762.v1
13. Cvetković, V. M., & Miljković, N. (2024). Legal and Organizational Framework for the Use of Search and Rescue Dogs in Disasters: A Comparative Analysis between Serbia, Croatia, and Slovenia. Preprints.Org. https://doi.org/10.20944/preprints202407.0841.v1
14. Cvetković, V. M., Tanasić, J., Renner, R., Roković, V., & Beriša, H. (2024). Comprehensive risk analysis of emergency medical response systems in Serbian healthcare: Assessing systemic vulnerabilities in disaster preparedness and response. Healthcare, 12(19), 1962.
15. Dai, J., & Azhar, A. (2024). Collaborative governance in disaster management and sustainable development. Public Administration and Development, 44(4), 358–380.
16. Dejanović, M., & Kriviņš, A. (2025). Legal and financial regulation of AI in Serbia, Latvia, and the EU. Srpska Politička Misao, 94(6), 167. https://doi.org/10.5937/spm94-59321
17. Dine, F. (2024, September). Cyber threat analysis and the development of proactive security strategies for risk mitigation [Manuscript]. Retrieved from ResearchGate.
18. Du, J. (2025). Toward responsible and beneficial AI: Comparing regulatory and guidance-based approaches—A comprehensive comparative analysis of artificial intelligence governance frameworks across the European Union, United States, China, and IEEE (arXiv preprint arXiv:2508.00868). Retrieved from https://arxiv.org/abs/2508.00868
19. George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51–75.
20. Government of the Republic of Serbia. (2025, January 10). Serbia adopts strategy for the development of artificial intelligence for the period 2025–2030. Retrieved from https://ai.gov.rs/vest/en/1296/serbia-adopts-strategy-for-the-development-of-artificial-intelligence-for-the-period-20252030.php
21. Gupta, R., Sharma, S. K., & Stevelal, S. (2025). TSAW Drones: Revolutionizing India's drone logistics with digital technologies. Communications of the Association for Information Systems, 55, 1121–1142.
22. Hanspal, M. S. (2024). Cyber-legal infrastructure: A new frontier in disaster management for Digital India. International Journal of Law Management and Humanities, 7(6), 1079–1089.
23. Hanspal, M. S., & Behera, B. (2024). Role of emerging technology in disaster management in India: An overview. International Journal of Disaster Risk Management, 6(2), 133–148.
24. Hanspal, M. S., & Behera, B. (2024). Role of Emerging Technology in Disaster Management in India: An Overview. International Journal of Disaster Risk Management, 6(2), 133. https://doi.org/10.18485/ijdrm.2024.6.2.9
25. Hanspal, M. S., & Behera, B. (2024). The Disaster Management Act, 2005: A critical review. DME Journal of Law, 5(1), 42–53.
26. Havu, K., Saleev, R., Polad, D., Pfau, D., Heydari, T., & Mäkelä, A.-S. (2024). Regulating Liability for AI-Induced Harm: Developments in EU Law and Insights from a Research Project. https://doi.org/10.2139/ssrn.4861450

27. He, S., Zhou, Y., Yang, Y., Liu, T., Zhou, Y., Li, J., ... Guan, X. (2024). Cascading failure in cyber–physical systems: A review on failure modeling and vulnerability analysis. IEEE Transactions on Cybernetics, 54(12), 7936–7954.
28. Ikeda, S., & Nagasaka, T. (2011). An emergent framework of disaster risk governance towards innovating coping capability for reducing disaster risks in local communities. International Journal of Disaster Risk Science, 2(2), 1–9.
29. Johnson, R., McIntosh, C., & Tropasso, C. (2023). Deploying modern technology for disaster management practitioners. In H. J. Scholl, E. E. Holdeman, & F. K. Boersma (Eds.), Disaster management and information technology: Professional response and recovery management in the age of disasters (pp. 25–34). Cham, Switzerland: Springer.
30. Kalinaki, K. (2024). Ransomware threat mitigation strategies for protecting critical infrastructure assets. In M. Ahmed (Ed.), Ransomware evolution (pp. 120–143). Boca Raton, FL: CRC Press.
31. Kešetović, Ž., & Samardžija, V. (2014). Regional civil security cooperation in South Eastern Europe: The case of disaster preparedness and prevention initiative. Public Policy and Administration, 13(2), 209–221.
32. Khan, A., Gupta, S., & Gupta, S. K. (2022). Emerging UAV technology for disaster detection, mitigation, response, and preparedness. Journal of Field Robotics, 39(6), 905–955.
33. Kirpalani, C. (2024). Technology-driven approaches to enhance disaster response and recovery. In S. Kanga, G. Meraj, S. K. Singh, M. Farooq, & M. S. Nathawat (Eds.), Geospatial technology for natural resource management (pp. 25–81). Hoboken, NJ: Wiley-Scrivener.
34. Klinke, A., & Renn, O. (2012). Adaptive and integrative governance on risk and uncertainty. Journal of Risk Research, 15(3), 273–292.
35. Kordi, M., & Ertz, M. (2025). Deciphering technological advancements for efficient disaster management and community resilience. Technology in Society, 84, 103057. https://doi.org/10.1016/j.techsoc.2025.103057
36. Krichen, M., Abdalzaher, M. S., Elwekeil, M., & Fouda, M. M. (2024). Managing natural disasters: An analysis of technological advancements, opportunities, and challenges. Internet of Things and Cyber-Physical Systems, 4, 99–109.
37. Krivokapić, Đ., Živković, I., & Nikolić, A. (2022). Artificial Intelligence Regulation in the Areas of Data Protection, Information Security, and Anti-discrimination in Western Balkan Economies. 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), 1233. https://doi.org/10.23919/mipro55190.2022.9803678
38. Leong, W. Y. (2025). Internet of Things for Enhancing Public Safety, Disaster Response, and Emergency Management. 61. https://doi.org/10.3390/engproc2025092061
39. Lescrauwaet, L., Wagner, H., Yoon, C., & Shukla, S. (2022). Adaptive legal frameworks and economic dynamics in emerging technologies: Navigating the intersection for responsible innovation. Law and Economics, 16(3), 202–220.
40. Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. Security and Privacy, 6(6), e318.
41. Lyu, M., Zhao, Y., Huang, C., & Huang, H. (2023). Unmanned aerial vehicles for search and rescue: A survey. Remote Sensing, 15(13), 3266.
42. Malhotra, C., & Malhotra, U. (2024). Putting interests of digital nagriks first: Digital personal data protection (DPDP) Act 2023 of India. Indian Journal of Public Administration, 70(3), 516–531.
43. Mandloi, D., Arya, R., & Verma, A. K. (2024). Internet of drones. In R. Arya, S. C. Sharma, A. K. Verma, & B. Iyer (Eds.), Recent trends in artificial intelligence towards a smart world: Applications in industries and sectors (pp. 353–373). Singapore: Springer Nature Singapore.
44. Milenković, D. (2025). Theoretical, Institutional and Organizational Aspects of the Integrated Disaster Risk Reduction System: Towards a Deeper Understanding of Disaster Resilience

in Serbia. International Journal of Contemporary Security Studies, 1(1), 175. https://doi.org/10.18485/fb_ijcss.2025.1.1.13

45. Milenković, D., Cvetković, V. M., Ivanov, A., & Renner, R. (2024). Impact of Cyber Space on Security in the Context of Armed Conflicts: Towards Disaster Risk Resilience. Preprints.Org. https://doi.org/10.20944/preprints202412.1099.v1
46. Milenković, D., Cvetković, V. M., Ivanov, A., & Renner, R. (2024). Impact of Cyber Space on Security in the Context of Armed Conflicts: Towards Disaster Risk Resilience. Preprints.Org. https://doi.org/10.20944/preprints202412.1099.v1
47. Mitchell, J. K. (2022). Megacity disaster risk governance. In Oxford Research Encyclopedia of Natural Hazard Science. Oxford University Press. Retrieved from https://oxfordre.com/naturalhazardscience/view/10.1093/acrefore/9780199389407.001.0001/acrefore-9780199389407-e-377
48. Muftić, N. (2025). Bases of liability. In Artificial intelligence and tortious liability: Case study of Bosnia and Herzegovina (pp. 97–151). Cham, Switzerland: Springer Nature Switzerland.
49. Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain-based governance models in e-government: A comprehensive framework for legal, technical, ethical and security considerations. International Journal of Law and Management, 67(1), 37–55.
50. Nuredin, A. (2022). An evaluation of the legal liability of artificial intelligence and robotics in Balkan states (Slovenia, Serbia and North Macedonia). Vision International Scientific Journal, 7(1), 9–20.
51. Okolo, F. C., Etukudoh, E. A., Ogunwole, O. L., Osho, G. O., & Basiru, J. O. (2021). Systematic review of cyber threats and resilience strategies across global supply chains and transportation networks. Iconic Research and Engineering Journals, 4(9), 204–217.
52. Oniani, D., Hilsman, J., Peng, Y., Poropatich, R. K., Pamplin, J. C., Legault, G. L., & Wang, Y. (2023). Adopting and expanding ethical principles for generative artificial intelligence from military to healthcare. NPJ Digital Medicine, 6(1), 225.
53. Ottun, A. R. O., & Flores, H. (2025, October 23). Trustworthy AI in practice: A comprehensive review of human oversight and human-in-the-loop approaches [Preprint]. TechRxiv. Retrieved from https://www.techrxiv.org/users/688001/articles/1346357
54. Pandey, N., Rani, P., & Kundu, S. (2025). An intelligent disaster management system: Integrating technology for effective response and recovery. In Proceedings of the 2025 3rd International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC) (pp. 1107–1112). Piscataway, NJ: IEEE.
55. Patidar, N., Mishra, S., Jain, R., Prajapati, D., Solanki, A., Suthar, R., ... Patel, H. (2024). Transparency in AI decision making: A survey of explainable AI methods and applications. Advances of Robotic Technology, 2(1), 000110.
56. Petrović, M. (2019). EU integration process of Serbia: A vicious circle of high politics? The Review of International Affairs, 70(1175), 23–48.
57. Raftopoulos, M., Pertoldi-Bianchi, S., Eleftherios, P., & Kjelmann, K. G. (2024). Conceptualizing the Nexus between Disaster Risk Reduction and Climate Change Adaption and Mitigation in Governance. Research Portal Denmark, 2024(3), 172. Retrieved from https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=aau&id=aau-4383f7e9-8d76-4169-9202-c1936d86740c&ti=Conceptualizing%20the%20Nexus%20between%20Disaster%20Risk%20Reduction%20and%20Climate%20Change%20Adaption%20and%20Mitigation%20in%20Governance
58. Rajlić, J. Z., Đoković, J. S., Piljak, A. D., & Panić, N. R. (2025, September). Implementation of environmental principles in the Republic of Serbia [Conference paper]. Retrieved from ResearchGate.
59. Rane, N. L., Mallick, S. K., & Rane, J. (2025). Artificial intelligence and machine learning for enhancing resilience: Concepts, applications, and future directions. Mumbai, India: Deep Science Publishing.

60. Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8), 4060.
61. Schlegelmilch, J. (2020). Rethinking readiness: A brief guide to twenty-first-century megadisasters. New York, NY: Columbia University Press.
62. Sharma, C. (2012). Remedies for environmental harm: Dharmic duty and tort liability in India—is there a common ground? Macquarie Journal of International and Comparative Environmental Law, 8(1), 48–70.
63. Singh, A. (Ed.). (2017). Disaster law: Emerging thresholds. Abingdon, England: Routledge
64. Sonkar, A. (2025). The Digital Personal Data Protection Act, 2023: Analysing its implications, challenges, and future prospects. International Cybersecurity Law Review, 6(4), 547–569.
65. Subash, B., & Whig, P. (2025). Principles and frameworks. In Ethical dimensions of AI development (pp. 1–22). Hershey, PA: IGI Global.
66. Tanasić, J., & Cvetković, V. M. (2024). The efficiency of disaster and crisis management policy at the local level: Lessons from Serbia. Belgrade, Serbia: Scientific-Professional Society for Disaster Risk Management.
67. Tariq, B., Ashraf, M. R., & Rashid, U. (2025). Ethical imperatives in AI design: A comprehensive framework for risk mitigation and responsible innovation. Ubiquitous Technology Journal, 1(2), 61–73.
68. Uddin, M. S., Haque, C. E., & Khan, M. N. (2021). Good governance and local level policy implementation for disaster-risk-reduction: Actual, perceptual and contested perspectives in coastal communities in Bangladesh. Disaster Prevention and Management: An International Journal, 30(2), 94–111.
69. United Nations Office for Disaster Risk Reduction (UNISDR). (2015). Sendai framework for disaster risk reduction 2015–2030. Geneva, Switzerland: Author. Retrieved from https://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf
70. Vidović, N., Beriša, H., & Cvetković, V. M. (2024). Optimising Disaster Resilience Through Advanced Risk Management and Financial Analysis of Critical Infrastructure in the Serbian Defence Industry. International Journal of Disaster Risk Management, 6(2), 183. https://doi.org/10.18485/ijdrm.2024.6.2.12.
71. Visave, J. (2024). AI in emergency management: Ethical considerations and challenges. Journal of Emergency Management and Disaster Communications, 5(1), 165–183.
72. World Health Organization. (2024). Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models. Geneva, Switzerland: World Health Organization.
73. Roković, V., & Stanojević, P. (2024). Disaster Risk Reduction Education Through Digital Technologies in the Context of Education for Sustainable Development: A Curricula Analysis of Security and Defense Studies in Serbia. Sustainability, 16(22), 9777. https://doi.org/10.3390/su16229777
74. Yamah, D., & Folorunsho, T. (2026). Leveraging Social Media and Mobile Technology for Disaster Communication in Nigeria. International Journal of Disaster Risk Management, 1–30. https://doi.org/10.66050/x77jr639
75. Van Grembergen, W. (Ed.). (2004). Strategies for information technology governance. Idea Group Publishing.