Procedural Flexibility and Legitimacy in Crisis Governance: A Survey of the EU Digital Services Act and Comparative Regulatory Frameworks

Abstract

This survey paper examines the dynamic interrelation between procedural flexibility, legitimacy, and crisis governance within the European Union, with a particular focus on the EU Digital Services Act (DSA). It explores how digital transformation and large digital platforms influence governance, emphasizing the need for adaptive regulatory frameworks. The paper evaluates the DSA's effectiveness in ensuring transparency, accountability, and consumer protection while fostering innovation. Through comparative analysis, it highlights the diversity of global regulatory approaches, contrasting the EU's comprehensive model with the more market-driven frameworks in the US and UK. The survey underscores the importance of legitimacy and expertise in regulatory processes, particularly in integrating advanced technologies like AI. It also addresses the challenges of ICT-based capitalism, advocating for robust global governance systems. Key findings suggest that while the DSA represents a significant step towards harmonized digital regulation, ongoing refinement and international cooperation are essential to address emerging challenges. Future directions include enhancing digital resilience, ethical data practices, and integrating advanced decision support systems to improve crisis management and regulatory efficacy.

1 Introduction

1.1 Contextual Background

Crisis governance is increasingly intertwined with digital technologies and artificial intelligence (AI), necessitating an understanding of procedural flexibility and legitimacy. The regulation of AI is essential for leveraging its benefits while managing associated risks [1]. However, adherence to Trustworthy AI governance practices remains inconsistent, complicating the regulatory landscape, particularly in democratic settings where automated decision-making can undermine legitimacy and public trust [2, 3].

The COVID-19 pandemic highlighted the urgent need for procedural flexibility and legitimacy, exposing IT-related challenges that call for adaptive governance frameworks [4]. It underscored the importance of flexible resource allocation strategies during crises, such as evacuations, which demand dynamic governance mechanisms [5]. Furthermore, the pandemic's impact on sectors like education demonstrated the necessity for effective leadership and procedural adaptability to safeguard stakeholders and maintain essential services [6].

In the European Union, the relationship between crisis management and political secrecy requires a nuanced understanding of how crises can trigger political secrecy, thereby affecting governance transparency and legitimacy [7]. The rising complexity and frequency of cybersecurity incidents impacting essential services in Europe further underscore the need for structured approaches to enhance cyber resilience, emphasizing the role of adaptive governance mechanisms [4].

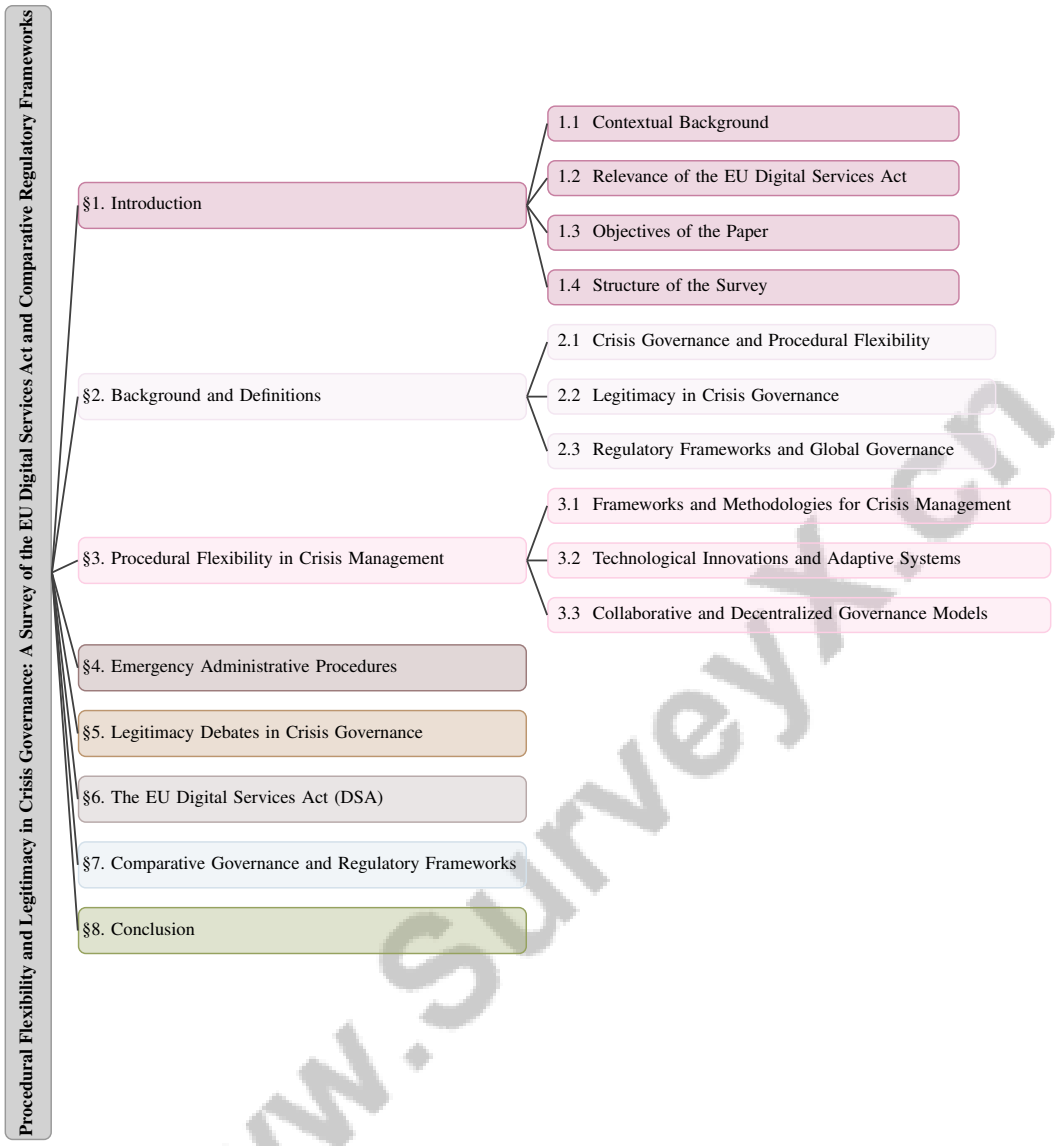


Figure 1: chapter structure

Effective crisis management hinges on the collaboration of all stakeholders, particularly in unpredictable environments [8]. This collaborative approach is crucial for efficient emergency management, as evidenced in nuclear crises where decision-making support systems are vital. Additionally, the disparity between regulatory frameworks and the practical implementation of AI ethics highlights the necessity of operationalizing principles to bridge this gap [1].

The evolving landscape of crisis governance requires robust frameworks that ensure procedural flexibility while maintaining legitimacy. As digital technologies reshape governance processes, the ability to adapt and uphold public trust will be crucial for managing future crises [3].

1.2 Relevance of the EU Digital Services Act

The EU Digital Services Act (DSA) serves as a pivotal element in the regulatory framework for digital services, addressing the complex challenges posed by digital transformation and the dominance of large platforms [9]. This legislation is vital for enhancing digital sovereignty in the EU, providing a structured approach to content moderation, algorithmic transparency, and disinformation mitigation [10]. By establishing clear obligations for intermediary service providers, the DSA aims to harmonize the digital market, ensuring fair competition and protecting consumer rights in the digital era [11].

AI-generated, for reference only.

A key feature of the DSA is its alignment with other regulatory measures, such as the Digital Markets Act (DMA), to collectively reform digital market regulations in the EU [12]. This synergy reflects the EU's commitment to countering the influence of major tech companies and fostering a competitive digital economy. The DSA also governs intermediary services, addressing regulatory implications related to copyright laws and online content-sharing obligations under the CDSM Directive [13].

In crisis governance, the DSA's focus on transparency and accountability is essential for developing effective crisis communication strategies, particularly during emergencies where real-time data and predictive analytics are critical for informed decision-making [14]. The introduction of the NIS Directive and its update, NIS2, complements the DSA by mandating EU Member States and Operators of Essential Services to establish baseline cybersecurity capabilities, thereby enhancing the resilience of digital infrastructures [15].

Moreover, the DSA addresses the challenges of regulating digital technologies without hindering innovation, ensuring that pre-digital transformation regulatory frameworks are appropriately adapted [6]. As digital services evolve, the DSA's role in crisis governance becomes increasingly important, providing a comprehensive framework for managing the complexities of digital transformation and maintaining legitimacy among EU citizens.

1.3 Objectives of the Paper

This survey paper aims to analyze the intricate dynamics of crisis governance and digital service regulation within the EU, focusing on the EU Digital Services Act (DSA). A primary objective is to examine how procedural flexibility and legitimacy are upheld amid rapid digital transformation and the rising influence of digital platforms [10]. The paper seeks to evaluate the effectiveness of regulatory frameworks established by the DSA and the Digital Markets Act (DMA) in addressing regulatory challenges, protecting consumers, ensuring fair competition, and fostering innovation.

A significant aspect of the survey is a comparative analysis of crisis management methodologies across various nations, aiming to address knowledge gaps left by outdated directives, such as the e-Commerce Directive from 2000 [16]. This includes examining crisis management practices in sectors like hospitality and tourism, identifying existing knowledge voids [17], and addressing governance crises related to managing extraordinary flows of refugees and migrants, highlighting the need for proficient crisis management planning.

Furthermore, the survey investigates the relationship between crisis management capacity and legitimacy, drawing insights from the Norwegian government's response to the COVID-19 pandemic and assessing how AI can enhance the legitimacy of political processes through empirical evidence. It also explores the impact of echo chambers on information consumption, particularly how political preferences shape engagement with reliable versus questionable news sources [18].

The paper evaluates the DSA's effectiveness in combating online disinformation and addressing challenges posed by emerging AI technologies [19]. It investigates the intersection of consumer protection and human rights within the digital services sector, emphasizing implications for investors [20], and examines the evolution of public attitudes towards COVID-19 apps, identifying factors influencing their adoption [21].

Additionally, the paper proposes a model for evolving data governance into information governance, bridging digital and non-digital information exchange [22]. It analyzes discrepancies between the DSA and previous European case law regarding general monitoring obligations [11], and addresses the need for improved preparedness, shared situational awareness, and coordinated incident response to enhance cybersecurity resilience [15]. The survey further explores the operationalization of the Blueprint for an AI Bill of Rights, encompassing principles like safety, privacy, explainability, fairness, and human fallback options [23]. Ultimately, it examines the causal significance of procedure and performance as sources of legitimacy, dissecting these dimensions into specific institutional qualities [24].

1.4 Structure of the Survey

The survey is organized to provide a thorough examination of crisis governance and digital service regulation, with a specific focus on the EU Digital Services Act (DSA) and its interaction with other regulatory frameworks such as the Digital Markets Act (DMA). The paper commences with

an introduction that establishes the context for understanding procedural flexibility and legitimacy in crisis governance, highlighting the relevance of the DSA. Following this, the survey presents a detailed analysis of the contextual background, emphasizing current challenges in crisis governance, particularly in migration and asylum contexts, and the urgent need for adaptive regulatory mechanisms to address the complexities of multilevel governance, legal fragmentation, and the evolving landscape of financial technologies [25, 26, 27].

Subsequent sections delve into the significance, objectives, and key provisions of the DSA, including a comparative analysis with previous EU legislation like the e-Commerce Directive and GDPR [28]. This is followed by an in-depth discussion on procedural flexibility in crisis management, showcasing frameworks and methodologies that facilitate adaptive responses to emergencies.

The survey then shifts its focus to emergency administrative procedures, analyzing their role and implementation within the EU and other jurisdictions. This section also addresses the impact of these procedures on governance during crises, emphasizing crisis communication, public engagement, and data-driven decision support.

Legitimacy debates in crisis governance are explored in detail, particularly within the EU context, examining how legitimacy is maintained or challenged during crises. A critical assessment of public trust, perception, and cultural factors reveals their significant influence on the legitimacy of international organizations, underscoring the importance of both procedural and performance-related aspects. By analyzing these dynamics across various global governance issues, the study emphasizes the necessity for international organizations to cultivate legitimacy through transparent and accountable practices that resonate with diverse audiences [29, 24].

The penultimate section provides an overview of the DSA, its objectives, and key provisions, with a focus on content moderation and algorithmic transparency. The survey concludes with a comparative analysis of governance and regulatory frameworks, highlighting similarities and differences in procedural flexibility and legitimacy concerns across regions. The PHOENI2X Cyber Resilience Framework is also discussed, illustrating the integration of AI to enhance cybersecurity capabilities [15].The following sections are organized as shown in Figure 1.

2 Background and Definitions

2.1 Crisis Governance and Procedural Flexibility

Crisis governance necessitates procedural flexibility to effectively address emergencies' unpredictable nature, ensuring efficacy and legitimacy in dynamic scenarios. Such adaptability is crucial for frameworks facilitating adaptive decision-making and resource allocation, safeguarding vulnerable populations [5]. The complexity of cybersecurity incidents further underscores the need for robust incident management capabilities, highlighting procedural flexibility's role in enhancing crisis governance [4].

Technological advancements, particularly AI, contribute significantly to procedural flexibility by providing decision-makers with responsive tools. However, AI compliance processes' complexity, requiring multiple steps and human oversight, presents governance challenges [2]. The absence of structured accountability in AI development and deployment complicates governance, potentially leading to adverse outcomes [6].

In the digital realm, procedural flexibility is vital for navigating evolving legal landscapes concerning intermediary liability and regulatory frameworks, exemplified by the EU Digital Services Act (DSA) [10]. The DSA emphasizes transparency and accountability in platform operations, countering the monopolistic control of digital spaces by major tech corporations that threaten democratic discourse and market fairness.

The collaborative city digital twin framework illustrates procedural flexibility, enabling adaptive responses through real-time data integration and stakeholder collaboration [4]. This framework is crucial for coordinated actions among diverse stakeholders, as in road accident scenarios where collaborative decision-making is often inadequate [8]. Adapting existing methodologies to novel crises, particularly through innovative social media data usage, underscores procedural flexibility's importance in crisis management.

Ultimately, procedural flexibility is essential for managing vast amounts of noisy data in real time, ensuring accurate information for decision-making. By fostering collaboration among various actors, including NGOs and local governments, crisis governance systems can enhance their effectiveness in emergency management. This collaborative approach is vital for efficient resource management and timely aid delivery during crises, exemplified by the Aerial-based Crisis Management Center (ACMC), which uses flexible UAS for real-time communications and computational resources tailored to crisis management applications [4].

2.2 Legitimacy in Crisis Governance

Legitimacy in crisis governance significantly impacts policy-making and governance effectiveness. Institutional characteristics shape legitimacy beliefs, yet specific attributes generating these beliefs remain underexplored [24]. The complexity of crises, such as the COVID-19 pandemic, necessitates governance frameworks extending beyond traditional response phases to include prevention, preparedness, recovery, and rehabilitation [30].

Global governance institutions (GGIs) have faced legitimacy challenges since the 1990s, highlighting the need for legitimacy in addressing major policy issues [7]. Digital technologies and AI's incorporation into crisis governance complicates the legitimacy landscape, as these innovations can enhance and undermine democratic values. Automation enables strategic task focus, yet the volume of data and misinformation on digital platforms complicates effective decision-making.

Transparency and accountability are essential for legitimate governance, particularly in the digital era. Current data governance mechanisms often fall short, exacerbating challenges in protecting individual rights and ensuring efficient crisis responses [6]. Integrating computational methods into digital twin frameworks offers a promising approach to enhancing legitimacy by simulating real-time scenarios, such as contaminant dispersion and optimizing evacuation routes [14].

Using secrecy to maintain authority during crises raises contentious legitimacy issues. While secrecy can manage public perception and maintain order, it often conflicts with democratic principles of transparency and accountability, particularly in AI and digital governance contexts, where a lack of transparency may foster public distrust and resistance [7].

Leadership effectiveness is crucial for sustaining legitimacy during crises. From a contingency theory perspective, leadership strategies must adapt to a crisis's situational demands to ensure decisions are perceived as legitimate and trustworthy, vital for maintaining business continuity and public confidence amid sudden operational changes [8].

2.3 Regulatory Frameworks and Global Governance

Regulatory frameworks underpin global governance, providing the legal and institutional structures necessary for effective crisis management. These frameworks facilitate coordinated and transparent responses, essential for addressing modern crises' complexities. Integrating advanced technologies, such as machine learning, into these frameworks offers sophisticated tools for evaluating and managing diverse crisis scenarios [31].

The EU's Digital Services Act (DSA) and Digital Markets Act (DMA) exemplify comprehensive regulatory efforts overseeing the digital ecosystem. These acts impose new obligations on service providers, enhancing regulatory oversight while potentially stifling innovation and market entry for startups in Europe [28]. The DSA's provisions, particularly regarding copyright enforcement, illustrate the challenges of aligning new regulations with existing legal frameworks [32].

A comparative analysis of global regulatory approaches reveals diverse models, such as the DMCA's conditional immunity framework contrasted with the DSA's broader regulatory expectations. This diversity underscores the various strategies employed by different regions to address similar digital governance challenges [33]. The World Trade Organization (WTO) plays a crucial role in global telecommunications regulation, emphasizing international cooperation in establishing effective regulatory standards [34]. The EU significantly influences global governance by shaping telecommunications policies and setting precedents in digital regulation [34].

Blockchain technology's role in regulatory frameworks, particularly within GovTech applications, is noteworthy. By providing decentralized solutions for data management and verification, blockchain

presents a robust framework relevant to crisis management [35]. The categorization of the DSA and DMA into stages of regulatory integration reflects the EU's commitment to principles such as non-discrimination and the direct effect of EU law, ensuring harmonization across member states [36].

The concentration of power among a few large digital platforms poses significant challenges to democratic processes and market fairness in Europe [9]. This situation necessitates regulatory frameworks that manage crises and address broader issues of equity and justice in the digital age. A comparative analysis of AI regulatory frameworks across the EU, China, and the US highlights the global diversity in regulatory approaches, emphasizing the need for adaptive governance models accommodating regional differences while adhering to global standards [37].

In the context of regulatory frameworks, the evolution of FinTech regulation, including innovations such as regulatory sandboxes and RegTech, is pertinent. These developments illustrate the dynamic nature of regulatory approaches and their relevance to global governance [26]. Furthermore, categorizing cryptocurrency regulations into various stances—ranging from bans to supportive regulation—demonstrates the diverse regulatory landscapes globally [38].

In recent years, the complexity of crisis management has necessitated an examination of procedural flexibility, which is essential for effective response strategies. As illustrated in Figure 2, the hierarchical structure of procedural flexibility encompasses various frameworks and methodologies, alongside technological innovations and collaborative governance models. This figure delineates how each category is subdivided into critical components, including ontology-based knowledge bases, AI and automated decision-making, and decentralized governance models. These elements collectively emphasize their significant roles in enhancing crisis response and management, thereby underscoring the importance of an integrated approach to navigating crises effectively.

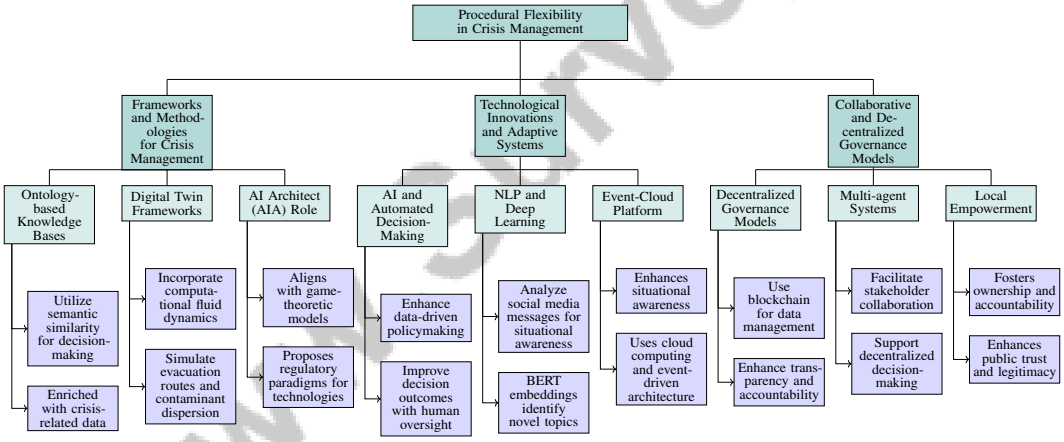


Figure 2: This figure illustrates the hierarchical structure of procedural flexibility in crisis management, highlighting frameworks and methodologies, technological innovations, and collaborative governance models. Each category is further divided into key components such as ontology-based knowledge bases, AI and automated decision-making, and decentralized governance models, emphasizing their roles in enhancing crisis response and management.

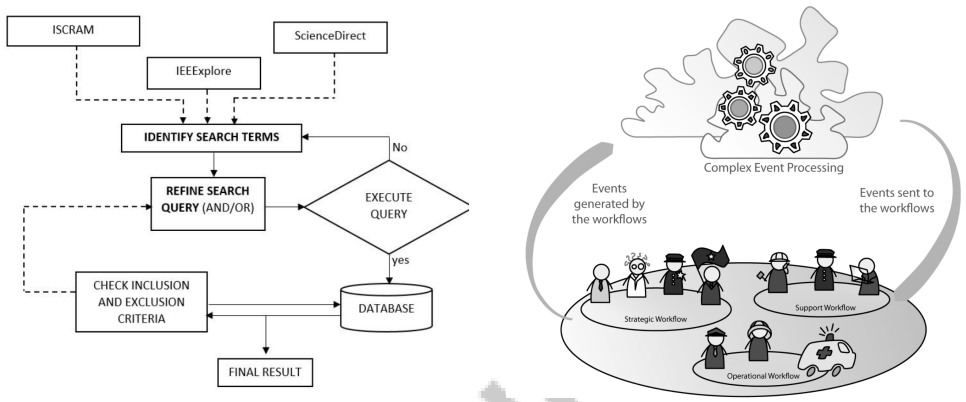
3 Procedural Flexibility in Crisis Management

3.1 Frameworks and Methodologies for Crisis Management

Crisis management requires adaptable frameworks and methodologies to navigate emergencies' complexities. Ontology-based knowledge bases, enriched with crisis-related data, utilize semantic similarity to identify analogous situations, aiding informed decision-making [39]. Digital twin frameworks, incorporating computational fluid dynamics and hybrid analysis, optimize evacuation routes and simulate contaminant dispersion, enhancing response strategies [14]. Large Language Models (LLMs) improve emergency communication processing, providing insights that support procedural flexibility [40].

The AI Architect (AIA) role underscores accountability in AI governance, aligning with game-theoretic models that propose regulatory paradigms for emerging technologies [6, 41]. The Technology-Organization-Environment (TOE) framework categorizes challenges for Emergency Management Agencies (EMAs) in adopting social media analytics, emphasizing adaptive methodologies [8]. This framework facilitates social media data integration into structured formats, enhancing crisis response through clustering and analysis [42].

Machine learning models with causal reasoning provide predictive insights into migration patterns, aiding adaptive strategies to mitigate infrastructure impacts [43]. The Aerial-based Crisis Management Center (ACMC) assembles Unmanned Aerial Systems (UAS) into Aerial Virtual Data Centers (AVDCs) for efficient resource allocation [4]. The Digital Services Act (DSA) introduces due diligence obligations, enhancing digital governance's regulatory landscape [13].



(a) A Flowchart of a Search Process for Scientific Research[31]

(b) Complex Event Processing in a Multi-Workflows System[44]

Figure 3: Examples of Frameworks and Methodologies for Crisis Management

Figure 4 illustrates the key frameworks and methodologies in crisis management, emphasizing ontology-based knowledge for semantic similarity and knowledge mining, digital twin frameworks for optimizing evacuation routes and simulating contaminant dispersion, and the use of large language models to enhance emergency communication and procedural flexibility. The first component, a search process flowchart, highlights the importance of systematic data collection, critical for accurate crisis management. The second component, complex event processing, underscores the necessity of coordination and flexibility in managing crises.

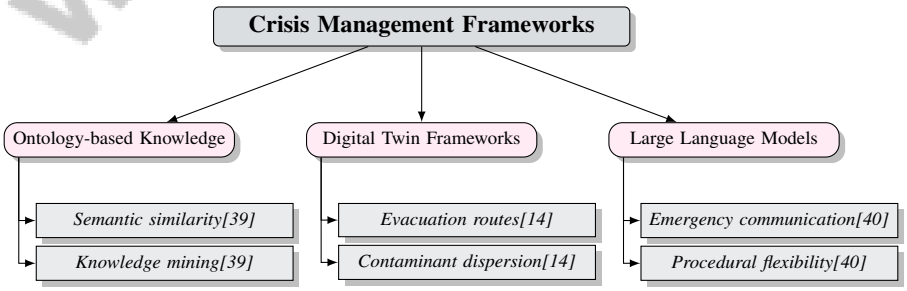


Figure 4: This figure illustrates the key frameworks and methodologies in crisis management, emphasizing ontology-based knowledge for semantic similarity and knowledge mining, digital twin frameworks for optimizing evacuation routes and simulating contaminant dispersion, and the use of large language models to enhance emergency communication and procedural flexibility.

3.2 Technological Innovations and Adaptive Systems

Technological advancements are pivotal in enhancing adaptive crisis management systems, improving decision-making and resource allocation during emergencies. AI and automated decision-making (ADM) systems integrated into crisis frameworks enhance data-driven policymaking and decision outcomes, particularly with human oversight [45]. These systems facilitate accurate forecasting and strategic planning in dynamic crisis environments.

Deep learning and natural language processing (NLP) technologies are essential for analyzing social media messages, contributing to adaptive crisis management systems by processing large data volumes for improved situational awareness [46]. BERT embeddings fine-tuned on crisis-related tweets identify novel topics, enhancing system adaptability [47].

The Event-Cloud Platform uses cloud computing and event-driven architecture to enhance situational awareness and decision-making in emergencies [44]. The PHOENI2X framework integrates AI tools for coordinated cybersecurity incident responses, highlighting technological innovation's role in crisis management [15].

Multiagent decision support systems enable effective crisis management by analyzing complex data sets and providing actionable insights [48]. The NGO-RMSD system uses blockchain to enhance NGO coordination and resource management during disasters [49]. Game-theoretic models optimize resource distribution by conceptualizing crisis locations as strategic players [50]. The Continual Distributed Learning for Crisis Management (CDLCM) methodology integrates federated and continual learning for efficient disaster-related tweet processing [51].

3.3 Collaborative and Decentralized Governance Models

Collaborative and decentralized governance models enhance procedural flexibility in crisis management by leveraging distributed networks and collective decision-making. Integrating ontologies and multi-agent systems facilitates stakeholder collaboration, improving communication and coordination [52]. This approach aligns various actors' objectives and actions for cohesive crisis responses.

Decentralized governance models, particularly those using blockchain, offer innovative frameworks for data management and verification, enhancing transparency and accountability. These models empower local decision-making and resource allocation, as demonstrated by projects like ALERT and NGO-RMSD, employing smart contracts and participatory approaches to improve coordination and resource delivery [49, 22, 53, 54]. Decentralization reduces single points of failure, enhancing governance systems' resilience. Multi-agent systems support decentralized decision-making by enabling autonomous collaboration and resource optimization.

Integrating collaborative and decentralized models into crisis governance frameworks encourages diverse perspectives and expertise, essential for addressing modern crises' multifaceted nature. Empowering local actors fosters ownership and accountability, enhancing public trust and legitimacy in governance processes. Research shows legitimacy in global governance is influenced by procedural and performance-related aspects and diverse social actors' active participation. Promoting local engagement addresses community-specific needs and contributes to governance institutions' broader legitimacy [7, 22, 29, 24]. Decentralized systems' flexibility allows rapid adaptation of strategies and policies, ensuring governance systems remain effective and responsive throughout crises.

4 Emergency Administrative Procedures

4.1 Crisis Communication and Public Engagement

Crisis communication and public engagement are vital components of emergency administrative procedures, facilitating effective information dissemination and trust-building during emergencies. Timely, accurate information is essential for mitigating impacts and ensuring public safety. The integration of Explainable Artificial Intelligence (XAI) into crisis communication frameworks, as mandated by AI Architect (AIA) obligations, enhances transparency and accountability, thereby bolstering public confidence in crisis management systems [6].

Technological advancements significantly augment crisis communication strategies. Geographic Information Systems (GIS) are crucial for spatial analysis, aiding evacuation planning and optimizing

resource allocation [55]. Large Language Models (LLMs) enhance emergency communication systems by improving the clarity and dissemination of critical information during crises [40]. Blockchain technology provides secure, transparent platforms for information exchange, thus fostering public trust through enhanced accountability in communication [35]. The Digital Services Act (DSA) further reinforces these efforts by promoting accountability and transparency in content moderation, thus strengthening trust in digital communication platforms [56].

The media plays a pivotal role in conveying government messages, influencing public perception and engagement. Effective media strategies ensure accurate information dissemination, bridging the communication gap between authorities and the public [57]. Advanced clustering methods, such as Semantic Vector Optimization for Semantic Similarity-based Text Clustering (SVOSSTC), organize information into semantically meaningful clusters, enhancing decision-making and crisis communication effectiveness [42].

Innovative frameworks like the Aerial-based Crisis Management Center (ACMC) showcase the potential of advanced technologies in crisis communication. Utilizing deep neural network-based coordination frameworks, ACMC ensures adaptive resource allocation and robust communication channels during crises, facilitating effective resource deployment [4].

4.2 Data-Driven Decision Support

Data-driven decision support systems are integral to emergency administrative procedures, providing insights that enhance situational awareness and inform effective crisis response strategies. As illustrated in Figure 5, the hierarchical structure of these systems highlights the critical roles of machine learning, deep learning, and social media analytics in enhancing crisis management capabilities. Machine learning techniques enable the analysis of vast data from diverse sources, including social media, which is crucial for real-time crisis management. These methods, as evaluated by Okpala et al., facilitate the processing and interpretation of social media data to assess situations, evaluate risks, and guide decision-making [31].

The use of factual agents in multi-agent decision support systems, as discussed by Kebair et al., exemplifies data-driven approaches in crisis management by creating detailed representations of the crisis environment, aiding risk assessment and informed decision-making [48]. Establishing a coherent framework for statistical inference enhances the reliability and accuracy of crisis management strategies [58].

Deep Learning-based classification techniques, highlighted by Padhee et al., effectively categorize social media messages during crises, improving the quality of information available to decision-makers [46]. The Continual Distributed Learning for Crisis Management (CDLCM) methodology, as noted by Priyanshu et al., leverages federated learning to classify raw textual data, supporting public utility services in maintaining operational continuity during emergencies [51].

Adopting social media analytics, emphasized by Stieglitz et al., enhances situational awareness by providing timely information that can dynamically adjust response strategies [8]. This capability is vital for maintaining an adaptive crisis management framework, enabling governance systems to effectively navigate modern emergency complexities.

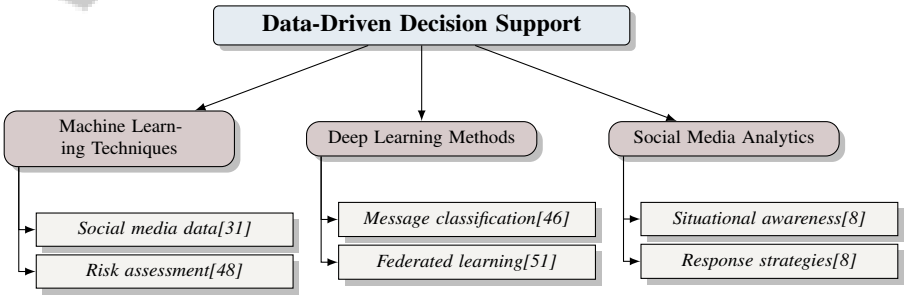


Figure 5: This figure illustrates the hierarchical structure of data-driven decision support systems, highlighting the role of machine learning, deep learning, and social media analytics in enhancing crisis management capabilities.

4.3 Transparency and Accountability in Automated Systems

Benchmark	Size	Domain	Task Format	Metric

Table 1: This table provides a comprehensive overview of various benchmarks used in the evaluation of automated decision-making systems. It categorizes these benchmarks based on their size, domain, task format, and the metrics employed for assessment. Such detailed classification aids in understanding the diverse landscape of evaluation criteria applicable to transparency and accountability in automated systems.

Transparency and accountability are crucial in deploying automated systems, particularly within crisis management, to maintain public trust and ensure alignment with democratic values and ethical standards [45]. Integrating automated decision-making (ADM) systems in crisis governance necessitates a robust framework that prioritizes transparency, allowing stakeholders to comprehend decision-making processes and influencing factors. Table 1 offers a detailed classification of representative benchmarks crucial for assessing transparency and accountability in automated decision-making systems within crisis management contexts.

Process mining is a key tool for enhancing transparency and accountability in ADM systems, offering clear visualizations of compliance processes that identify gaps and improve adherence to regulatory requirements [2]. This capability is essential for ensuring automated systems operate within established legal and ethical boundaries, especially in high-stakes environments like crisis management.

Implementing transparency measures in ADM systems involves developing XAI frameworks that elucidate complex algorithms and decision-making processes. These frameworks provide stakeholders with insights into decision-making, thereby enhancing accountability and fostering trust in automated systems [45]. Continuous monitoring and auditing of ADM systems are critical to ensure compliance with regulatory standards and address potential biases or errors in decision-making processes.

5 Legitimacy Debates in Crisis Governance

5.1 Public Trust and Perception

Public trust and perception are pivotal to crisis governance legitimacy, influencing policy implementation and compliance. Effective collaboration between human and machine actors within crisis management frameworks is crucial, as highlighted by the integration of automation [59]. Technologies like the Aerial-based Crisis Management Center (ACMC) enhance resource allocation and communication, boosting public confidence in crisis responses [4]. The democratization of technologies challenges traditional governance structures, impacting public perception and trust. AI regulatory frameworks emphasize accountability to sustain public trust [6].

To illustrate these dynamics, Figure 6 presents a comprehensive overview of key aspects of crisis governance trust, focusing on human-machine interaction, the role of AI in crisis management, and the challenges to public trust. This figure underscores the importance of automation, AI accountability, and effective resource allocation in fostering public confidence. Advanced clustering methods, such as Semantic Vector Optimization for Semantic Similarity-based Text Clustering (SVOSSTC), improve situational awareness by creating semantically rich clusters from social media data, enhancing decision-making relevance [42]. Real-time insights into compliance processes aid crisis communication strategies, enabling proactive risk management [2]. However, challenges like inadequate training for Emergency Management Agency (EMA) personnel and resistance to social media analytics adoption hinder public trust enhancement [8]. Addressing these issues is essential for effective communication and adaptability in legitimate crisis governance.

5.2 Balancing Effectiveness and Democratic Legitimacy

Balancing effectiveness and democratic legitimacy in crisis governance involves reconciling swift action with adherence to democratic principles and accountability. This balance is critical in rapidly evolving crises, where urgent responses may conflict with procedural rigor [60]. The COVID-19 pandemic exemplifies this tension, as governments enacted public health measures while maintaining

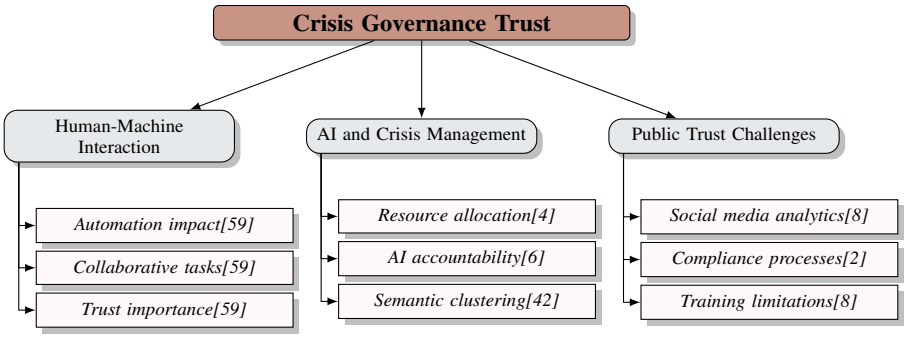


Figure 6: This figure illustrates key aspects of crisis governance trust, focusing on human-machine interaction, AI and crisis management, and public trust challenges, highlighting the importance of automation, AI accountability, and effective resource allocation.

trust in democratic processes [57]. Crises require rapid decision-making based on incomplete information, straining governance legitimacy, especially when public perceptions are swayed by misinformation and institutional distrust [29]. Regulatory frameworks like the Digital Services Act (DSA) must address issues like hate speech while respecting democratic freedoms [56]. Blockchain integration into governance frameworks offers transparency and accountability but faces scalability and jurisdictional challenges [38]. Innovative regulatory approaches are needed to accommodate decentralized technologies while safeguarding democratic values. Engaging citizen volunteers in crisis management enhances democratic legitimacy by fostering participation and trust, leading to inclusive and responsive systems aligned with democratic ideals [5].

5.3 Cultural and Contextual Considerations

Cultural and contextual factors crucially influence crisis governance legitimacy. Cultural norms vary across regions, necessitating customized crisis management approaches that respect local customs. Tailored strategies are essential for addressing crises effectively, as diverse stakeholders may respond differently [25, 27, 61]. Cultural sensitivity ensures governance actions are perceived as legitimate and accepted locally. The global nature of crises, like pandemics and climate change, complicates cultural integration in governance. Multinational organizations must navigate diverse cultural and regulatory environments, requiring a comprehensive understanding of cultural dynamics and flexible frameworks [27]. Contextual elements, including political, economic, and social conditions, impact crisis governance legitimacy by affecting resource availability, communication capacity, and public trust. In politically unstable and economically disparate regions, governance faces challenges in gaining legitimacy and ensuring adherence to public health measures. Fragmented actor landscapes, complex legal frameworks, and renationalization narratives further complicate crisis management effectiveness, as seen in varied COVID-19 responses where trust and communication were key [60, 25, 62, 30]. Automated decision-making systems in crisis governance must balance transparency with sensitive information protection, ensuring cultural and contextual sensitivity to maintain public trust and legitimacy [3].

6 The EU Digital Services Act (DSA)

6.1 Objectives and Key Provisions of the DSA

The EU Digital Services Act (DSA) establishes a unified regulatory framework for digital services across the European Union, enhancing accountability and transparency among online intermediaries [16]. It employs a tiered regulatory approach, with general obligations for all intermediaries, additional obligations for hosting services, and specific measures for very large online platforms (VLOPs) and search engines (VLOSEs), based on their size and influence.

A core component of the DSA is its focus on risk assessment and mitigation, requiring platforms to uphold democratic norms and protect fundamental rights within the EU [63]. These provisions address the dominance of large digital platforms, promoting a fair and competitive digital market while

safeguarding consumer protection and human rights [20]. Despite its progress, the DSA underscores ongoing technological and legal challenges necessitating further exploration and refinement [56].

The DSA introduces specific monitoring obligations for online platforms, reflecting a shift towards stricter compliance, as seen in various Court of Justice of the European Union (CJEU) cases [11]. These obligations integrate legal norms into data systems, ensuring compliance with regulatory standards [64]. The interplay between the DSA and the CDSM Directive is crucial for establishing a clear legal framework for Online Content-Sharing Service Providers (OCSSPs), ensuring digital services operate within defined legal parameters [13].

In crisis management, the DSA's provisions on content moderation, algorithmic transparency, and disinformation are particularly relevant, offering a structured framework to maintain digital service integrity during emergencies [10]. Advanced classification methods, as noted by Brunila, further aid crisis managers by providing coherent and interpretable topics for informed decision-making [47].

6.2 Content Moderation and Algorithmic Transparency

The DSA significantly advances the regulation of digital platforms, focusing on content moderation and algorithmic transparency. It aims to ensure accountability and transparency in online platforms, addressing concerns about the influence of large digital entities on public discourse and democratic processes [16].

Content moderation under the DSA is designed to curb illegal content while respecting fundamental rights, including freedom of expression. The Act mandates platforms to implement effective mechanisms for detecting, reporting, and removing illegal content, ensuring transparency and oversight in these processes [65]. By categorizing platforms based on size and impact, the DSA places greater responsibility on VLOPs in managing content, reflecting their significant role in shaping public communication [28].

Algorithmic transparency is another critical aspect of the DSA, requiring platforms to clarify their algorithmic decision-making processes, particularly those affecting content visibility and user engagement. This transparency is crucial for maintaining public trust and addressing concerns about algorithmic bias and manipulation [63]. The integration of advanced AI technologies, such as Large Language Models (LLMs), into crisis management frameworks highlights the potential of algorithmic transparency in enhancing situational awareness and decision-making [40].

AI technologies significantly enhance content moderation by improving search operations, information integration, and coordination among responders through multi-agent systems [66]. These technologies enable platforms to manage vast information volumes during crises, ensuring content moderation aligns with the DSA's regulatory objectives.

7 Comparative Governance and Regulatory Frameworks

7.1 Comparative Analysis with Other Regulatory Frameworks

Examining regulatory frameworks globally reveals significant differences in digital services and artificial intelligence (AI) management. The EU's Digital Services Act (DSA) exemplifies a comprehensive approach emphasizing transparency, accountability, and consumer protection, contrasting with the more lenient and deregulatory tendencies in the United States and the United Kingdom [67]. The U.S. regulatory environment favors innovation and market-driven solutions, prioritizing economic growth over strict oversight [68]. Conversely, the DSA mandates digital platforms to adhere to democratic norms and protect fundamental rights, illustrating the EU's commitment to a balanced digital market. Post-Brexit, the UK seeks a unique regulatory identity, blending EU comprehensiveness with U.S. deregulatory strategies, focusing on flexibility and adaptability to encourage innovation while ensuring consumer protection and market competitiveness [67]. This is evident in the UK's approach to platforms like Uber, where a balance between market freedom and regulatory control is pursued [68]. Germany, on the other hand, adopts a more restrictive stance, emphasizing stringent measures to protect existing industries and uphold national standards, thus maintaining high regulatory benchmarks against disruptive entrants [68].

7.2 Legitimacy and Expertise in Regulatory Frameworks

Legitimacy and expertise are pivotal in crafting and executing regulatory frameworks for digital services and crisis governance. The interaction between regulatory frameworks, advancing technologies, and socio-political contexts significantly influences the effectiveness and public acceptance of regulations, especially in complex areas like AI and cybersecurity. Traditional regulatory methods may be inadequate in these dynamic environments, necessitating innovative paradigms that embrace the chaotic nature of these technologies while underscoring the need for human oversight to enhance ethical standards and transparency [41, 69, 70]. The DSA enhances legitimacy through mechanisms ensuring transparency and accountability in digital platforms, safeguarding democratic values and consumer rights [16]. Its emphasis on risk assessment and mitigation further underscores its commitment to democratic norms and fundamental rights [63]. Expertise is crucial for addressing complex regulatory challenges, particularly with AI integration into regulatory processes, requiring a nuanced understanding of technological and ethical implications [45]. The inclusion of roles such as the AI Architect (AIA) within governance frameworks exemplifies the need for specialized knowledge to ensure accountability and compliance [6]. Variations in regulatory approaches across jurisdictions highlight differing emphases on legitimacy and expertise, with the EU prioritizing comprehensive oversight while the U.S. adopts a market-driven approach, reflecting distinct legal traditions and policy priorities [67].

7.3 Global Regulatory Systems and ICT-Based Capitalism

The convergence of global regulatory systems with ICT-based capitalism creates a complex landscape where technological advancements and economic models interact with regulatory frameworks to shape the digital economy. ICT-based capitalism, characterized by the dominance of information and communication technologies, transforms traditional economic structures, necessitating robust regulatory systems to address its implications. Global regulatory systems must balance ICT-based capitalism's innovative potential with the need for oversight and accountability, ensuring fair and transparent digital markets that safeguard consumer rights and promote competition. The DSA exemplifies this approach by harmonizing digital service regulations across member states, addressing issues like content moderation, algorithmic transparency, and platform accountability. By imposing obligations on digital platforms, the DSA aims to mitigate risks associated with market power concentration and the proliferation of illegal content, thereby enhancing digital ecosystem integrity [10]. Integrating blockchain technology into regulatory frameworks offers promising solutions for enhancing transparency and accountability in ICT-based capitalism. Its decentralized nature provides a secure method for managing digital transactions and data, reducing reliance on centralized authorities and the risks of fraud [35]. This technology can transform regulatory practices by enabling more efficient processes in areas like supply chain management, financial services, and digital identity verification. However, implementing global regulatory systems in the context of ICT-based capitalism faces significant challenges. The rapid pace of technological innovation often outstrips regulatory bodies' ability to adapt, leading to oversight gaps. Additionally, the global nature of digital platforms complicates jurisdictional boundaries, necessitating international cooperation and harmonization of regulatory standards to effectively address cross-border issues [67].

8 Conclusion

8.1 Future Directions and Challenges

The landscape of crisis governance and digital regulatory frameworks is evolving rapidly, presenting both challenges and opportunities as new technologies emerge. Research should prioritize refining digital resilience frameworks to address digital inequalities highlighted by crises like the COVID-19 pandemic. This involves developing adaptive regulatory frameworks that balance user protection with innovation incentives. Longitudinal studies on the EU Digital Services Act (DSA) are essential to evaluate its long-term impact on digital services regulation and AI governance, including standardized metrics for disinformation regulation and shifts in legitimacy over time. Integrating constraint-based recommender systems into agent-based simulations can enhance crisis management, necessitating enriched ontologies and constraints to effectively navigate evolving crisis scenarios.

Practical frameworks and tools must be developed to ensure regulatory compliance while maintaining ethical data practices. Future research should focus on optimizing hyperparameters for broader applicability, critical for advancing crisis governance and regulatory frameworks. This includes improving detection technologies, exploring alternative content moderation strategies, and addressing ethical implications. Refining integration algorithms for Intelligent Decision Support Systems (IDSS) and applying them across various domains is crucial for future advancements in crisis governance.

Future studies should also explore the long-term impacts of suppression strategies on public health and economic recovery, as seen during the COVID-19 pandemic. Decentralized and robust service infrastructures for optimizing data collection and analysis are vital for enhancing crisis governance. Empirical validation of proposed governance frameworks in real-world blockchain scenarios is necessary. Evaluating platforms like the Event-Cloud Platform in real emergency contexts, assessing their adaptability to diverse crisis types, and understanding cultural influences on emergency management stakeholders are essential research areas. Future efforts should refine models for improved performance, address ethical concerns, and investigate additional applications of LLMs in emergency management. Developing distributed governance models and addressing technical challenges in linking digital identities with physical counterparts are critical for advancing crisis governance.

Addressing these future directions and challenges will fortify crisis governance and regulatory frameworks, ensuring resilience and adaptability in an increasingly digital environment. Research should also refine smart regulation concepts and explore the implications of emerging technologies on financial regulation, identifying future pathways and challenges. Incorporating socio-economic indicators and expanding networks to include a broader range of variables can enhance understanding of migration dynamics in crisis contexts. Investigating questions across human-machine network contexts, such as social media and knowledge creation networks, will further improve crisis governance effectiveness. Future research should explore alternative linguistic typologies and advanced clustering techniques to enhance semantic clustering processes and address identified limitations.

Efforts must build on existing initiatives to ensure inclusivity in the regulatory process and adapt to the changing landscape of AI technologies. Developing robust algorithms for process mining to navigate diverse and complex AI compliance scenarios is another vital research area. Creating a dynamic system for real-time resource management is essential for addressing challenges in crisis governance. Lastly, fostering international cooperation to harmonize regulations and address unique challenges posed by emerging technologies in the cryptocurrency sector is crucial for future research. Enhancing the robustness of the Aerial-based Crisis Management Center (ACMC) under various crisis scenarios and exploring advanced DNN training methods for improved coordination are significant areas for future exploration. Developing tailored educational and regulatory frameworks for the AIA, alongside pilot programs to evaluate effectiveness in real-world applications, will further enrich the discourse.

AI-generated, for reference only.

References

[1] Olivia J. Erdélyi and Judy Goldsmith. Regulating artificial intelligence: Proposal for a global solution, 2020.

[2] Andrew Pery, Majid Rafiei, Michael Simon, and Wil M. P. van der Aalst. Trustworthy artificial intelligence and process mining: Challenges and opportunities, 2021.

[3] Niko Tsakalakis, Sophie Stalla-Bourdillon, Trung Dong Huynh, and Luc Moreau. A taxonomy of explanations to support explainability-by-design, 2024.

[4] Hossein Rastgoftar and Salim Hariri. Aerial-based crisis management center (acmc), 2024.

[5] Ngoc Luyen Le, Jinfeng Zhong, Elsa Negre, and Marie-Hélène Abel. Système de recommandations basé sur les contraintes pour les simulations de gestion de crise, 2023.

[6] Labhaoise NiFhaolain, Andrew Hines, and Vivek Nallur. Statutory professions in ai governance and their consequences for explainable ai, 2023.

[7] Jonas Tallberg, Karin Bäckstrand, and Jan Aart Scholte. *Legitimacy in global governance: Sources, processes, and consequences*. Oxford University Press, 2018.

[8] Stefan Stieglitz, Milad Mirbabaie, Jennifer Fromm, and Stefanie Melzer. The adoption of social media analytics for crisis management–challenges and opportunities. 2018.

[9] Annegret Bendiek. Integrationspolitische bedeutung des digital service act (dsa) und digital markets act (dma). *Stiftung Wissenschaft und Politik*, 2021.

[10] János Tamás Papp. Moving forward: Charting the much-needed evolution of the digital services act. In *Hungarian Yearbook of International Law and European Law 2024*, pages 457–476. Nomos Verlagsgesellschaft mbH & Co. KG, 2024.

[11] Gergely Gosztonyi, Ewa Galewska, and Andrej Skolkay. Challenges of monitoring obligations in the european union's digital services act. *ELTE LJ*, page 45, 2024.

[12] Maria Luisa Chiarella. Digital markets act (dma) and digital services act (dsa): New rules for the eu digital environment. *Athens JL*, 9:33, 2023.

[13] João Pedro Quintais and Sebastian Felix Schwemer. The interplay between the digital services act and sector regulation: how special is copyright? *European Journal of Risk Regulation*, 13(2):191–217, 2022.

[14] Max von Danwitz, Jacopo Bonari, Philip Franz, Lisa Kühn, Marco Mattuschka, and Alexander Popp. Contaminant dispersion simulation in a digital twin framework for critical infrastructure protection, 2024.

[15] Konstantinos Fysarakis, Alexios Lekidis, Vasileios Mavroeidis, Konstantinos Lampropoulos, George Lyberopoulos, Ignasi Garcia-Milà Vidal, José Carles Terés i Casals, Eva Rodriguez Luna, Alejandro Antonio Moreno Sancho, Antonios Mavrelos, Marinos Tsantekidis, Sebastian Pape, Argyro Chatzopoulou, Christina Nanou, George Drivas, Vangelis Photiou, George Spanoudakis, and Odysseas Koufopavlou. Phoeni2x – a european cyber resilience framework with artificial-intelligence-assisted orchestration, automation and response capabilities for business continuity and recovery, incident response, and information exchange, 2023.

[16] Tambiama Madiega. Digital services act. *Regulation*, page 2065, 2022.

[17] Tai Ming Wut, Jing Bill Xu, and Shun-mun Wong. Crisis management research (1985–2020) in the hospitality and tourism industry: A review and research agenda. *Tourism Management*, 85:104307, 2021.

[18] Niccolò Di Marco, Matteo Cinelli, and Walter Quattrociocchi. Reliability of content and echo chambers on youtube during the covid-19 debate, 2022.

[19] Luca Nannini, Eleonora Bonel, Davide Bassi, and Michele Joshua Maggini. Beyond phase-in: assessing impacts on disinformation of the eu digital services act. *AI and Ethics*, pages 1–29, 2024.

[20] Cristina Elena Popa Tache. About the human rights and consumer protection in the digital age of digital services act 2022 or what aspects interested investors should pay attention to. *International Investment Law Journal*, 3(2):121–132, 2023.

[21] Marvin Kowalewski, Christine Utz, Martin Degeling, Theodor Schnitzler, Franziska Herbert, Leonie Schaewitz, Florian M. Farke, Steffen Becker, and Markus Dürmuth. 52 weeks later: Attitudes towards covid-19 apps for different purposes over time, 2023.

[22] Philippe Page, Paul Knowles, and Robert Mitwicki. Distributed governance: a principal-agent approach to data governance – part 1 background core definitions, 2023.

[23] Alex Oesterling, Usha Bhalla, Suresh Venkatasubramanian, and Himabindu Lakkaraju. Operationalizing the blueprint for an ai bill of rights: Recommendations for practitioners, researchers, and policy makers, 2024.

[24] Lisa Maria Dellmuth, Jan Aart Scholte, and Jonas Tallberg. Institutional sources of legitimacy for international organisations: Beyond procedure versus performance. *Review of International Studies*, 45(4):627–646, 2019.

[25] Zeynep Sahin-Mencutek, Soner Barthoma, N Ela Gökalp-Aras, and Anna Triandafyllidou. A crisis mode in migration governance: comparative and analytical insights. *Comparative Migration Studies*, 10(1):12, 2022.

[26] Dirk A Zetzsche, Ross P Buckley, Janos N Barberis, and Douglas W Arner. Regulating a revolution: from regulatory sandboxes to smart regulation. *Fordham J. Corp. & Fin. L.*, 23:31, 2017.

[27] W Timothy Coombs and Daniel Laufer. Global crisis management–current research and future directions. *Journal of International Management*, 24(3):199–203, 2018.

[28] Bence Kis Kelemen and Balázs Hohmann. Is there anything new under the sun? a glance at the digital services act and the digital markets act from the perspective of digitalisation in the eu. *Croatian Yearbook of European Law and Policy*, 19:225–248, 2023.

[29] Jonas Tallberg and Michael Zürn. The legitimacy and legitimation of international organizations: Introduction and framework, 2019.

[30] Frederick M Burkle Jr. Challenges of global public health emergencies: development of a health-crisis management framework. *The Tohoku journal of experimental medicine*, 249(1):33–41, 2019.

[31] Izunna Okpala, Shane Halse, and Jess Kropczynski. Machine learning methods for evaluating public crisis: Meta-analysis, 2023.

[32] Alexander Peukert, Martin Husovec, Martin Kretschmer, Péter Mezei, and João Pedro Quintais. European copyright society–comment on copyright and the digital services act proposal. *IIC-International Review of Intellectual Property and Competition Law*, 53(3):358–376, 2022.

[33] Martin Husovec. Rising above liability: The digital services act as a blueprint for the second generation of global internet rules. *Berkeley Tech. LJ*, 38:883, 2023.

[34] Seamus Simpson and Rorden Wilkinson. Conceptualising regulatory change - explaining shifts in telecommunications governance, 2001.

[35] Anwitaman Datta. Blockchain in the government technology fabric, 2019.

[36] Annegret Bendiek. The impact of the digital service act (dsa) and digital markets act (dma) on european integration policy. *Working Paper Research Division EU/Europe 2021*, (02):15, 2021.

[37] Jon Chun, Christian Schroeder de Witt, and Katherine Elkins. Comparative global ai regulation: Policy perspectives from the eu, china, and the us, 2024.

[38] Xihan Xiong and Junliang Luo. Global trends in cryptocurrency regulation: An overview, 2024.

[39] Ngoc Luyen Le, Marie-Hélène Abel, and Elsa Negre. Recognizing similar crises through the application of ontology-based knowledge mining, 2024.

[40] Hakan T. Otal and M. Abdullah Canbaz. Llm-assisted crisis management: Building advanced llm platforms for effective emergency response and public collaboration, 2024.

[41] Dimitri Kusnezov and Wendell B. Jones. Are some technologies beyond regulatory regimes?, 2017.

[42] Charlie Kingston, Jason R. C. Nurse, Ioannis Agrafiotis, and Andrew Milich. Using semantic clustering to support situation awareness on twitter: The case of world views, 2018.

[43] Kenneth Lai and Svetlana Yanushkevich. Causal models applied to the patterns of human migration due to climate change, 2023.

[44] Matthieu Lauras, Frederick Benaben, Sebastien Truptil, and Aurelie Charles. Event-cloud platform to support decision- making in emergency management, 2015.

[45] Christopher Starke and Marco Lünich. Artificial intelligence for political decision-making in the european union: Effects on citizens' perceptions of input, throughput, and output legitimacy. *Data & Policy*, 2:e16, 2020.

[46] Swati Padhee, Tanay Kumar Saha, Joel Tetreault, and Alejandro Jaimes. Clustering of social media messages for humanitarian aid response during crisis, 2020.

[47] Mikael Brunila, Rosie Zhao, Andrei Mircea, Sam Lumley, and Renee Sieber. Bridging the gap between supervised classification and unsupervised topic modelling for social-media assisted crisis management, 2021.

[48] Fahem Kebair and Frédéric Serin. Towards a multiagent decision support system for crisis management, 2014.

[49] Arzu Özkan, Umutcan Korkmaz, Cemal Dak, and Enis Karaarslan. A decentralized resource management system proposal for disasters: Ngo-rmsd (stk-akys), 2022.

[50] Rudrashis Majumder, Rakesh R Warier, and Debasish Ghose. Game-theoretic model based resource allocation during floods, 2021.

[51] Aman Priyanshu, Mudit Sinha, and Shreyans Mehta. Continual distributed learning for crisis management, 2021.

[52] Ahmed Maalel and Henda Ben Ghézala. Towards a collaborative approach to decision making based on ontology and multi-agent system application to crisis management, 2020.

[53] Frédéric Le Mouël, Carlos Barrios Hernández, Oscar Carrillo, and Gabriel Pedraza. Decentralized, robust and efficient services for an autonomous and real-time urban crisis management, 2017.

[54] Andrej Zwitter and Jilles Hazenberg. Decentralized network governance: blockchain technology and the future of regulation. *Frontiers in Blockchain*, 3:12, 2020.

[55] Sara Shaker Abed El-Hamied, Ahmed Abou El-Fotouh Saleh, and Aziza Asem. Survey on using gis in evacuation planning, 2012.

[56] Ioanna Tourkochoriti. The digital services act and the eu as the global regulator of the internet. *Chi. J. Int'l L.*, 24:129, 2023.

[57] Tom Christensen and Per Lægreid. The coronavirus crisis—crisis communication, meaning-making, and reputation management. *International public management journal*, 23(5):713–729, 2020.

[58] Jim Q. Smith, Martine J. Barons, and Manuele Leonelli. Coherent frameworks for statistical inference serving integrating decision support systems, 2015.

[59] Asbjørn Følstad, Vegard Engen, Ida Maria Haugstveit, and Brian Pickering. Automation in human-machine networks: How increasing machine agency affects human agency, 2017.

[60] Tom Christensen and Per Lægreid. Balancing governance capacity and legitimacy: how the norwegian government handled the covid-19 crisis as a high performer. *Public Administration Review*, 80(5):774–779, 2020.

[61] Nataliia Gavkalova, Liudmyla Akimova, and Oleksandr Akimov. Anti-crisis management mechanism in the digital age. *Marketing i menedžment innovacij*, 14(4):188–199, 2023.

[62] Christian Kreuder-Sonnen. Political secrecy in europe: Crisis management and crisis exploitation. In *Secrecy in European Politics*, pages 134–156. Routledge, 2020.

[63] Anupam Chander. When the digital services act goes global. *Berkeley Tech. LJ*, 38:1067, 2023.

[64] Serge Abiteboul and Julia Stoyanovich. Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation, 2019.

[65] Ilaria Buri and Joris van Hoboken. The digital services act (dsa) proposal: a critical overview. *Digital Services Act (DSA) Observatory*, 2021.

[66] Khaled M. Khalil, M. Abdel-Aziz, Taymour T. Nazmy, and Abdel-Badeeh M. Salem. The role of artificial intelligence technologies in crisis response, 2008.

[67] Sangchul Park. Bridging the global divide in ai regulation: A proposal for a contextual, coherent, and commensurable framework, 2024.

[68] Kathleen Thelen. Regulating uber: The politics of the platform economy in europe and the united states. *Perspectives on politics*, 16(4):938–953, 2018.

[69] Alejandro Tlaie. Using ai alignment theory to understand the potential pitfalls of regulatory frameworks, 2024.

[70] Cary Coglianese and Colton R. Crum. Taking training seriously: Human guidance and management-based regulation of artificial intelligence, 2024.

Disclaimer:

SurveyX is an AI-powered system designed to automate the generation of surveys. While it aims to produce high-quality, coherent, and comprehensive surveys with accurate citations, the final output is derived from the AI's synthesis of pre-processed materials, which may contain limitations or inaccuracies. As such, the generated content should not be used for academic publication or formal submissions and must be independently reviewed and verified. The developers of SurveyX do not assume responsibility for any errors or consequences arising from the use of the generated surveys.