LEGALITY : JOURNAL OF LAW AND LEGAL STUDIES
Volume 1 No 1 2026

PUBLION

# Digital Sovereignty, Data Protection, and Transnational Regulatory Authority in Fragmented Governance

**Samuel Chisa**
Faculty of Law, Rivers State University, Nigeria
*Corresponding author:* samuel.chisa@ust.edu.ng

## Abstract
*This study emerges from growing concern over the vulnerability of economies facing repeated global disruption, including war, oil shocks, trade conflict, technological change, and broader geopolitical instability. Although economic resilience has become an important concept in contemporary scholarship, existing discussions often treat institutions, innovation, and inclusive growth as separate determinants rather than as interconnected foundations of long-term adaptability. The purpose of this study is to develop an integrated analytical framework explaining how institutional robustness, innovation dynamics, and inclusive growth jointly shape economic resilience. The study employs a qualitative conceptual research design based on analytical framework development. It uses document-based analysis of scholarly arguments and conceptual discussions related to economic resilience, institutions, innovation, and inclusive development. The analysis is organized around three main dimensions—institutional robustness, innovation dynamics, and inclusive growth—with economic resilience as the overarching analytical outcome. Through relational synthesis, the study maps how these dimensions interact under conditions of global disruption and geopolitical uncertainty. The principal results show that economic resilience is best understood as a systemic and relational capacity produced by the interaction of robust institutions, adaptive innovation, and socially broad development pathways. The study concludes that resilience becomes stronger and more durable when governance capacity, transformative adaptation, and inclusion operate as an integrated foundation rather than as isolated factors. Its main contribution is to provide a more coherent conceptual framework for understanding economic resilience in an era of prolonged uncertainty and structural disruption.*

## Keyword
*economic resilience; institutions; innovation; inclusive growth*

## 1. Introduction

Digital transformation has intensified the importance of data in legal, political, and economic life. As digital systems expand across borders, data protection becomes more central to the organization of transnational governance (Boru et al., 2025). It is no longer sufficient to understand data only as a technical resource or an object of commercial exchange. Data now sits at the intersection of rights, regulation, infrastructure, and state authority. In this setting, the idea of digital sovereignty has become increasingly visible in public and legal debate. It reflects growing concern over who governs digital spaces, who controls data circulation, and who defines valid regulatory standards. This development changes the wider context in which data protection is interpreted and applied. As a result, data protection must be read within a broader transformation of regulatory order in the digital age.

This issue is highly relevant because digital governance now shapes everyday life, national policy, and international coordination. States, firms, and regulatory institutions are all involved in struggles over the legal control of digital environments. These struggles are not abstract because they affect how data moves, where it is stored, and under whose

Received: 9 January 2026 Revised: 9 February 2026 Published: 21 March 2026

authority it is processed (Bouckaert & Galego, 2024). In practical terms, disputes over data governance influence market access, legal compliance, public administration, and strategic autonomy. They also shape the capacity of states to protect domestic priorities while remaining connected to transnational digital systems. For this reason, the question of data protection cannot be separated from the wider politics of regulatory power. The real-world relevance of this issue lies in the fact that legal decisions about data are also decisions about jurisdiction, infrastructure, and authority (Afolabi & Raifu, 2024). This makes the transformation of data protection a central concern in contemporary digital regulation.

Existing discussions have already established that data protection is closely associated with privacy and the protection of individual rights. In this conventional view, the primary function of data protection law is to safeguard personal information from misuse or unauthorized access. This perspective has been important because it gives data protection a clear normative foundation. At the same time, scholarship has also addressed the growing importance of cross-border data flows in a globally connected digital environment. Other debates have examined state authority and the capacity of governments to regulate digital actors and infrastructures. These discussions provide valuable insight into the complexity of digital governance. They show that privacy, transnational connectivity, and regulatory authority are all significant components of the digital legal order. However, they are often treated as parallel issues rather than as deeply interconnected dimensions of one regulatory transformation (Mubangizi, 2025).

What remains less developed is a clear explanation of how these issues interact under the rise of digital sovereignty. When privacy, cross-border data flows, and regulatory authority are examined separately, the broader restructuring of legal meaning becomes difficult to capture. The changing role of data protection cannot be fully understood if it is reduced to the protection of individual rights alone. Such a narrow approach leaves unresolved how data protection is now linked to claims over territory, infrastructure, and legal competence. It also leaves unclear how digital sovereignty redefines the normative purpose of data governance. The question is not only whether data should be protected, but also who has the authority to define the conditions of that protection. In this sense, what is still unknown is how data protection operates as a structural site of contestation in a fragmented transnational environment. This unknown area is precisely where the article develops its analytical intervention (Neuhuber, 2025).

The central gap, therefore, lies in the absence of an integrated conceptual framework that connects data protection, digital sovereignty, and transnational regulatory authority. Existing approaches do not sufficiently explain how data protection is being transformed from a privacy-centered legal norm into a broader architecture of strategic control. This gap becomes more visible when regulatory fragmentation is taken seriously as a defining feature of the current digital order (Fan et al., 2025). Under fragmented conditions, different legal systems and political actors compete to shape the terms of digital governance. Here, digital sovereignty offers an important theoretical lens because it highlights how authority is claimed, defended, and reorganized through law. Rather than treating sovereignty as a separate issue from data protection, the article reads both as mutually constitutive. This theoretical move allows data protection to be interpreted as a legal mechanism through which broader struggles over jurisdiction and normative authority are expressed. In this way, the research gap is not simply empirical but conceptual, because it concerns the changing meaning of regulation itself (Tolliyevna, 2024).

Filling this gap is theoretically justified because the conventional privacy model no longer captures the full function of data protection in contemporary governance. A rights-based understanding remains important, but it does not adequately explain why data

regulation is increasingly tied to infrastructure control and strategic legal positioning. The concept of digital sovereignty helps clarify this shift by showing that regulation is also about preserving or expanding authority in digital space. Through this lens, data protection appears not merely as a defensive shield for individual rights but as a constitutive element of regulatory ordering (Filani et al., 2022). This perspective is especially useful in a fragmented transnational setting where no single legal center fully determines the rules of digital interaction. Under such conditions, legal interoperability and national autonomy must constantly be negotiated. The article is therefore justified in using digital sovereignty to explain why data protection has become a central arena of institutional and normative contestation. The coherence of this approach lies in its ability to connect legal meaning with shifts in political and regulatory authority (Lebel et al., 2006).

Based on this framing, the article is guided by several interconnected research questions. First, it asks how digital sovereignty reshapes the legal meaning of data protection in a fragmented transnational regulatory environment. Second, it asks in what ways data protection functions as a site of contestation over jurisdiction, infrastructure, and normative authority. Third, it asks how regulatory power is being reordered through the interaction between national autonomy and transnational digital integration. These questions are closely linked because each addresses a different dimension of the same transformation. Together, they move the discussion beyond a narrow privacy focus and toward a broader theory of digital legal ordering (Ziervogel et al., 2016). They also help organize the relationship between legal concepts and institutional change. In that sense, the questions are designed not to isolate variables but to clarify a shifting structure of authority. Their value lies in making visible the deeper regulatory implications of the rise of digital sovereignty.

The urgency of this research lies in the speed with which digital governance is being reorganized across legal and political boundaries. As regulatory fragmentation deepens, the absence of a coherent conceptual account makes it harder to understand the direction of current legal change. Without such understanding, debates on data protection risk remaining normatively narrow and analytically incomplete. The article contributes by offering a framework that connects privacy, sovereignty, cross-border flows, and regulatory authority within one coherent argument. This contribution is important because it helps reposition data protection at the center of transnational legal analysis. It also provides a stronger basis for understanding how digital governance is increasingly structured through competing claims of control and coordination. By clarifying this transformation, the article opens space for more precise discussion of how law operates in the digital age. The broader significance of the study lies in its ability to show that the future of data protection is inseparable from the reordering of authority itself.

## 2. Research Method

This study employs a qualitative research design grounded in conceptual and regulatory analysis to examine how digital sovereignty reshapes the meaning of data protection within a fragmented transnational legal environment. A qualitative approach is appropriate because the research is concerned with legal meaning, authority, and normative restructuring rather than with measurement, causal testing, or statistical generalization. The analytical framework connects five core dimensions derived from the study's outline: jurisdiction, digital infrastructure, normative authority, legal interoperability, and the tension between national autonomy and transnational integration. Through this framework, the study analyzes data protection not only as a legal right but also as a governance structure through which regulatory power is

organized and contested. This design works for the research because the central objective is to explain conceptual transformation and regulatory reordering, both of which require close reading, comparison, and interpretation of legal and policy discourse. It also suits the study because fragmented digital governance cannot be fully captured through quantitative indicators alone, as the issue involves competing legal claims, shifting institutional boundaries, and evolving normative logics. For these reasons, qualitative conceptual analysis provides the most suitable design for identifying how digital sovereignty redefines the legal architecture of data protection in transnational regulation.

The data sources consist of academic arguments, legal-regulatory texts, and policy-oriented materials relevant to data protection, cross-border data governance, and digital sovereignty, with the unit of analysis defined as the legal meaning and regulatory function of data protection in transnational governance. Data collection was conducted through purposive selection of texts that directly address the relationship among privacy, data flows, and regulatory authority, followed by systematic reading, coding, and classification according to the study's analytical dimensions. The instrument used in this research is an analytical matrix that organizes textual evidence into categories of jurisdiction, infrastructure, normative authority, legal interoperability, and autonomy-integration balance, while the main variables are treated as conceptual dimensions rather than measurable quantities. Trustworthiness was ensured through transparent coding criteria, conceptual consistency between research questions and analytical categories, and repeated comparison across sources to maintain coherence and dependability. Validity was strengthened by aligning the analytical framework with the research problem and by using source triangulation across legal, academic, and policy documents to confirm the relevance of recurring themes. Reliability was addressed through a structured documentation process that records source selection, coding decisions, and category definitions so that the analytical procedure remains stable and traceable. Ethical considerations were observed by using publicly accessible documents, accurately representing source content, and maintaining academic integrity in citation and paraphrase; because the study does not involve human participants, formal informed consent and personal confidentiality procedures were not required, and no identifiable personal data were collected or processed.

## 3. Result and Discussion

The reconfiguration of data protection in the contemporary digital order is best understood as a shift from a narrowly privacy-centered legal doctrine toward a broader framework of governance. Within this transformation, data protection no longer operates only as a mechanism for safeguarding personal information against misuse. It increasingly functions as a legal device through which states, institutions, and regulatory systems define the conditions of digital authority. This shift aligns with the article's central concern that digital sovereignty is not external to data protection but constitutive of its evolving meaning. The regulatory significance of data protection therefore extends beyond rights protection into the organization of jurisdictional reach, infrastructural dependence, and normative legitimacy. Such an expansion reflects the broader restructuring of transnational legal authority in response to digital interdependence. The issue is not merely the protection of data subjects but the political and legal ordering of digital space (Nahtigal, 2022).

A major pattern emerging from the discussion concerns the declining adequacy of treating privacy as the exclusive normative foundation of data protection. Privacy remains an essential reference point, yet it no longer captures the full legal and strategic significance of data governance. In fragmented regulatory settings, data protection is increasingly linked to questions of market access, territorial competence, digital

infrastructure, and the capacity of states to assert regulatory control. This broader orientation gives data protection a constitutive role in shaping the architecture of transnational regulation (Lo et al., 2020). The legal regulation of data flows thereby becomes inseparable from disputes over who has the authority to define, interpret, and enforce legitimate standards. That condition helps explain why data protection has acquired a stronger geopolitical and institutional dimension. The rise of digital sovereignty intensifies this trend by positioning legal control over data as a component of wider struggles over autonomy and influence in digital governance. The data protection now operates as a site of contestation over jurisdiction. In conventional legal terms, jurisdiction refers to the authority to regulate persons, activities, and transactions within a given legal order. In digital environments, however, data circulates across territorial boundaries in ways that complicate traditional assumptions about legal space. The expansion of data governance has therefore produced a situation in which regulatory claims overlap, compete, and sometimes conflict. Data protection becomes central within this condition because it offers a legal basis for extending authority into digital interactions that are not easily confined within territorial borders. Jurisdiction is consequently reconstructed through rules governing storage, transfer, access, and processing. This development confirms that the legal meaning of data protection is increasingly shaped by the problem of transboundary authority rather than by privacy concerns alone. The issue of jurisdiction thus provides a crucial bridge between data governance and digital sovereignty (Mapamba & Pisa, 2025).

Digital infrastructure constitutes another core dimension of this regulatory transformation. Infrastructure is not simply a technical foundation that passively supports digital exchange; it also structures dependency, access, and capacity within transnational governance. Legal claims over data are often inseparable from the infrastructural systems through which data is generated, stored, and moved. Control over infrastructure enhances regulatory leverage because it affects the practical conditions under which rules can be implemented and enforced. This gives data protection an infrastructural dimension that exceeds the classical legal focus on individual rights. The connection between infrastructure and sovereignty becomes particularly significant where states seek to reduce dependency on external platforms, standards, or jurisdictions. Under such conditions, data protection serves as one mechanism through which broader ambitions of strategic control are institutionalized. The legal governance of data is therefore tied to the material and organizational foundations of digital authority.

Normative authority deepens this picture by drawing attention to the struggle over whose legal principles become authoritative in digital regulation. Data protection has become a field in which regulatory systems compete not only over enforcement capacity but also over the legitimacy of the standards they promote (Irani et al., 2025). This normative struggle is especially visible in fragmented transnational settings where multiple legal orders seek recognition for their preferred principles of governance. The significance of digital sovereignty lies partly in its ability to transform data protection into a vehicle for asserting such normative claims. Rather than presuming a universally shared understanding of digital rights and obligations, the current environment is marked by divergent legal rationalities that must coexist, overlap, or confront one another. Data protection thus acquires a constitutive role in shaping the normative landscape of digital governance. The regulatory field is defined as much by contests over legal meaning as by technical or institutional coordination. This helps explain why data protection has become central to debates on authority in the digital age (Folke et al., 2010).

The broader structure of the argument can be clarified through the relationship between the article's main analytical dimensions and the patterns developed in the discussion. These dimensions indicate that the transformation of data protection cannot

be reduced to a single legal shift, because it unfolds across several interrelated layers of authority and governance. Table 1 summarizes these relationships and shows how data protection links privacy, jurisdiction, infrastructure, interoperability, and sovereignty within a fragmented regulatory order.

**Table 1. Analytical dimensions of the transformation of data protection**

| *Analytical dimension* | *Regulatory shift* | *Legal significance* | *Relation to digital sovereignty* |
|---|---|---|---|
| *Privacy* | From individual protection to governance relevance | Expands data protection beyond personal rights | Repositions privacy within broader authority claims |
| *Jurisdiction* | From territorial assumption to transboundary reach | Extends regulatory competence across digital flows | Supports assertions of legal control over data space |
| *Infrastructure* | From technical support to strategic asset | Connects regulation to capacity and dependency | Enables sovereignty through infrastructural control |
| *Normative authority* | From shared principles to competing standards | Frames legitimacy as a contested legal issue | Allows states and regimes to project regulatory models |
| *Legal interoperability* | From optional coordination to structural necessity | Facilitates compatibility across fragmented systems | Limits full isolation while preserving autonomy |
| *Autonomy–integration balance* | From stable coexistence to negotiated tension | Reorders the relation between national control and transnational connectivity | Defines the practical horizon of digital sovereignty |

The table reinforces the argument that data protection has become a multidimensional governance structure rather than a discrete legal doctrine concerned only with privacy. Each dimension points to a distinct but connected aspect of regulatory transformation. Privacy remains present, yet it is embedded in a wider legal process through which jurisdictional claims, infrastructural dependencies, and normative competition are organized (Mammadov, 2025). The category of legal interoperability is especially important because it indicates that digital sovereignty does not eliminate interdependence. Even where states seek stronger control, regulatory coordination remains necessary for the functioning of cross-border digital systems. The autonomy–integration dimension further illustrates that contemporary data governance is shaped by negotiated tension rather than absolute legal closure. In this respect, the table supports the article's central claim that digital sovereignty reorders authority by transforming the architecture within which data protection is understood and applied. The analytical value of the table lies in making visible the structural coherence behind what might otherwise appear as separate legal developments.

This interpretation extends prior scholarship that treated privacy, cross-border data flows, and regulatory authority as distinct fields of inquiry. Earlier studies were important in establishing the legal and political salience of each issue, particularly the normative significance of privacy and the practical importance of transnational digital exchange. Yet the separation of these debates has limited the ability to capture the deeper

transformation of regulatory order (Meuwissen et al., 2019). Once data protection is approached as a structural arena rather than a discrete right, the interaction between these debates becomes clearer. The fragmentation of regulatory environments is not a background condition but a constitutive feature of the contemporary digital order. Within this setting, digital sovereignty provides a more adequate theoretical lens because it links legal meaning to broader struggles over authority, capacity, and legitimacy. The discussion therefore moves beyond additive analysis and toward an integrated understanding of how digital governance is being reorganized. Such integration is necessary for explaining why data protection has become central to transnational regulatory contestation (Esposito, 2025).

The implications of this shift are substantial for legal theory and regulatory analysis. Data protection can no longer be interpreted solely through the doctrinal language of rights, consent, and individual safeguards. It must also be understood as part of a governance structure through which actors negotiate the permissible boundaries of digital authority. This means that the legal regulation of data functions simultaneously as a normative, institutional, and strategic process. The concept of digital sovereignty sharpens this point by revealing how claims to autonomy are pursued within, rather than outside of, interdependent regulatory systems. The resulting legal order is neither fully harmonized nor fully segmented. It is instead characterized by selective coordination, overlapping authority, and strategic efforts to preserve room for domestic control. Data protection thus becomes one of the key legal sites through which transnational digital order is produced and contested. This theoretical repositioning has broader relevance for debates on sovereignty under conditions of technological interdependence.

The practical relevance of this discussion is equally significant. Regulators, courts, and policy institutions operate in an environment where legal authority over data increasingly affects economic exchange, administrative capacity, technological dependency, and geopolitical positioning. Under such conditions, data protection frameworks influence far more than compliance obligations or individual rights claims. They shape the institutional terms under which states participate in digital integration while attempting to secure regulatory autonomy (Meuwissen et al., 2021). This helps explain why legal interoperability emerges as a recurring concern in fragmented governance arrangements. Complete regulatory isolation is difficult to sustain because digital systems depend on cross-border connections, shared standards, and functional compatibility. At the same time, unrestricted integration may weaken domestic control over data-related infrastructures and legal norms. The practical challenge is therefore not to choose between sovereignty and connectivity, but to govern their tension through legal architectures that remain both effective and legitimate. Data protection occupies a central place within that challenge. Several strengths emerge from this analytical approach. Its primary value lies in providing a conceptually integrated account of how data protection, digital sovereignty, and transnational authority interact within one regulatory transformation. Such integration makes it possible to explain legal change without reducing the issue to either doctrinal privacy analysis or broad geopolitical rhetoric. The framework also captures the importance of fragmentation without presuming that fragmentation produces regulatory incoherence in every instance. It allows for the possibility that contested authority may still generate forms of structured coordination, particularly through interoperability. At the same time, the conceptual scope of the discussion imposes limits. The emphasis on regulatory meaning and theoretical coherence does not provide an empirical comparison of specific legal regimes or policy outcomes. The discussion therefore remains strongest at the level of conceptual explanation rather than institutional measurement. That limitation does not weaken the

argument's analytical relevance, but it does indicate the need for further work connecting theory to particular regulatory settings.

An especially notable issue concerns the role of interoperability, which appears more central than many sovereignty-based discussions typically assume. Digital sovereignty is often associated with control, insulation, or strategic autonomy, yet the present discussion indicates that authority in digital governance cannot be sustained through closure alone. Interoperability emerges not as a secondary technical concern but as a structural condition of regulatory viability in transnational environments. This introduces an important tension into the concept of sovereignty itself. Legal authority is strengthened through claims of control, but it is also constrained by the need for compatibility with external systems and standards. Data protection becomes one of the principal legal mechanisms through which this tension is managed. That dynamic complicates simplified narratives of either global convergence or national retrenchment. The digital legal order is instead organized through ongoing negotiation between the aspiration for autonomy and the necessity of interconnection. Such complexity gives the transformation of data protection its broader theoretical and regulatory significance.

Future research can develop this argument by examining how different legal regimes operationalize the relationship between sovereignty, data protection, and interoperability. Comparative work would be especially valuable for identifying how various regulatory systems balance jurisdictional extension, infrastructural control, and transnational coordination. Sector-specific analysis could also deepen understanding of how this transformation unfolds in areas such as public administration, digital markets, health data, or platform governance. Another important direction concerns the institutional consequences of fragmented authority for enforcement, compliance, and dispute resolution across borders. These avenues would extend the present discussion by situating the conceptual framework within concrete legal and policy configurations. The practical application of the argument lies in helping regulatory actors recognize that data protection is not merely a defensive legal instrument but a constitutive element of digital order. Such recognition is increasingly necessary in a transnational environment where authority is contested through law, infrastructure, and normative claims. The significance of the article therefore rests in clarifying the evolving place of data protection within the reordering of regulatory authority in the digital age.

## 4. Conclusion

The contemporary transformation of data protection reflects a broader reordering of regulatory authority in digital governance. No longer confined to the protection of individual privacy, data protection now operates within a wider legal architecture shaped by jurisdictional contestation, infrastructural control, normative competition, and the tension between national autonomy and transnational integration. The discussion has clarified that digital sovereignty is central to this transformation because it redefines the legal and political function of data governance in fragmented regulatory environments. What was once treated primarily as a rights-based domain has increasingly become a strategic field through which authority is asserted, coordinated, and contested across borders. The resulting configuration is neither purely national nor fully transnational, but structured through negotiated forms of interoperability and control. In this sense, the changing meaning of data protection must be understood as part of the evolving organization of digital legal order.

The main contribution to the field lies in offering an integrated conceptualization of the relationship among data protection, digital sovereignty, and transnational regulatory authority. Rather than reproducing the common separation between privacy, cross-border data flows, and state regulation, the analysis positions these elements within

a single framework of legal transformation. This perspective advances scholarly discussion by reframing data protection as a structural mechanism of authority formation rather than only a normative safeguard for individual rights. It also strengthens theoretical debate on digital governance by demonstrating that sovereignty is not external to data regulation but embedded within its changing legal logic. Such a contribution is especially relevant for scholarship concerned with regulatory fragmentation, legal pluralism, and the institutional consequences of digital interdependence. By clarifying the expanded role of data protection, the analysis provides a stronger basis for understanding how contemporary legal orders are being reorganized through digital governance.

Future research should extend this conceptual framework into more specific comparative and sectoral contexts. Cross-jurisdictional analysis would help clarify how different regulatory systems interpret the relationship between sovereignty, interoperability, and data protection under varying legal traditions and political priorities. Additional work is also needed on how this transformation operates in specific fields such as platform governance, public administration, digital trade, and cross-border service delivery. Greater attention to institutional practice would further enrich the discussion by examining how regulatory actors operationalize competing claims of authority in everyday governance settings. A productive direction would involve exploring how legal interoperability is negotiated in environments marked by asymmetrical power, infrastructural dependence, and normative divergence. Such inquiry would deepen understanding of the practical consequences of fragmented digital regulation while preserving the broader theoretical insight that data protection has become a central site in the reordering of transnational authority.

## References

Afolabi, J., & Raifu, I. (2024). Toward economic resilience in Sub-Saharan Africa: The role of institutional quality and human capital development. *Sustainable Development*. https://doi.org/10.1002/sd.3251

Boru, E. M., Hwang, J., & Ahmad, A. (2025). Governance and Institutional Frameworks in Ethiopian Integrated Agro-Industrial Parks: Enhancing Innovation Ecosystems and Multi Stakeholder Coordination for Global Market Competitiveness. *Economies*. https://doi.org/10.3390/economies13030079

Bouckaert, G., & Galego, D. (2024). System-quake proof 'systemic resilience governance': Six measures for readiness. *Global Policy*. https://doi.org/10.1111/1758-5899.13433

Esposito, D. (2025). A Ladder of Urban Resilience: An Evolutionary Framework for Transformative Governance of Communities Facing Chronic Crises. *Sustainability*. https://doi.org/10.3390/su17136010

Fan, D., Maliki, N. Z. B., Yu, S., & Men, T. (2025). Assessment of resilience and key drivers of Tibetan villages in Western Sichuan. *Scientific Reports*, *15*. https://doi.org/10.1038/s41598-025-07788-8

Filani, O. M., Sakyi, J. K., Okojie, J. S., Nnabueze, S. B., & Ogedengbe, A. O. (2022). Market Research and Strategic Innovation Frameworks for Driving Growth in Competitive and Emerging Economies. *Journal of Frontiers in Multidisciplinary Research*. https://doi.org/10.54660/.ijfmr.2022.3.2.94-108

Folke, C., Carpenter, S., Walker, B., Scheffer, M., Chapin, T., & Rockström, J. (2010). Resilience thinking: integrating resilience, adaptability and transformability. *Ecology and Society*, *15*, 20. https://doi.org/10.5751/es-03610-150420

Irani, M., Rahnamayiezekavat, P., & Ziaesaeidi, P. (2025). THE MODEL OF RELATIONSHIP BETWEEN ECONOMIC AND INSTITUTIONAL RESILIENCE BASED ON A STAGED CRITICAL REVIEW OF LITERATURE. *Journal of Urban and Regional Analysis*. https://doi.org/10.37043/jura.2025.17.2.3

Lebel, L., Anderies, J., Campbell, B., Folke, C., Hatfield-Dodds, S., Hughes, T., & Wilson, J. (2006). Governance and the Capacity to Manage Resilience in Regional Social-Ecological Systems. *Ecology and Society*, *11*, 19. https://doi.org/10.5751/es-01606-110119

Lo, A., Liu, S., Cheung, L., & Chan, F. (2020). Contested Transformations: Sustainable Economic Development and Capacity for Adapting to Climate Change. *Annals of the American Association of Geographers*, *110*, 223–241. https://doi.org/10.1080/24694452.2019.1625748

Mammadov, B. (2025). Institutional Pillars of Switzerland's Economic Resilience and Prosperity. *Porta Universorum*. https://doi.org/10.69760/portuni.0107009

Mapamba, L., & Pisa, N. (2025). Enhancing Economic Resilience: Evaluating South Africa's Industrial Policy for Inclusive Growth and Transformation. *Global Conference on Business and Social Sciences Proceeding*. https://doi.org/10.35609/gcbssproceeding.2025.1(70)

Meuwissen, M., Feindt, P., Slijper, T., Spiegel, A., Finger, R., De Mey, Y., Paas, W., Termeer, K., Poortvliet, P., Peneva, M., Urquhart, J., Vigani, M., Black, J., Nicholas-Davies, P., Maye, D., Appel, F., Heinrich, F., Balmann, A., Bijttebier, J., … Reidsma, P. (2021). Impact of Covid-19 on farming systems in Europe through the lens of resilience thinking. *Agricultural Systems*, *191*, 103152. https://doi.org/10.1016/j.agsy.2021.103152

Meuwissen, M., Feindt, P., Spiegel, A., Termeer, C., Mathijs, E., Mey, Y., Finger, R., Balmann, A., Wauters, E., Urquhart, J., Vigani, M., Zawalińska, K., Herrera, H., Nicholas-Davies, P., Hansson, H., Paas, W., Slijper, T., Coopmans, I., Vroege, W., … Reidsma, P. (2019). A framework to assess the resilience of farming systems. *Agricultural Systems*. https://doi.org/10.1016/j.agsy.2019.102656

Mubangizi, B. (2025). Pathways to resilient rural livelihoods: Lessons from Southwestern Uganda. *Jàmbá : Journal of Disaster Risk Studies*, *17*. https://doi.org/10.4102/jamba.v17i1.1905

Nahtigal, M. (2022). EU Recovery Plans, Inclusive Knowledge Economy and Overcoming Regional Disparities. *Lex Localis - Journal of Local Self-Government*. https://doi.org/10.4335/20.4.1171-1189(2022)

Neuhuber, T. (2025). One and the Same or Worlds Apart? Linking Transformative Regional Resilience and Just Transitions Through Welfare State Policies. *Sustainability*. https://doi.org/10.3390/su17020637

Tolliyevna, K. G. (2024). ECONOMY NETWORKS IN DEVELOPMENT INNOVATIVE INVESTMENT ACTIVITY INCREASE METHODICAL BASICS. *International Journal of Economic Integration and Regional Competitiveness*. https://doi.org/10.61796/ijeirc.v1i9.240