ORIGINAL SCIENTIFIC PAPER
DOI:10.65949/jdeis.2025.1.3
UDC: 658:004.7
005.334:004.056.5
COBISS.SR-ID 184117513

SECURITY AND TRUST AS KEY DRIVERS OF SUSTAINABLE DEVELOPMENT IN THE DIGITAL ECONOMY

Dimitrić Biljana[3]

ABSTRACT

Security and trust represent key prerequisites for the sustainable development of the digital economy, as they directly influence the adoption of digital services, innovation capacity, investment climate, and the long-term competitiveness of organizations and national economies. In the context of accelerated digital transformation, data are becoming a strategic resource, while platform-based business models, electronic commerce, fintech services, and digital entrepreneurship increasingly rely on robust mechanisms for protecting privacy, integrity, and information availability. At the same time, the growing incidence of cyber risks and increasingly stringent regulatory requirements mean that security can no longer be viewed solely as a technical function, but rather as a strategic and managerial factor shaping user trust and the sustainability of digital ecosystems.The aim of this paper is to examine the interdependence between security, trust, and sustainability in the digital economy through a synthesis of relevant scientific literature and empirical research, as well as to highlight their implications for the long-term adoption of digital innovations. The empirical study was conducted on a sample of 98 respondents in the Republic of Serbia, using a structured questionnaire and applying descriptive statistics and correlation analysis.The research findings indicate that respondents largely perceive security as a fundamental prerequisite for the use of digital services and that perceived security has a significant impact on the level of trust in digital systems. The existence of conditional trust was identified, whereby users accept digital services despite reservations regarding the

[3] *University Bijeljina, Faculty of Psychology,Bijeljina, Republika Srpska , Bosnia and Herzegovina, e-mail: biljanazdimitric@gmail.com*

transparency of data processing. The results also confirm that security and trust are key factors for the long-term sustainability of digital business models.

This paper contributes to the theoretical understanding of security and trust as interdependent determinants of the sustainable development of the digital economy and provides practical guidelines for organizations and policymakers regarding strategic cybersecurity management and trust-building in the digital environment.

***Keywords**: digital economy, cybersecurity, trust, sustainable development, digital platforms, risk management*
***JEL classification**: O33, L86, D83*

INTRODUCTION

The digital economy is evolving as the dominant form of contemporary economic activity, in which digital technologies and data have become the foundation for value creation, delivery, and appropriation. Platform-based business models, electronic commerce, fintech services, digital entrepreneurship, and "smart" services in both the public and private sectors are transforming market structures and accelerating innovation (Parker, Van Alstyne, & Choudary, 2016; OECD, 2020). However, the rapid pace of digitalization simultaneously increases the exposure of organizations and users to various risks, including data misuse, online payment fraud, infrastructure attacks, and disruptions to business continuity. These risks are not merely technical in nature; they also affect economic efficiency, reputation, investment flows, and social stability.Security and trust represent fundamental prerequisites for the sustainable development of the digital economy. Security refers to the management of risks that threaten the confidentiality, integrity, and availability of information, as well as system resilience to incidents and rapid recovery (NIST, 2018). Trust, on the other hand, relates to the willingness of users and organizations to accept vulnerability in digital transactions, based on the expectation that the other party or the system will behave reliably and in accordance with established norms (Luhmann, 1979; Mayer et al., 1995). In practice, security and trust are interdependent: security mechanisms (technical measures, procedures, certifications, and transparency) reduce perceived risk, while trust influences the adoption of digital services and the willingness to share data (McKnight et al., 2002; Pavlou, 2003).

The sustainable development of the digital economy goes beyond short-term growth in the number of users and transactions. It encompasses long-term economic sustainability (stable revenues and productivity), social sustainability (protection of rights, reduction of digital inequalities, and the well-being of users and employees), and environmental sustainability (energy efficiency and

responsible management of digital infrastructure). Contemporary literature increasingly emphasizes the concept of "digital sustainability," suggesting that digital innovations can accelerate the achievement of sustainable development goals, but may also generate negative effects if not managed responsibly (George et al., 2021). In this context, security and trust emerge as key mechanisms that support social legitimacy and economic stability within digital systems.

The research problem addressed in this paper arises from the fact that security is often viewed as an operational IT issue, while trust is analyzed separately within the domains of marketing or consumer behavior. The theoretical foundations of this study are based on theories of trust in organizational and interorganizational relationships (Luhmann, 1979; Mayer, Davis, & Schoorman, 1995), as well as empirical research on trust in electronic commerce and online environments (McKnight, Choudhury, & Kacmar, 2002; Gefen, Karahanna, & Straub, 2003; Pavlou, 2003). The paper also considers the role of standards and frameworks for security management (ISO/IEC 27001, 2022; NIST, 2018), as well as the economic and social effects of cybercrime, which undermine trust and increase business costs (Anderson et al., 2013).

The sustainable development of the digital economy therefore requires an integrated understanding of how security practices, institutional frameworks, and governance decisions influence the trust of users and business partners, and how this trust, in turn, shapes the adoption of innovations, competitiveness, and long-term societal outcomes. Accordingly, the aim of this paper is to systematize relevant theoretical approaches to trust and security in the digital environment, to explain the mechanisms of their interdependence, and to propose a conceptual framework that can serve as a foundation for future empirical research and practical recommendations for organizations and policymakers.

LITERATURE REVIEW

Trust is one of the key mechanisms that enable the functioning of complex social and economic systems. Luhmann (1979) conceptualizes trust as a means of reducing complexity: under conditions of uncertainty, individuals and organizations make decisions based on expectations that other actors or systems will behave in a predictable manner. This perspective is particularly relevant to the digital economy, where users are often unable to directly assess the reliability of technology and therefore rely on signals such as platform reputation, certifications, recommendations, and visible security measures.

Research in the field of information systems indicates that trust is a central determinant of the adoption of online services. McKnight et al. (2002) distinguish between "initial trust," which is formed prior to direct experience and is based on institutional mechanisms and perceived security, and experience-based trust. Gefen et al. (2003) demonstrate that trust in an online vendor has a strong influence on the intention to use electronic commerce, while perceived risk acts as a deterrent. Pavlou (2003) develops a model in which institutional structures (e.g., privacy policies, security mechanisms, legal frameworks, and dispute resolution mechanisms) influence trust and thereby indirectly facilitate transactions in electronic commerce.

For the digital economy, these findings have broader implications: trust is not merely a psychological category, but an economic resource that affects the rate of adoption of digital innovations, user retention, and the competitive position of platforms. In the context of the platform economy, trust becomes even more complex because platforms mediate between multiple parties (e.g., buyers and sellers), requiring trust to be simultaneously directed toward the system itself and toward the actors operating within the ecosystem (Parker et al., 2016).

Although there is a substantial body of research on trust in electronic commerce and digital platforms, relatively few studies systematically link trust to security practices and the sustainability of the digital economy. These findings suggest that trust in the digital environment cannot be considered independently of the security mechanisms that shape perceptions of risk.

CYBERSECURITY AS A STRATEGIC RESOURCE OF THE DIGITAL ECONOMY

Cybersecurity is increasingly treated as a strategic management component rather than as an isolated IT function. The NIST Cybersecurity Framework (2018) provides a foundation for managing cyber risks through five core functions—Identify, Protect, Detect, Respond, and Recover—which emphasize continuity and resilience. Similarly, ISO/IEC 27001 (2022) introduces a risk-based and continuous improvement approach to information security management.

From the perspective of the digital economy, cybersecurity has three key effects. First, it affects costs and efficiency, as security incidents lead to business disruptions, data losses, and reputational damage. Second, it influences user behavior, since breaches of privacy and security reduce users' willingness to engage in online transactions. Third, it affects innovation: organizations with mature cybersecurity capabilities are better positioned to introduce new digital

products and services because they are able to manage risks and comply with regulatory requirements. Anderson et al. (2013) emphasize that the economic costs of cybercrime are significant and multifaceted, ranging from direct financial losses to indirect costs related to security investments and the erosion of trust, further confirming that cybersecurity influences competitiveness and sustainability.

The literature indicates that cybersecurity and trust are not identical, but they are closely interconnected. Cybersecurity represents the more objective and measurable aspect of risk management, whereas trust reflects a subjective perception of reliability and fairness. In online environments, users rarely have insight into actual security mechanisms and therefore form trust based on visible privacy policies, two-factor authentication, certifications, the experiences of other users, and brand reputation (McKnight et al., 2002; Pavlou, 2003). Consequently, managing trust is simultaneously a matter of managing communication about security.

Trust may also be undermined even when technical security is high if organizations fail to manage transparency and ethical issues related to data processing. This is particularly relevant in platform-based business models, where monetization is often data-driven. In such cases, users may experience a loss of control over their data, which reduces trust and the acceptance of digital services, even in the absence of an immediate "incident." Therefore, trust requires broader governance principles such as transparency, accountability, fair treatment, and effective mechanisms for redress and complaints.

The concept of sustainability in the digital economy implies that digital innovations should not contribute solely to economic productivity and competitiveness, but also to the achievement of social and environmental goals. George et al. (2021) point out that digital innovations can significantly contribute to addressing sustainable development challenges, such as optimizing energy consumption, developing smart grids, and enabling digital monitoring of supply chains. At the same time, they warn that digitalization may generate new risks, including the deepening of digital inequalities, infringements of privacy, and increased energy consumption by data centers.

Cybersecurity and trust are integral parts of the "social infrastructure" of digital sustainability, as digital services will not be widely adopted and innovations will not achieve their expected economic and social effects without their development. OECD (2020) further emphasizes that digital transformation must be accompanied by effective risk management, the development of digital skills, and institutional mechanisms that foster trust. This is equally important at both

the national and organizational levels: if users do not trust the security of e-government or fintech services, the digitalization of public services and financial inclusion will remain limited. Similarly, organizations that fail to develop cyber resilience face business disruptions and losses that, in the long run, undermine economic sustainability.

CONCEPTUAL MODEL

Based on a synthesis of the literature, it is possible to propose a simplified conceptual model that explains how security and trust influence the sustainable development of the digital economy:

1. Security capacities and practices (NIST, 2018; ISO/IEC 27001, 2022) influence risk perception and institutional trust (McKnight et al., 2002; Pavlou, 2003).
2. Higher levels of trust lead to greater adoption of digital services and a higher willingness to share data and engage in transactions (Gefen et al., 2003).
3. User adoption and retention accelerate business model innovation and platform growth (Parker et al., 2016).
4. Through economic stability and the broader use of digital solutions, conditions are created for sustainable outcomes (economic, social, and environmental), provided that risks are managed ethically and transparently (George et al., 2021; OECD, 2020).

This model is suitable as a basis for empirical testing in future research, for example through surveys on perceptions of security and trust, analyses of user behavior, or case studies of digital platforms.

RESEARCH METHODOLOGY

The objective of the empirical research is to examine how perceptions of security and trust influence the sustainable development of the digital economy, viewed through the willingness of users and employees to adopt digital services, support innovation, and use digital business models over the long term.

The research is guided by the following questions:

1. To what extent do respondents perceive security as a key factor in the use of digital services?

2. Does trust in digital systems affect the willingness to adopt innovations?
3. How do security and trust jointly influence perceptions of the sustainability of the digital economy?

Research Sample

The empirical research was conducted on a sample of 98 respondents in the Republic of Serbia. The sample includes employees, entrepreneurs, and users of digital services who, in their everyday professional or private lives, use digital platforms, electronic services, online payments, or other forms of the digital economy.

Sample structure:

Gender: 56% women (55 respondents), 44% men (43 respondents)
Age:

- up to 30 years: 24%
- 31–40 years: 38%
- 41–50 years: 26%
- over 50 years: 12%

Education:

- secondary education: 11%
- higher education: 61%
- master's degree or higher: 28%

The structure of the sample enables an examination of different generational and educational perspectives related to the digital economy.

Instrument and Method

A structured questionnaire was used as the research instrument, consisting of three parts:

1. sociodemographic questions,
2. questions related to perceptions of the security of digital systems,
3. questions related to trust and the sustainability of the digital economy.

Responses were measured using a five-point Likert scale (1 – strongly disagree, 5 – strongly agree). The data were analyzed using descriptive statistics and analyses of relationships among variables, with the support of appropriate statistical software.

RESEARCH RESULTS

The results of the study indicate that respondents largely recognize security as one of the fundamental prerequisites for the functioning and sustainable development of the digital economy. In response to the statement that the security of personal and business data is crucial for the use of digital services, 74% of respondents fully agreed, while an additional 17% mostly agreed. These findings suggest that the perception of security plays a decisive role in the decision to adopt digital solutions.

With regard to trust in digital platforms, 69% of respondents reported that they trust the systems they regularly use, but only 31% believe that digital systems are fully transparent in terms of data processing practices. This finding indicates the existence of "conditional trust," whereby users adopt digital services despite certain reservations.

The results show that 62% of respondents believe that increasing security directly contributes to greater trust in the digital economy. In contrast, 22% consider that security measures often complicate the use of digital services, which may represent a barrier to the broader adoption of innovations.

In terms of sustainability, 58% of respondents believe that the digital economy can contribute to long-term economic development only if security and trust are at a high level. In addition, 55% of respondents stated that, in the event of a serious security incident, they would reduce or completely discontinue the use of certain digital services, indicating the fragility of trust in the digital environment.

An analysis of responses shows that younger respondents exhibit a higher tolerance for risk, while simultaneously expecting greater transparency and faster responses in the event of security issues. Older respondents demonstrate greater caution toward digital innovations and more strongly associate trust with stability and institutional support.

The results further indicate that 67% of respondents consider security and trust to be key factors for the long-term sustainability of digital business models,

while only 19% believe that economic benefits can compensate for a lack of trust.

Overall, the empirical findings confirm a strong relationship between the perception of security, the level of trust, and the sustainability of the digital economy.

DISCUSSION

The obtained results confirm the theoretical assumptions from contemporary literature indicating that security and trust represent fundamental pillars of the digital economy. The high percentage of respondents emphasizing the importance of data protection supports the view that the digital economy cannot develop solely on the basis of technological innovation, but requires a strong social and institutional framework. The findings are consistent with studies highlighting that trust is not an absolute category, but rather a dynamic process dependent on user experience, system transparency, and incident management practices. In this sense, the "conditional trust" identified in this study reflects the contemporary reality of digital business.

The discussion of the findings indicates that security plays a dual role: on the one hand, it strengthens trust and encourages the use of digital services, while on the other hand, excessive or poorly implemented security measures may diminish the user experience. This confirms the need for a balanced approach that combines technical protection with simplicity and transparency.

A particularly important finding is that the majority of respondents would change their behavior in the event of a security incident, confirming that trust is easily undermined and slow to recover. This has significant implications for organizations relying on digital business models, as sustainable growth cannot be achieved without long-term trust.

The results also confirm that the sustainability of the digital economy cannot be viewed exclusively through economic indicators. The social dimension—trust, a sense of security, and transparency—holds equal importance in the eyes of users.

CONCLUSION

Based on the conducted research, it can be concluded that security and trust represent key determinants of the sustainable development of the digital economy. The results indicate that users and employees recognize the

importance of data protection and the stability of digital systems as the foundation for the long-term adoption of digital innovations.

The study shows that trust in digital systems exists, but is often conditional and depends on perceptions of security, transparency, and organizational responsibility. Security incidents can seriously undermine trust and call into question the sustainability of digital business models.

The practical implications of this study suggest that organizations and policymakers must view security as a strategic resource rather than a technical cost. Investment in security, open communication, and trust-building represents a key prerequisite for the long-term, stable, and sustainable development of the digital economy.

REFERENCES

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. *In R. Böhme (Ed.), The Economics of Information Security and Privacy* (pp. 265–300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12
2. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90.
3. George, G., Merrill, R. K., & Schillebeeckx, S. J. D. (2021). Digital sustainability and entrepreneurship: How digital innovations are helping tackle climate change and sustainable development. *Entrepreneurship Theory and Practice, 45*(5), 999–1027. https://doi.org/10.1177/10422587211009095
4. ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.
5. Luhmann, N. (1979). *Trust and power*. John Wiley & Sons.
6. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359.
7. NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). National Institute of Standards and Technology.
8. OECD. (2020). *Digital transformation and the circular economy*. OECD Publishing. https://doi.org/10.1787/43b3a4f4-en

9. Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). *Platform revolution: How networked markets are transforming the economy and how to make them work for you*. W. W. Norton.
10. Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model. *International Journal of Electronic Commerce, 7*(3), 101–134.

Article history:
Received 1 April 2025
First revision 14 May 2025
Accepted 30 May 2025