Ius et Securitas 2/2025 | ISSN 3071-799X

Krzysztof Kaczmarek
Koszalin University of Technology
krzysztof.kaczmarek@tu.koszalin.pl
ORCID: 0000-0001-8519-1667

Social Security in the Age of Digital Transformation: Demographic, Institutional and Technological Challenges

Abstract

The article explores how digital transformation, demographic shifts, and institutional change are reshaping the concept of social security in Europe. Rather than focusing solely on technology or national-level strategies, it emphasises the importance of local institutions, which are often the first to confront the consequences of these overlapping challenges. Particular attention is given to digital exclusion affecting children, alongside issues such as disinformation, ageing societies, and ecological risks, all analysed through the lens of local resilience. Drawing on both policy documents and research findings, the article argues that social security in the digital age must be understood as a system of interdependent responses, combining infrastructure, education, crisis preparedness and public trust. Only then can institutions at all levels adapt effectively to a rapidly evolving environment.

Keywords: digital transformation, local resilience, social security.

Introduction

Contemporary societies are experiencing profound transformations shaped by the expansion of digital technologies. These changes reach far beyond the realm of technological innovation, altering social structures, interpersonal communication, and the functioning of public institutions[1]. Digitalisation is

[1] D. Hanandini, *Social Transformation in Modern Society: A Literature Review on the Role of Technology in Social Interaction*, „Jurnal Ilmiah Ekotrans & Erudisi" 2024, No. 1, pp. 82-83.

now a decisive factor in shaping how communities operate, how citizens access information, and how states respond to emerging threats. The increasing entanglement of everyday life with algorithms, platforms and automated systems raises new concerns about security – concerns that are no longer confined to military or criminal contexts, but affect the social fabric itself[2].

Security in this environment cannot be viewed in narrow or static terms. The proliferation of social media, the rise of artificial intelligence, and the digitalisation of public administration create risks that are diffuse, unpredictable and increasingly transnational. A single cybersecurity incident may destabilise essential services. Disinformation can corrode civic trust or influence political behaviour. At the same time, digital exclusion continues to marginalise entire social groups, exacerbating inequality and weakening societal cohesion[3]. These risks intersect with demographic challenges that are particularly pressing in many European countries. Ageing populations, declining fertility rates and migration flows have long-term implications for the sustainability of social systems. Yet these phenomena are not isolated – they are interlinked with digital trends. The way media portray parenthood or social roles can discourage family formation. Public institutions must respond to these shifts while operating within new technological frameworks[4].

Local government has a distinct position in this dynamic landscape. Though often under-resourced, it is at the local level that the effects of demographic decline, digital transition and social needs converge most directly. Municipalities act as both implementers of national policies and first responders to local vulnerabilities – making them essential yet strained actors in the evolving security ecosystem[5]. These overlapping developments call for a broader understanding of social security – one that is not merely reactive, but anticipatory, systemic and inclusive. The resilience of communities depends on cooperation across public and private sectors, on cross-border co-

[2] M. Jovanović, J. Dlačić, M. Okanović, *Digitalization and society's sustainable development – Measures and implications*, „Zbornik radova Ekonomskog fakulteta u Rijeci: *časopis* za ekonomsku teoriju i praksu" 2018, No. 2, pp. 921-922.

[3] L. Jaeger, A. Eckhardt, *Eyes wide open: The role of situational information security awareness for security-related behaviour*, „Information Systems Journal" 2021, No. 3, p. 430.

[4] T. Olsson, D. Viscovi, *Digitalised Welfare: Access, Usage, and Outcomes Among Older Adults*, „Media and Communication" 2023, No. 3, pp. 18-20.

[5] N.L. Bonnett, S.J. Birchall, *The influence of regional strategic policy on municipal climate adaptation planning*, „Regional Studies" 2023, No. 1, pp. 18-21.

ordination, and on strategies that consider not only technical infrastructure but also the social consequences of digital transformation.

Accordingly, this article assumes the hypothesis that the effectiveness of social security in the digital age depends not only on technological infrastructure or national-level strategies, but also on the adaptive capacity of local institutions to respond to overlapping digital, demographic and informational challenges. The interplay between local governance, technological change and social dynamics plays a decisive role in shaping long-term resilience and public trust. To examine this hypothesis, the article adopts a qualitative approach that combines comparative analysis and a critical review of the literature, supported by selected examples of institutional practice. This methodological framework makes it possible to identify patterns and tensions in how social security systems evolve under the pressure of digital transformation, demographic shifts and structural institutional constraints.

Digital society and emerging social risks

Social media has permanently changed how people communicate, respond to information, and function in everyday life. While it offers easy access to content and connections, it increasingly replaces traditional relationships. The pandemic only accelerated this shift. At the same time, it's hard to talk about demographics today without mentioning culture, technology, and how they shape attitudes toward family. In Poland, the issue isn't just the low birth rate but also a change in mindset. The Demographic Strategy 2040 won't solve much if it ignores social factors. Many young people no longer see parenthood as something valuable — and it's not just about money. Media can deepen this, reinforcing patterns of individualism. That's why we need more than administrative fixes. Cultural and educational efforts are just as important[6].

This shift in social values, perceptions and behavioural norms not only influences private life but also extends into the public sphere, shaping how local communities experience and interpret security. Contemporary societies face a range of security threats, addressed through modern technologies, the work of law enforcement agencies, and the actions of local administrative bodies. In many cases,

[6] D. Cholewińska, *Media społecznościowe w dobie kryzysu demograficznego w Polsce. Szanse, wyzwania, zagrożenia*, „Ius et Securitas" 2025, No. 1, pp. 49-51.

the responsibility for developing and implementing procedures in response to natural events or risks such as terrorism rests with local governments. Civil protection officers operate within administrative structures, and cooperation with the police is common, with some municipalities also maintaining local security services. Increasingly, threats to local security are of a more everyday nature and relate to manifestations of common crime. The type and scale of criminal activity vary by location. Areas with higher population movement, especially during certain seasons, tend to experience greater public order challenges than more static, less frequented regions. The issue of unemployment is also relevant, as social conditions strongly influence the level of local security. The link between joblessness and petty crime has become a subject of interest for sociologists, psychologists, and social service professionals, who view it as shaped by community norms, environment, and prevailing local attitudes[7].

In the face of growing challenges related to cybersecurity and disinformation, it is essential to strengthen the protection of critical infrastructure and to develop effective crisis management strategies. Digital education and public awareness play a vital role in countering disinformation and enhancing resilience to cyberattacks. Both digital and security education are increasingly important in the context of threats arising from rapid technological advancement. In a digitized world, where technology permeates nearly every aspect of life, the ability to use digital tools safely and responsibly is fundamental. Such education enables a better understanding of cyber risks and fosters the ability to respond effectively.

International cooperation, innovation in digital security, and continuous threat monitoring are becoming central to ensuring global stability and protection. In this fast-evolving environment, adaptation and proactive responses are necessary to guard against increasingly sophisticated threats. Preparing for unlikely yet possible scenarios is also crucial, as technological complexity and the speed of change increase the risk of unforeseen events. Societal readiness and adaptability must be developed, alongside critical thinking and analytical skills that allow individuals to verify information sources and resist manipulation in an era of widespread disinformation[8].

[7] T. Wojciechowski, *Bezpieczeństwo lokalne w wybranych gminach powiatu koszalińskiego*, „Ius et Securitas" 2025, No. 1, p. 30.

[8] T. Wojciechowski, *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas" 2024, No. 1, p. 92.

These interwoven dynamics – spanning cultural norms, demographic trends and local vulnerabilities – highlight the urgent need to reconsider how public institutions, particularly at the local level, adapt to the rapidly evolving conditions of the digital era. This necessitates a closer examination of the institutional capacities, coordination mechanisms and strategic frameworks that shape resilience in the face of emerging risks.

These risks are particularly evident among children, who have become especially vulnerable to digital exclusion in the wake of the COVID-19 pandemic. The shift to online education has underscored stark inequalities in access to technology, with serious consequences for their educational and social development. Recent research highlights that not all children in Europe have access to a computer or home internet connection – resources that became essential during the pandemic. For many, especially in vulnerable households, the lack of connectivity meant falling behind in school and losing contact with peers. This phenomenon, described as *digital deprivation*, refers to children living in households that cannot afford a computer and/or home internet access. On average, around 5.4% of children in the EU are affected, but national disparities are striking: from less than 1% in Iceland to over 20% in Bulgaria and Romania[9].

The pandemic has revealed that the so-called *first-level digital divide* – previously considered resolved – remains a real barrier for many families. While earlier studies assumed that most households had at least basic access to digital infrastructure, the reality proved otherwise. In response, attention has returned to access itself, without abandoning the importance of digital competencies (*second-level divide*). Factors such as low parental education, material deprivation, poverty, or being part of a large family are associated with a higher risk of digital deprivation. However, these patterns are not uniform across Europe. For example, living in a family of non-European immigrant origin increases the likelihood of deprivation in many Western countries, but not in Eastern Europe or the Baltics[10].

The persistence of these inequalities is a pressing issue for public policy. Digital access is no longer optional – it has become a basic condition for full

[9] S. Ayllón, H. Holmarsdottir, S. Lado, *Digitally Deprived Children in Europe*, „Child Indicators Research" 2023, No. 16, pp. 1315-1317.

[10] Ibidem.

participation in education, culture, and society. Without addressing the root causes of digital deprivation, especially among children, efforts to build digital resilience and social cohesion may remain incomplete. Therefore, closing this gap requires both investment in infrastructure and targeted social support, adapted to the diverse socio-economic realities across Europe.

Digital security and local resilience in the EU

Digital transformation plays a crucial role in advancing sustainable development in OECD countries and the European Union. In response to the unprecedented challenges posed by the COVID-19 pandemic, the EU focused on reshaping its economic model through the advancement of information and communication technologies, and more recently, artificial intelligence systems. Recognizing the need to restructure its socio-economic foundations, the EU integrated widespread ICT adoption into its broader strategy for building an information society. The objective is to foster digital integration and develop infrastructure suited to the ongoing digital revolution within public policy frameworks. The implementation of artificial intelligence in public sector operations is also gaining importance. As a result, EU policy on digital skills, digitization, and e-governance encompasses a wide range of initiatives, legal frameworks, and strategies aimed at enhancing digital economies, improving public administration efficiency, and raising citizens' digital competencies across member states. Although the EU treaties do not explicitly define regulations for ICT, actions are undertaken within the scope of the Treaty on the Functioning of the European Union. A growing concern, however, is the unequal access to digital space. Despite the opportunities it offers, not all EU citizens can benefit equally due to infrastructural, financial, or skill-related barriers. To address this, the EU promotes digital inclusion through public policy efforts focusing on ICT accessibility, assistive technologies, digital literacy, and social inclusion, with the aim of reducing marginalization and improving participation in public, social, and economic life[11]. This general institutional direction is further explored in academic research, which highlights both the structural shifts and the implementation challenges faced by EU member states in their pursuit of digital resilience.

[11] E.M. Włodyka, *Odbiór społeczny bezpieczeństwa realizacji polityk publicznych państwa w obszarze e-administracji: studium przypadku*, „Ius et Securitas" 2024, No. 1, pp. 71-72.

Academic studies underline the vital role of digital transformation in reshaping the socio-economic structures of EU member states. A relevant contribution comes from E. M. Włodyka, who examines how the COVID-19 pandemic accelerated the deployment of ICT and artificial intelligence in public administration. Although EU treaties lack explicit provisions on digital technologies, the Union has developed a range of strategies aimed at improving digital infrastructure, enhancing citizens' skills, and increasing the efficiency of public services. The author also draws attention to persistent inequalities in access to digital tools, often linked to financial or educational limitations. In response, EU initiatives focus increasingly on combating digital exclusion and reinforcing social inclusion within the digital space, which has become a key element of modern public policy[12]. Building on these strategic priorities, cybersecurity emerges as a critical dimension of digital transformation – particularly in light of the growing complexity and severity of cross-border threats to digital infrastructure.

The NIS 2 Directive rightly recognises the transboundary nature of cyberattacks and their potential to disrupt critical infrastructure essential for the functioning of the EU internal market. As a result, both EU institutions and Member States are expected to ensure the protection of such infrastructure against increasingly sophisticated cyber threats. These threats may trigger crisis situations, necessitating measures consistent with crisis management protocols, including temporary restrictions on certain civil liberties. In the Polish legal system, such limitations are only permitted under statutory law, in accordance with constitutional principles. Effective cybersecurity governance requires multilevel cooperation—international, European, and national – as well as information sharing, risk mitigation strategies, and qualified personnel. The availability of skilled professionals is essential for maintaining access to digital services while ensuring resilience and the integrity of ICT systems in both public and private sectors[13]. In this context, crisis management serves as a key operational response mechanism, aligning legal mandates with the practical need for preparedness and coordinated action across multiple levels of governance. Crisis management aims to safeguard the population, their assets,

[12] E.M. Włodyka, *Functioning of Local Government Units in the Light of the Law of 5 December 2024 on Civil Protection and Civil Defence*, „Ius et Securitas" 2024, No. 2.

[13] M. Czuryk, *Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa*, „Ius et Securitas" 2025, No. 1, pp. 10-11.

and essential infrastructure, while ensuring effective coordination and coherence among the systems responsible for these tasks. Its role includes strengthening and maintaining the ability of those systems to anticipate threats, prepare for disruptions, take effective action during emergencies, and support recovery afterwards. This responsibility has also been formally assigned to the regional governor[14]. Beyond immediate crisis response, the responsibility for public security also encompasses long-term environmental risks – requiring sustained coordination across all levels of government, including local authorities.

When analysing the position of local self-government in the context of ecological security, it should be acknowledged that activities undertaken by the State in this area result from the collective involvement of all public authorities and entities operating within the hierarchical framework of the State, including municipalities. Ensuring ecological security requires coordinated and systematic efforts from all responsible bodies, as failure by any one of them undermines the effectiveness of the whole and renders the adopted measures inadequate. It must be clearly stated that ecological security at the national level cannot be effectively achieved without the participation of municipal authorities. At the same time, their role remains limited in scope. Municipalities primarily carry out tasks addressing local matters and serve as a complement to the responsibilities fulfilled by other tiers of self-government, such as districts and regions. Their efforts also align with national-level initiatives conducted by central government institutions. Despite their constrained mandate, municipalities play a significant role in contributing to the broader system of actions undertaken by the State to maintain ecological security[15].

These interrelated domains – digital transformation, cybersecurity, and ecological responsibility – demonstrate that social security in the 21st century cannot be reduced to isolated interventions. Instead, it requires systemic thinking, long-term coordination, and the capacity to operate across institutional, technological, and territorial boundaries. The evolving role of local authorities, combined with supranational frameworks and crisis protocols, points to a growing need for flexible governance structures capable of responding to complex, multidimensional risks.

[14] M. Karpuk, J. Kostrubiec, *Provincial Governor as a Body Responsible for Combating State Security Threats*, „Studia Iuridica Lublinensia" 2024, No. 1, p. 115.

[15] J. Kostrubiec, M. Karpiuk, D. Tyrawa, *The status of municipal government in the sphere of ecological security*, „Hungarian Journal of Legal Studies" 2024, No. 2, p. 177.

Conclusions

The analysis confirms the initial hypothesis: the effectiveness of social security in the digital age cannot be ensured solely through national strategies or investments in technological infrastructure. It also requires the adaptive capacity of local institutions to manage overlapping demographic, digital and informational challenges. Their proximity to citizens makes them uniquely positioned to respond – but also exposes them to structural limitations. These local responses, however, cannot function in isolation. Their success is contingent upon coordination with national frameworks, access to expertise and funding, and clarity in the division of responsibilities. Digital risks, particularly those linked to disinformation or exclusion, demand not just technological solutions but also community-based educational and cultural interventions.

Crisis management, in this context, must be reframed. It should not be understood only as a set of protocols triggered during emergencies, but as an integrated part of long-term institutional resilience. Preparedness, adaptability, and public engagement are increasingly essential components of a functioning security system.

Finally, the findings highlight the pivotal role of trust. Local governments, despite constrained resources, often serve as the primary interface between public policy and social needs. Their ability to maintain social trust may prove more decisive than formal strategies in ensuring resilience under conditions of rapid technological and demographic change.

Bibliography

Ayllón S., Holmarsdottir H., Lado S., *Digitally Deprived Children in Europe*, „Child Indicators Research" 2023, No. 16.

Bonnett N.L., Birchall S.J., *The influence of regional strategic policy on municipal climate adaptation planning*, „Regional Studies" 2023, No. 1.

Cholewińska D., *Media społecznościowe w dobie kryzysu demograficznego w Polsce. Szanse, wyzwania, zagrożenia*, „Ius et Securitas" 2025, No. 1.

Czuryk M., *Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa*, „Ius et Securitas" 2025, No. 1.

Hanandini D., *Social Transformation in Modern Society: A Literature Review on the Role of Technology in Social Interaction*, „Jurnal Ilmiah Ekotrans & Erudisi" 2024, No. 1.

Jaeger L., Eckhardt A., *Eyes wide open: The role of situational information security awareness for security-related behaviour*, „Information Systems Journal" 2021, No. 3.
Jovanović M., Dlačić J., Okanović M., *Digitalization and society's sustainable development – Measures and implications*, „Zbornik radova Ekonomskog fakulteta u Rijeci: *časopis* za ekonomsku teoriju i praksu" 2018, No. 2.
Karpuk M., Kostrubiec J., *Provincial Governor as a Body Responsible for Combating State Security Threats*, „Studia Iuridica Lublinensia" 2024, No. 1.
Kostrubiec J., Karpiuk M., Tyrawa D., *The status of municipal government in the sphere of ecological security*, „Hungarian Journal of Legal Studies" 2024, No. 2.
Olsson T., Viscovi D., *Digitalised Welfare: Access, Usage, and Outcomes Among Older Adults*, „Media and Communication" 2023, No. 3.
Włodyka E.M., *Functioning of Local Government Units in the Light of the Law of 5 December 2024 on Civil Protection and Civil Defence*, „Ius et Securitas" 2024, No. 2.
Włodyka E. M., *Odbiór społeczny bezpieczeństwa realizacji polityk publicznych państwa w obszarze e-administracji: studium przypadku*, „Ius et Securitas" 2024, No. 1.
Wojciechowski T., *Bezpieczeństwo lokalne w wybranych gminach powiatu koszalińskiego*, „Ius et Securitas" 2025, No. 1.
Wojciechowski T., *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas" 2024, No. 1.

* * *

Zabezpieczenie społeczne w erze transformacji cyfrowej: wyzwania demograficzne, instytucjonalne i technologiczne

Streszczenie

Niniejszy artykuł podejmuje problematykę przekształceń systemu zabezpieczenia społecznego w kontekście dynamicznych zmian wywołanych transformacją cyfrową, procesami demograficznymi oraz ewolucją instytucji publicznych. Szczególny nacisk położono na znaczenie szczebla lokalnego, który w praktyce najczęściej staje się pierwszym ogniwem reagującym na skutki wykluczenia cyfrowego, dezinformacji, starzenia się społeczeństwa czy zagrożeń ekologicznych. W oparciu o analizę polityk publicznych, dokumentów strategicznych oraz wyników badań naukowych, autor wskazuje na konieczność rozumienia zabezpieczenia społecznego nie jako zbioru odrębnych działań administracyjnych, lecz jako zintegrowanego systemu opartego na synergii infrastruktury, edukacji, zarządzania kryzysowego i zaufania obywateli do struktur państwa. Artykuł stanowi próbę odpowiedzi na pytanie, w jaki sposób instytucje mogą efektywnie adaptować się do złożonych, nakładających się wyzwań współczesności w warunkach postępującej cyfryzacji życia społecznego.

Słowa kluczowe: transformacja cyfrowa, odporność lokalna, bezpieczeństwo społeczne.