Technoarete Transactions on Advances in Computer Applications (TTACA)
Volume 5, Issue 2, June 2026
e-ISSN: 2583-3472

Bridging the Digital Divide: The Evolving Role of the National Telecoms Regulator in Achieving Sustainable Development Goals

Agnieszka Budziewicz-Guźlecka

University of Szczecin, Szczecin, Poland
Corresponding Author Email: Agnieszka.budziewicz-guzlecka@usz.edu.pl

Abstract

This article analyses the role of the Office of Electronic Communications (UKE) in the process of bridging the digital divide in Poland in the context of achieving the Sustainable Development Goals (SDGs). Particular attention is paid to Goal 9 (Industry, Innovation and Infrastructure) and Goal 10 (Reduced Inequalities). The aim of the article is to assess the changing role of the telecommunications regulator as a key factor in combating digital exclusion in Poland and in the implementation of the 2030 Agenda. An analysis of telecommunications policy highlights the need to shift from merely providing infrastructure to co-creating a digital ecosystem, with a particular focus on the intensive development of digital skills. Digital awareness is central to combating digital exclusion. The analysis demonstrates that a modern regulatory body must combine supervisory functions with the role of coordinator of socio-economic innovation, which is a prerequisite for removing digital barriers at regional and social levels. These measures will reduce the infrastructure gap between urban and rural areas. The study utilized an analysis of original research conducted in 2024 (a representative sample of 1,080 respondents) and case studies of selected regulatory interventions. Our own research has shown that the greatest gaps lie in the areas of cybersecurity and the safe use of e-services, which exacerbates the divide between urban and rural areas. The conclusion sets out recommendations for regulatory policy in the era of 5G roll-out, highlighting the need for systematic education in digital skills as a prerequisite for building an inclusive information society.

Keywords

Broadband infrastructure, digital competences, digital exclusion, regulatory policy, sustainable development, telecommunications market.

INTRODUCTION

The current digital transformation, driven by the roll-out of fifth-generation (5G) networks and the Internet of Things (IoT), is redefining the structure of the global economy and social relations. In the age of the information society, access to information and communication technologies (ICT) is no longer merely a factor in market advantage. It has become the foundation of social inclusion, underpinning the realization of fundamental civil rights, access to education, healthcare and the modern labour market. For this reason, the United Nations 2030 Agenda for Sustainable Development explicitly identifies digital technologies as a key catalyst for development [1] [2] [3]. This issue is particularly relevant to Goal 9 (Industry, Innovation and Infrastructure), which focuses on building reliable infrastructure, and to Goal 10 (Reduced Inequalities), which aims to eliminate socio-economic and territorial disparities [4] [5]. At the same time, the dynamic development of the networked environment closely links these aspirations to Goal 4 (Quality Education), particularly in terms of developing the advanced technical and digital skills required in today's labour market, which is essential for the effective use of available technologies [6].

The traditional approach to the issue of the digital divide focused on the so-called 'first-level digital divide', which is equated with infrastructure barriers and a lack of physical access to networks and computer equipment [7] [8]. However, the rapid expansion of broadband investment, funded in part by EU funds, has led to a radical reduction in physical 'white spots' on the map of Poland. As a result, the focus of the research problem has shifted towards second-level digital exclusion. This encompasses motivational barriers, a lack of advanced digital skills, and deficits in awareness of online risks [9]. The mere presence of telecommunications infrastructure in 'digital dead zones' – often rural areas – does not automatically guarantee social inclusion if the residents of these areas lack the skills to use e-services safely and in a cost-effective manner.

This evolution of the exclusion paradigm poses new challenges for public institutions, and in particular for Poland's national telecommunications regulator – the Office of Electronic Communications (UKE). The traditional model of market regulation, centred on breaking up monopolies, allocating radio frequencies and controlling wholesale access, is becoming insufficient in the era of the digital ecosystem [10].

A modern regulatory body must evolve from the role of a passive arbiter and supervisor towards that of an active coordinator of socio-economic innovation, combining hard supervisory instruments with soft educational and partnership-based measures.

This article attempts to assess this changing role of UKE as a key player in the process of implementing the 2030 Agenda and tackling secondary digital exclusion in Poland. The main research objective is to analyse the transformation of the

e-ISSN: 2583-3472

regulator's role from the perspective of co-creating an inclusive digital ecosystem, with particular emphasis on fostering digital literacy amongst the public.

The article puts forward the following research hypotheses:

- H1: Contemporary digital exclusion in Poland is no longer purely technological in nature, but has become a problem of skills and motivation (second level), which may widen the development gap between urban and rural areas.
- H2: The key barrier to the full uptake of e-services by the public lies in gaps in cybersecurity and fear of online threats, rather than a lack of physical access to the internet.
- H3: The effective implementation of the Sustainable Development Goals requires the regulator (UKE) to transition into the role of a creator of a digital education ecosystem, in which inclusive education and skills development (SDG 4) act as an essential catalyst for infrastructural transformation (SDG 9) towards reducing socio-spatial inequalities (SDG 10).

In order to verify the hypotheses formulated in this way, the study employed research method triangulation. The empirical basis consists of the results of original quantitative research conducted in 2024 on a representative sample of adult Poles (N=1,080), supplemented by case studies of selected flagship regulatory and educational interventions undertaken by UKE. This article summarises the current state of knowledge regarding barriers to digitalization in Poland and formulates practical recommendations for regulatory policy in the era of the mature roll-out of 5G technology.

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

The Multi-Level Evolution of the Concept of the Digital Divide

The theoretical conceptualization of the digital divide has undergone a profound evolution over the last three decades: from a dichotomous technological approach to a multidimensional socio-cognitive construct. The literature on the subject, dating from the 1990s, defined this phenomenon in binary terms as a division between those with physical access to computers and telecommunications networks and those who lacked such access [11]. This approach, now referred to as the 'first-level digital divide', was based on a technocratic paradigm. It assumed that the provision of technological capital and the removal of infrastructure barriers (so-called 'white spots') would automatically lead to digital inclusion [12].

As markets have become relatively saturated with broadband infrastructure, researchers such as van Dijk and Hargittai have demonstrated that merely providing physical access to information does not eliminate structural inequalities [13]. They laid the foundations for the concept of the 'second-level digital divide', which redefines the barrier to entry from the level of 'having' (access) to the levels of 'knowing how' (skills) and 'wanting' (motivation) [14] [15].

Within this paradigm, three key sub-components are identified:

1. The motivational barrier (attitudinal/psychological divide) – resulting from technophobia, a lack of perceived usefulness of technology, and a fear of digital exclusion due to a lack of a sense of security.
2. The skills barrier (skills divide) – encompassing both operational skills (using hardware and software) and information and communication skills.
3. The ability to select and evaluate content (critical digital literacy) – the ability to critically analyse data, distinguish information from disinformation (fake news) and navigate safely within the ecosystem of public and commercial e-services.

Contemporary literature (which often already addresses the issue of third-degree exclusion) emphasises the feedback loop between digital exclusion and social exclusion. Skills gaps and fear of technology translate directly from digital exclusion into social exclusion, as they lead to a weaker position in the labour market, financial exclusion and a reduction in an individual's social and cultural capital [16].

Emerging theoretical discussions suggest that future network evolutions (such as AI integration and 6G concepts) may extend digital inequality into a 'third-level digital divide'. In this prospective framework, barriers may shift from basic device usability toward cognitive interaction with automated systems, potentially giving rise to disparities in AI literacy and data-driven autonomy. This process shifts the focus to the so-called 'third-level digital divide', which concerns the inability to translate network access and basic skills into tangible life, economic and social benefits. In AI-native network environments (where algorithms form a native network layer), the traditional dichotomy of 'having' versus 'knowing how to use' gives way to a barrier to cognitive cooperation. A phenomenon known as 'prompt illiteracy' is emerging, in which vulnerable groups (e.g. older people) lose the ability to communicate effectively with autonomous assistants managing e-services. Furthermore, the 'data divide' means that users with low cognitive capital become merely passive data providers for algorithms, whilst privileged individuals dramatically increase their market advantage through AI-based automation. Emerging theoretical literature suggests that future technological developments, such as artificial intelligence (AI) integration and conceptual 6G frameworks, may give rise to a prospective 'third-level digital divide'. In this context, researchers note that barriers could shift from basic hardware usability toward cognitive interaction with automated systems, potentially widening socio-technical inequalities for digitally vulnerable groups.

The 2030 Agenda and Technology: The Role of ICT as a Catalyst for the Sustainable Development Goals (SDGs)

The incorporation of information and communication technologies (ICT) into the sustainable development paradigm was endorsed by the United Nations in the 2030 Agenda. Although digital technologies do not constitute a separate, dedicated goal, the international literature

e-ISSN: 2583-3472

unequivocally classifies them as a horizontal enabler accelerating the implementation of all 17 Sustainable Development Goals (SDGs) [17] [18]. The International Telecommunication Union (ITU) points out that without widespread, secure and inclusive digitalization, achieving the goals of economic and social transformation by 2030 is structurally impossible.

In the context of this study, the synergy between the three goals of the Agenda is of key importance:

- Goal 9: Industry, innovation and infrastructure (SDG 9) – in particular target 9.c, which explicitly calls for a significant increase in access to information and communication technologies and for efforts to ensure universal and affordable access to the internet. At the national level, this means not only building the network, but also ensuring its resilience and universal usability,
- Goal 10: Reduced inequalities (SDG 10) – focused on reducing income and social disparities. In the era of the e-government and the e-economy, asymmetry in access to and skills in using digital tools (second level) is becoming a new, powerful factor in social stratification. This generates the phenomenon of territorial marginalization (primarily in rural areas) and demographic marginalization (the classic generation gap) [19].
- Goal 4: Quality education (SDG 4) – in the era of digital transformation, Target 4.4 takes on crucial importance, as it requires a significant increase in the number of young people and adults possessing the relevant skills, including technical and vocational skills, for the purposes of employment and entrepreneurship. Indicator 4.4.1 (percentage of people with information and communication technology (ICT) skills) directly translates educational issues into the digital sphere. From this perspective, formal education is not merely the preserve of the formal education system, but becomes an integral part of lifelong learning, which is co-created by specialised public institutions.

From the perspective of the article's theoretical framework, the actions of the telecommunications regulator constitute a direct interface linking SDG 9, SDG 4 and SDG 10. Infrastructural progress alone (SDG 9), without integrated, high-quality educational program in digital skills (SDG 4), proves insufficient to prevent social polarization. It is only by stimulating cognitive and skills-based capital that the loop of ecosystemic transformation is closed, enabling a tangible reduction in socio-spatial inequalities (SDG 10).

THE EVOLUTION OF THE UKE'S ROLE IN POLAND

An analysis of source material, strategic documents and activity reports by the President of the Office of Electronic Communications (UKE) allows us to reconstruct the process of institutional evolution of the Polish regulator. This process was not linear, but rather a sequence of responses to changing market, technological and social conditions. UKE's transformation can be divided into three distinct phases, which reflect the transition from a purely market-based paradigm to an ecosystem-based regulatory model.

Historical Phase: Market Consolidation and Ex-Ante Regulation (Regulator 1.0)

In the early days of the telecommunications regulator's operations in Poland, the institutional priority was the implementation of the EU regulatory framework aimed at breaking up the monopoly in the sector. UKE's activities centred on ex-ante hard economic regulation instruments. The main objective was to break the monopolistic position of the incumbent operator (Telekomunikacja Polska) and to stimulate competition in terms of demand and pricing. The key mechanisms of this phase included:

- Regulation of wholesale rates (MTR/FTR) – the setting of asymmetric, and subsequently symmetric, rates for call termination on mobile and fixed networks, which enabled new operators to develop,
- Local loop unbundling (LLU) – imposing regulatory obligations regarding the unbundling of the incumbent operator's copper infrastructure, which lowered barriers to entry into the internet services market,
- Allocation of scarce resources (spectrum) – conducting tenders and auctions for radio spectrum (including key LTE auctions), generating revenue for the state budget and imposing minimum coverage obligations on operators.

During this period, success was measured by economic indicators: a fall in prices for end-user services, an increase in market penetration, and the number of ported numbers. Digital exclusion was then equated solely with economic barriers and the absence of a physical telephone line in the household.

Transition Phase – Infrastructure Mapping and Geolocation of 'White Spots'

As the simple reserves for price competition were exhausted and mobile and fibre-optic technologies became widespread, UKE entered a transition phase. This coincided with the implementation of the Digital Poland Operational Program (POPC). The dominant challenge became mapping the actual state of the country's telecommunications infrastructure and precisely identifying areas affected by structural underdevelopment (so-called 'white spots').

The turning point in this phase was the implementation of advanced ICT systems for collecting spatial data on broadband networks. The annual inventory of telecommunications infrastructure conducted by UKE became a key tool. These tools enabled:

- Real-time data aggregation – replacing operators' declarative, annual reports with a dynamic database on service availability at specific addresses,
- The effective targeting of public subsidies – data from UKE's systems formed the basis for designating competition areas for public interventions under the National Recovery Plan (KPO) and the European Funds for Digital Development (FERC) program,
- Empowerment of consumers – citizens have gained public access to search tools (e.g. internet.gov.pl), enabling them

e-ISSN: 2583-3472

to check available services and submit requests for network roll-out.

During the transitional phase, UKE's role evolved from that of an institution solely responsible for price regulation into a government analytical and information centre, providing the hard data necessary to achieve Goal 9 of the 2030 Agenda (building resilient infrastructure).

A New Institutional Role: 'Soft Regulation' and Co-Creation of the Digital Ecosystem (Regulator 2.0)

The current phase of UKE's activities, which will be fully evident in 2025 and 2026, is characterized by the final transition to the Ecosystem Regulator model. Experience gained from the roll-out of KPO/FERC networks and the widespread adoption of the 5G standard has shown that extending fibre-optic cables to property boundaries in rural areas does not automatically generate demand for advanced e-services. In response to this challenge, UKE has reoriented its strategy, shifting the focus from ex-ante regulation to soft regulation measures. UKE's current catalogue of interventions in the social sphere is based on three pillars:

- Original educational program tailored to at-risk groups – UKE has ceased to be an impersonal institution, actively developing projects such as 'Klikam z głową' (online safety for the youngest in the age of smartphones) and 'W sieci zdrowego rozsądku' (overcoming motivational barriers and the fear of cyber threats amongst older people),
- Building cross-sector partnerships – UKE acts as a facilitator of relations between the market (commercial operators) and civil society (non-governmental organizations). Examples include joint initiatives with research institutes (e.g. NASK) aimed at combating disinformation and building public trust in new wireless technologies (5G),
- Institutional support for local government bodies (JST) – by initiating local digitalization pacts, the regulator supports smaller rural municipalities in providing digital education to opinion leaders (e.g. local officials, teachers), who become natural ambassadors for digital transformation in the regions.

The findings of the institutional analysis show that UKE has successfully adapted the structure of its activities to the requirements of the 2030 Agenda. By combining supervisory functions with the role of coordinator of socio-economic innovation, the regulator has shifted the focus from the struggle for access to the network itself (SDG 9) to a systemic approach to countering secondary social and territorial inequalities (SDG 10).

The Concept of the 'Ecosystem Regulator' and the Transformation of Public Institutions

The evolving nature of the digital divide necessitates a redefinition of the public governance paradigm and the role of national regulatory authorities (NRAs), such as the Office of Electronic Communications in Poland. Classical economic regulation theory, rooted in the new institutional economics school, assigned the telecommunications regulator the role of a technocratic arbiter [20]. Its fundamental tasks included correcting market failures, breaking up monopolies, managing a scarce resource (radio frequencies) and stimulating infrastructure investment through the regulation of wholesale access [21] [22].

In a mature digital economy, this traditional model (often referred to as 'Regulator 1.0') is becoming obsolete. The theory of institutional transformation points to the need to move towards a 'Regulator 2.0' or 'Ecosystem Regulator' model. In this framework, the regulatory body ceases to be merely a supervisory and sanctioning authority, and instead becomes an active moderator and architect of a multifaceted digital ecosystem.

This transformation is based on three theoretical pillars:

- Public Value Creation – a concept developed by Mark Moore, according to which the aim of institutions is not merely to enforce the law, but to generate measurable social benefits, including the building of an inclusive society [23].
- Flexible and participatory regulation (Soft Regulation / Responsive Regulation) – a shift from rigid administrative decisions towards building governance networks involving operators, non-governmental organizations and local government bodies.
- Coordination of socio-economic innovation – an approach in which the regulator stimulates the demand side of the market by actively boosting citizens' trust in technology (e.g. through the certification of secure services and cybersecurity education), which is a prerequisite for the uptake of next-generation networks (5G/6G).

MATERIALS AND METHODS

The quantitative fieldwork was conducted between September 20 and October 30, 2024, using the Computer-Assisted Web Interview (CAWI) technique on the Poznaj.to nationwide research panel managed by PBS. The sampling frame comprised adult Polish internet users. The primary questionnaire instrument consisted of 12 single-choice questions, 17 multi-item grid questions, 3 multiple-response questions, and 8 socio-demographic items. Quality control was conducted on 100% of the completed questionnaires, eliminating speeders and incomplete responses. The survey achieved an overall completion/response rate of 82.4% among eligible panelists who initiated the questionnaire. The research sample was selected using a two-stage stratified random sampling method. Prior to the draw, respondents were stratified by province and then, within each province, by category of place of residence, distinguishing between large towns (over 100,000 inhabitants), medium-sized towns (20,000–100,000 inhabitants), small towns (under 20,000 inhabitants) and rural areas. In the stratified sampling, proportional allocation was applied at the voivodeship level in proportion to the number of residents aged 18 and over, and at the settlement size category level in proportion to the number of municipalities of the relevant sizes.

e-ISSN: 2583-3472

The study population consisted of people aged 18 or over living in Poland. A total of 1,080 interviews were conducted. The quantitative method and sample selection used in the study allow the results to be generalized to the entire adult population with a margin of error of +/- 3.0% (95% confidence level).

Table 1. Breakdown of respondents by size of place of residence

Size of the City	%	Number of Respondents
Rural areas	39,4%	430
A town with up to 20,000 inhabitants	13,3%	143
A town with a population of 20,000–100,000	19,7%	200
A town with a population of 100,000 or more	27,6%	305
Total	**100%**	**1080**

Source: own analysis

The survey was monitored in two ways:

- Field monitoring – whilst the survey was being conducted, the responses received were monitored on an ongoing basis, which made it possible to respond to and eliminate instances where the data raised concerns, e.g. where the time allowed to complete the questionnaire was too short, or where there were undesirable trends, inconsistencies or discrepancies in the responses. The questionnaire's structure prevented panellists from skipping key questions, such as those presenting content relevant to the survey,
- Off-site quality control – a substantive analysis enabled the elimination of incomplete or unreliable data. Quality control covered 100 per cent of the collected data, during which the consistency of responses, response patterns and the wording of answers to semi-open-ended questions were analysed.

Before the analyses began, the dataset underwent a weighting procedure, the aim of which was to correct for discrepancies between the resulting empirical distributions and the structure of the general population, taking into account the characteristics used in the stratification.

An iterative weighting methodology (RIM) was applied, utilizing the following characteristics: province, settlement size class, age and gender.

Spearman's correlation coefficient was used for the purposes of the analyses. It is used when the data do not follow a normal distribution or consist of categorical variables. The correlation can take values from -1 to +1. An extremely negative correlation value means that the higher the value of one variable, the lower the value of the other. When the result is extremely positive, it means that both values will increase or decrease simultaneously. A correlation value of 0 indicates a complete lack of relationship between a given pair of variables.

For the purposes of the Chi-squared test, the 'refused' and 'difficult to say/don't know' categories were not taken into account. Otherwise, footnotes might have appeared alongside the test values, stating that the test result may be unreliable and does not meet the test's assumptions.

Verifying the research hypotheses put forward requires comparing the theoretical model of the 'Ecosystem Regulator' with the actual competence deficits within Polish society. As demonstrated in the literature review, modern digital exclusion is no longer solely an infrastructural problem (first-level gap), but has become a mental and cognitive barrier (second-level gap). An analysis of the results of a nationwide quantitative survey (N=1,080) provides significant evidence to support this phenomenon, particularly in the areas of cybersecurity, the safe use of e-services and skills asymmetry. It should be noted that the survey design is cross-sectional and observational in nature. Consequently, the statistical associations, Chi-squared tests, and Spearman rank correlation coefficients reported herein describe co-occurrences and relationships between demographic, attitudinal, and competence variables, but do not directly establish causal mechanisms.

The qualitative arm relies on descriptive, institutional case studies of UKE's interventions. These case studies serve to illustrate regulatory frameworks and program outputs rather than provide formal counterfactual impact assessments.

RESULTS: AN EMPIRICAL ANALYSIS OF SECOND-LEVEL DIGITAL EXCLUSION IN POLAND IN THE LIGHT OF QUANTITATIVE RESEARCH

Gaps in Awareness of Online Threats and Digital Identity Management

A key element of secondary digital exclusion is the so-called psychological and operational barrier, manifested in the inability to safeguard one's own online presence. The study conducted demonstrates that Poles' behaviour regarding the protection of personal data is in clear contradiction to the requirements of a secure information society.

As many as 59.1% of respondents admit that they have sent scans of documents or sensitive personal data via email or instant messaging without any encryption. Furthermore, over half of users (56.3 per cent) regularly or occasionally use open, public Wi-Fi networks to carry out sensitive activities, such as logging into online banking, email or making online purchases. However, the most common behavioural mistake remains a lack of attention to the uniqueness of login credentials – as many as 72.7 per cent of respondents use the same password in more than one online account (including 17.2 per cent who do so consistently).

e-ISSN: 2583-3472

Importantly, a correlation analysis shows that the severity of these errors is determined by demographic and income metrics. A negative correlation with age was observed – older people are less likely to admit to making obvious mistakes online; however, as demonstrated later in this report, this stems from their lower level of online activity and greater technophobia, rather than from greater technical competence. With regard to income, it was observed that a higher financial status tends to encourage greater caution online.

While these observed correlations demonstrate statistical associations between age, income, and cybersecurity practices, they reflect cross-sectional patterns rather than direct cause-and-effect relationships.

Deficits in Cognitive and Operational Competences

Testing hypotheses H1 and H2 required an examination of the declarative level of knowledge. The data collected reveal a marked asymmetry between the prevalence of ICT use and the level of critical digital illiteracy. Selected research findings are as follows:

- Verifying the security of sources – nearly half of adult Poles (46.4 per cent) explicitly state that they lack the ability to verify the security of links and attachments in emails without opening them. This poses a direct threat in the context of mass phishing attacks, Chi-squared tests confirmed significant association with gender ($chi2 = 36.49$, $df = 2$, $p < 0.001$), age ($chi2 = 14.43$, $df = 4$, $p = 0.006$), and household income ($chi2 = 21.11$, $df = 5$, $p = 0.002$), while no significant association was observed with place of residence ($chi2 = 3.32$, $df = 4$, $p = 0.508$),
- Password security management – as many as 63.4 per cent of the population lack basic knowledge of how to check whether their password has been compromised in a mass data breach and is known to cybercriminals,
- Incident response – over a third of citizens would not know how to respond in critical situations where their digital integrity has been compromised. In the event of an email account being compromised, 37.9 per cent of respondents say they would feel helpless, whilst 37.8 per cent would feel the same in the event of data loss due to hardware failure. Almost 40 per cent of Poles are also unable to name any public institution or body (e.g. CERT) to which attempts at cyber-attacks should be reported.

A particularly worrying picture emerges from the analysis of competence in managing mobile devices (smartphones), which, in the era of 5G networks, constitute the main gateway to e-government. In the event of a phone being lost or stolen, as many as 60 per cent of respondents would be unable to remotely wipe its contents, and nearly half would be unable to remotely recover files (48.7 per cent) or messages (around 50 per cent).

Statistical analysis (chi-squared test and correlations) revealed two key correlations in this area, namely: women were significantly more likely than men to report a lack of the technical skills necessary to remotely lock the device, locate a phone or recover data; and that age remains the strongest differentiating factor – the older the respondent, the lower their operational competence in crisis situations (a negative correlation with age). The income variable has a similar, albeit positive, effect – higher economic capital goes hand in hand with higher cognitive capital. The inability to remotely wipe device content showed a significant negative correlation with age ($r_s = -0.189$, $p < 0.001$) and a significant association with gender ($chi2 = 48.16$, $df = 2$, $p < 0.001$), with female respondents reporting lower confidence in technical device management.

It is worth emphasizing that the deficits in basic digital hygiene identified in the study represent a direct starting point for the deepening of third-degree exclusion in the coming era of AI networks. Given that almost half of the respondents show a lack of coping skills when faced with classic threats such as phishing or remote smartphone management, the interaction of this population with autonomous assistants and the phenomenon of the data divide will generate an even deeper cognitive asymmetry. A lack of basic skills in verifying digital identity or securing passwords will prevent these groups from cooperating safely with artificial intelligence algorithms. These identified deficits in basic digital hygiene highlight that low operational competence and cybersecurity anxiety remain major hurdles. Without foundational digital safety skills, users are less likely to safely adopt more advanced digital services or navigate emerging automated and AI-driven public platforms.

A detailed summary of the main survey variables measuring digital hygiene, operational competencies, and their statistical associations with key socio-demographic factors is presented in Table 2.

Table 2. Key survey indicators of second-level digital exclusion and their socio-demographic associations (N=1,080)

Category / Variable	Sub-Category / Response	Prevalence (% of respondents)	Significant Demographic Associations & Test Statistics
Cybersecurity Practices & Digital Hygiene	Sending unencrypted sensitive personal data/scans via email/instant messaging	**59.1%**	Negatively correlated with age; positively correlated with household income.
	Using open, public Wi-Fi for sensitive activities (banking, e-shopping)	**56.3%**	Higher frequency among younger age groups and active internet users.

Category / Variable	Sub-Category / Response	Prevalence (% of respondents)	Significant Demographic Associations & Test Statistics
	Reusing the same password across multiple online accounts	**72.7%** *(17.2% consistently)*	Widespread across all groups; lower caution among lower-income respondents.
Cognitive & Verification Deficits	Inability to verify link/attachment security without opening	**46.4%**	**Gender:** chi2 = 36.49, df = 2, p < 0.001**Age:** chi2 = 14.43, df = 4, p = 0.006 **Income:** chi2 = 21.11, df = 5, p = 0.002 **Residence:** chi2 = 3.32, df = 4, p = 0.508 (n.s.)
	Lack of knowledge on checking if passwords have been compromised	**63.4%**	Statistically significant negative correlation with age (p < 0.001).
	Unawareness of reporting bodies/institutions for cyberattacks (e.g., CERT)	**~40.0%**	Higher proportion of unawareness in rural areas and small towns.
Crisis Management & Operational Competencies (Smartphones)	Helplessness in case of email account compromise	**37.9%**	Strongly associated with older age categories and lower digital self-efficacy.
	Helplessness in case of data loss due to hardware failure	**37.8%**	Negatively associated with educational attainment and income level.
	Inability to remotely wipe phone contents if lost/stolen	**60.0%**	**Age:** r_s = -0.189, p < 0.001**Gender:** chi2 = 48.16, df = 2, p < 0.001 (lower confidence among female respondents)
	Inability to remotely recover lost files or messages	**48.7% – 50.0%**	Significant negative correlation with age (p < 0.001).

Source: own analysis

Case Studies: UKE's Educational and Regulatory Interventions in Practice

The following descriptive case studies highlight two flagship educational initiatives launched by the Office of Electronic Communications (UKE). The evaluation presented here is based on programmatic objectives, thematic scope, and output metrics (such as reach and nominations), while long-term behavioral and societal impact indicators remain subject to future longitudinal evaluation studies. In order to empirically verify the 'Ecosystem Regulator 2.0' paradigm (hypothesis H3) and to assess the actual mechanisms for combating second level, two flagship educational and preventative program implemented by the Office of Electronic Communications were analysed. These initiatives were deliberately targeted at marginalized demographic groups which, in quantitative studies, were found to be most vulnerable to online threats.

The 'Click Wisely' campaign – building digital resilience from the ground up

The 'I Click Wisely' campaign represents a soft, horizontal regulatory approach, in which UKE moves away from the role of a technocratic arbiter towards that of a creator of cognitive capital (in line with SDG 4). The target group comprises primary school pupils, teachers and parents. The main thematic pillars include: cyberbullying (hate speech), the protection of one's image and personal data online, and the pitfalls of artificial intelligence (including deepfake). In terms of scale and operational innovation, the program is based on interactive webinars and dedicated workshops. The campaign directly addresses the challenges set out in hypothesis H3. It demonstrates that the key to technology adoption is not merely physical access to the internet, but the ability to critically evaluate content and defend against algorithmic manipulation. The success of this approach is confirmed by the project's nomination for the international ITU WSIS Prizes 2026, which places the Polish regulator among the world's leading institutions implementing the 2030 Agenda.

Another example is the 'Seniors Online' project – bridging the generation gap and overcoming technophobia

The second intervention directly addresses the issue of demographic marginalization described in the theoretical section and confirmed by statistical tests (a negative correlation between competence and age). The project is being carried out in collaboration with non-governmental organizations (including the MANKO Association). The target group consists of older people who display profound

e-ISSN: 2583-3472

technophobia or passive withdrawal from e-services. The main thematic pillars include: protection against phishing and vishing (telephone fraud and data theft by individuals impersonating public trust institutions) and good digital identity management practices. UKE experts conduct direct regional training sessions, teaching participants how to verify the authenticity of online communications and how to report incidents (e.g. to CERT teams). This qualitative case study provides illustrative support consistent with the assumptions of hypotheses H1 and H3, highlighting how competence and psychological barriers shape exclusion among older adults. The exclusion of older people in rural and small-town areas is purely a matter of competence and psychology. These measures have a tangible impact on the achievement of Goal 10 (Reduced Inequalities), protecting the most vulnerable social group from financial exclusion and digital fraud.

DISCUSSION: AN ASSESSMENT OF THE STATE'S EDUCATION POLICY THROUGH THE PRISM OF THE DIGITAL DIVIDE

In the context of redefining the role of the market regulator (UKE) from that of an economic arbiter to an educational facilitator, public perception of the state's actions to date is crucial. Citizens take a critical view of public institutions' involvement in building digital resilience within society.

When it comes to educating the public about cybersecurity, as many as 32.7 per cent of respondents express a negative opinion, whilst just under 30.4 per cent view it positively. Crucially for testing hypothesis H1, this criticism increases with the respondents' level of education and age (negative correlations). Users with higher levels of competence clearly recognize the anachronism and inadequacy of existing, centralized information campaigns. Furthermore, over 40 per cent of respondents consider the state's actions in the fight against disinformation and 'fake news' to be definitely or rather poor.

Significantly, residents of large cities judge the actions of state institutions much more harshly than rural residents (a statistically significant correlation, $p=0.005$). This stems directly from the fact that the urban population, which makes more intensive use of public and commercial e-services, more frequently encounters systemic barriers and a lack of institutional support, whilst in rural areas this problem is still often masked by a motivational barrier and a complete withdrawal from advanced network interactions. This paradox can be explained through the prism of the psychological concept of aspiration levels and public choice theory. Metropolitan residents, characterized by higher cognitive capital and more intensive digital practices, exhibit significantly higher service level expectations of digital public services. In their case, criticism does not stem from a lack of access, but from cognitive dissonance between a smoothly functioning commercial market (e.g. e-commerce, fintech) and the bureaucratic barriers of the e-government. In rural areas, by contrast, the lower level of criticism may be a result of anchoring – lower expectations of public institutions and less frequent interaction with advanced administrative platforms mean that these citizens are less likely to notice systemic dysfunctions within the state.

It is worth further examining the above perceptual paradox and the behavioural errors identified in studies through the lens of social psychology and behavioural theory. Firstly, the discrepancy between a declared sense of security and actual practices (such as the widespread use of the same password or the transmission of unencrypted personal data) is a classic illustration of the Dunning–Kruger effect in the field of digital hygiene. Heavy internet users tend to exhibit a false sense of superiority and so-called 'cognitive optimism', equating operational proficiency (e.g. fluency in using apps or social media) with cybersecurity competence. As a result, high digital self-confidence paradoxically lulls them into a false sense of security, leading to a drastic reduction in the actual standards of protection for their own identity. Conversely, amongst older people or those who use the internet less frequently, the lower frequency of reported errors stems from an overcautious approach and technophobia, rather than from greater technical knowledge, which creates a false impression of their digital resilience. Secondly, a critical assessment of the state's systemic measures to combat cyber threats is directly linked to the psychological phenomenon of 'alert fatigue'. Today's citizens are constantly bombarded with scattered warning messages – ranging from widespread Civil Defence alerts to repetitive notifications in banking apps. This information overload leads to sensory and cognitive desensitization; as a result, users automatically ignore or thoughtlessly dismiss key warnings, treating them as information noise. For the Ecosystem Regulator 2.0 paradigm, this is a clear signal that traditional, fear-based 'ex-ante warning' techniques have exhausted their effectiveness. A shift towards 'education in action' is essential, which UKE is attempting to implement through interactive scenarios and simulations in its flagship educational program.

A comparison of the illustrative case studies with the quantitative survey results ($N=1,080$) suggests that the regulator's active educational interventions hold strong potential for generating public value by addressing non-infrastructural barriers that market mechanisms alone cannot solve. Traditional market-based instruments are unable to address barriers related to motivation and fear. It is only through UKE's transformation into a body coordinating cybersecurity education (SDG 4) that investments in 5G broadband infrastructure (SDG 9) can be fully and securely capitalized upon.

CONCLUSIONS

The empirical findings from the quantitative survey, complemented by the descriptive case studies, provide strong empirical alignment with hypotheses H1, H2, and H3. Physical access to broadband is no longer a determining factor for digital inclusion. The modern digital divide runs along the lines of operational competence and a

e-ISSN: 2583-3472

psychological sense of security. Widespread illiteracy in the basics of cybersecurity, an inability to manage identities and passwords, and paralysis in crisis situations (phishing, loss of a device) mean that a significant proportion of the population remains 'excluded within the system' – they have access to the infrastructure but are unable to transform it into socio-economic capital.

In this context, a phenomenon comes to the fore that can be defined as the Availability Paradox. It consists in the fact that the closer we get to theoretical, 100 per cent coverage of the country with fibrotic networks and 5G technology (which means the almost complete elimination of primary exclusion), the more drastically social and economic disparities resulting from secondary and tertiary exclusion may grow. The mere fact that a given rural or peripheral area has gained physical access to gigabit bandwidth does not automatically bridge the development gap. If residents of cognitively excluded regions use the modern network solely for simple, passive entertainment or communication, whilst the urban elite actively capitalize on the same connectivity standard for advanced professional purposes, lifelong learning, financial investments or the development of e-entrepreneurship, the gap between them widens dramatically. Modern telecommunications infrastructure, devoid of parallel, systemic development of cognitive capital, thus becomes – counterintuitively – a factor that entrenches and exacerbates socio-spatial inequalities, rather than reducing them. This phenomenon demonstrates that technological accessibility without cognitive inclusion generates an asymmetry of benefits, which directly threatens the achievement of Goal 10 of the 2030 Agenda.

This state of affairs poses a direct challenge to the Office of Electronic Communications. The traditional regulatory model (Regulator 1.0), focused on building infrastructure to eliminate physical 'dead zones', has exhausted its potential for modernization. In the era of 5G, IoT and e-government, UKE must fully embrace the role of Ecosystem Regulator 2.0 (in line with the assumptions of hypothesis H3). This necessitates:

- A shift in financial and operational priorities – from hard measures to stimulate investment in cable and radio infrastructure (SDG 9) to soft educational program that build cognitive capital (SDG 4),
- Coordination of social innovation – creating systemic certification schemes for the security of e-services, dedicated educational platforms on digital hygiene, and multi-level cooperation networks with NGOs and local authorities to address technological anxieties at regional and local levels,
- Focusing on vulnerable groups – bridging the generational and income gaps and addressing gender disparities through targeted workshops on the use of mobile devices and e-services for older people and residents of smaller towns and villages.

Adapting prevention program to the challenges of the AI and 6G era – the new educational mission of the Office of Electronic Communications as an Ecosystem Regulator 2.0 must not be limited to identifying the barriers of the past. The architecture of the upcoming 6G networks requires the regulator to urgently expand its proprietary educational program (such as 'Klikam z głową' or 'Seniorzy online') to include elements of critical AI literacy. The UKE's preventative measures must evolve towards teaching safe interaction with autonomous agents, defence against algorithmic manipulation, deepfake-type disinformation and new forms of fraud (e.g. vishing based on voice cloning by AI). In this context, the phenomenon referred to in the literature as 'authority hallucination' becomes a fundamental challenge. People with low digital literacy, in fact, show a strong tendency to anthropomorphise artificial intelligence systems and to place uncritical, complete trust in the responses generated by large language models (LLMs). When contrasted with the finding from our own research that nearly half of adult Poles (46.4 per cent) lack the basic ability to verify information sources, this deficit leaves vulnerable groups completely defenceless against mass, automated disinformation. Synthetic content, generated autonomously by bots, is equated by digitally illiterate users with objective expert knowledge. This potential over-reliance on automated outputs indicates that future regulatory education frameworks should proactively incorporate critical AI literacy to mitigate emerging risks of automated disinformation and algorithmic exclusion.

Furthermore, at the institutional level, the regulator should aim to develop standards and certification schemes for the inclusivity of artificial intelligence systems deployed in the telecommunications sector, thereby minimizing the risk of citizens being excluded at the level of conversational interfaces.

Only by integrating infrastructure development with widespread, systematic digital education will the national regulator be able to effectively counteract new forms of social stratification and achieve the 2030 Agenda's goals regarding the reduction of inequality (SDG 10).

Acknowledgements

This publication is co-financed by the Minister of Science under the "Regional Excellence Initiative".

REFERENCES

[1]. Shafik, W., 2025, Technology as a catalyst for achieving the Sustainable Development Goals (SDGs). In: Factoring Technology in Global Sustainability: A Focus on the Sustainable Development Goals (Singapore: Springer Nature Singapore), pp. 3–39. DOI: 10.1007/978-981-96-7299-8_1.

[2]. Bocean, C. G., 2025, Sustainable development in the digital age: Harnessing emerging digital technologies to catalyze global SDG achievement. Applied Sciences, 15(2), 816. DOI: 10.3390/app15020816.

[3]. Bajpai, N., and Biberman, J., 2021, Digital transformation and the 2030 sustainable development agenda. ICT India Working Paper, No. 44. https://doi.org/10.7916/d8-ybcz-3d35.

[4]. Rawal, T., Agarwal, S., Pahwa, M., Choudhury, T., and Kanojia, P., 2025, Empowering Economies: The Intersection

e-ISSN: 2583-3472

of Innovation, Industry, and Infrastructure for SDG 9. In: Open Access as a Knowledge Platform for Implementing the United Nations Sustainable Development Goals: Open Access and Sustainable Development Goals (Cham: Springer Nature Switzerland), pp. 253–281. DOI: 10.1007/978-3-031-99605-4_11.

[5]. Bachmann, N., Tripathi, S., Brunner, M., and Jodlbauer, H., 2022, The contribution of data-driven technologies in achieving the sustainable development goals. Sustainability, 14(5), 2497. DOI: 10.3390/su14052497.

[6]. Gunawan, W. B., 2025, Revisiting the sustainable development goal 4 "Quality Education": Insights, prospects, and recommendations. SAKAGURU: Journal of Pedagogy and Creative Teacher, 2(1), 12–36. https://journal.wiseedu.co.id/index.php/sakaguru/article/view/202.

[7]. Van Dijk, J., 2020, The Digital Divide (Hoboken, NJ: John Wiley & Sons). DOI: 10.1002/9781119444121.

[8]. Valdez, V. B., and Javier, S. P., 2021, Digital divide: From a peripheral to a core issue for all SDGs. In: Reduced Inequalities, edited by W. Leal Filho et al. (Cham: Springer International Publishing), pp. 88–101. DOI: 10.1007/978-3-030-57565-6_10.

[9]. Hargittai, E., 2001, Second-level digital divide: Mapping differences in people's online skills. Working paper, arXiv:cs/0109014. DOI: 10.48550/arXiv.cs/0109014.

[10]. Cave, M., 2022, Liberalizing network utilities: Economic principles and European regulatory experience. In: The Interaction of Competition Law and Sector Regulation, edited by P. Ibáñez Colomo and A. Lamadrid de Pablo (Oxford: Oxford University Press), pp. 17–34. DOI: 10.1093/oso/9780192864611.003.0002.

[11]. Partridge, H. L., 2007, Establishing the human perspective of the information society. Doctoral dissertation, Queensland University of Technology. DOI: 10.5204/thesis.eprints.16431.

[12]. Kuś, A., Kuflewska, W., and Trocewicz, A., 2025, European vision of a gigabit society: Evidence from Poland. Sustainability, 17(3), 1271. DOI: 10.3390/su17031271.

[13]. DiMaggio, P., Hargittai, E., Celeste, C., and Shafer, S., 2004, From unequal access to differentiated use: A literature review and agenda for research on digital inequality. Social Inequality, 1(1), 355–400. https://www.russellsage.org/research/outputs/unequal-access-differentiated-use-literature-review-and-agenda-research-digital.

[14]. Hacker, K. L., and van Dijk, J. (eds), 2000, Digital Democracy: Issues of Theory and Practice (London: Sage). DOI: 10.4135/9781446218846.

[15]. Van Dijk, J. A., 2013, A theory of the digital divide. In: The Digital Divide: Arguments for and Against, edited by J. A. van Dijk (London: Routledge), pp. 29–51. DOI: 10.4324/9780203074558-8.

[16]. Vulpe, M. I., Stancu, S., Munteanu, P., and Bărbulescu, R., 2026, Digital divide and technological exclusion: Strategies for inclusive ict skill development in adult education. International Journal of Education, Leadership, Artificial Intelligence, Computing, Business, Life Sciences, and Society, 5, 81–92. DOI: 10.65222/VIRAL.2026.2.12.32.

[17]. Ga, J., Bong, J., Yu, M., and Kwak, M., 2025, Digital enablers of sustainability: Insights from sustainable development goals (SDGs) research mapping. Sustainability, 17(15), 7031. DOI: 10.3390/su17157031.

[18]. Janowski, T., 2016, Implementing sustainable development goals with digital government–aspiration-capacity gap. Government Information Quarterly, 33(4), 603–613. DOI: 10.1016/j.giq.2016.12.001.

[19]. Ranchordás, S., 2022, Connected but still excluded? Digital exclusion beyond internet access. In: The Cambridge Handbook of Life Sciences, Information Technology and Human Rights, edited by M. B. Brömdal et al. (Cambridge: Cambridge University Press), pp. 244–258. DOI: 10.1017/9781108991200.021.

[20]. Picciotto, S., 2006, Regulatory networks and global governance. Working paper, University of London, Institute of Advanced Legal Studies. https://eprints.lancs.ac.uk/id/eprint/232/.

[21]. Budziewicz-Guźlecka, A., 2011, Przekształcenia polskiego rynku usług telekomunikacyjnych. In: Rynek usług telekomunikacyjnych, edited by H. Babis and K. Flaga-Gieruszyńska (Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego). https://sip.lex.pl/komentarze-i-publikacje/monografie/rynek-uslug-telekomunikacyjnych-369233876.

[22]. Budziewicz-Guźlecka, A., 2019, Oddziaływanie polityki społeczno-gospodarczej na zmiany polskiego rynku usług telekomunikacyjnych (Szczecin: Wydawnictwo Naukowe Uniwersytetu Szczecińskiego). https://wn.usz.edu.pl/sklep/nauki-spoleczne/ekonomia-i-finanse/oddzialywanie-polityki-spoleczno-gospodarczej-na-zmiany-polskiego-rynku-uslug-telekomunikacyjnych./

[23]. Moore, M. H., 2012, Recognizing public value: Developing a public value account and a public value scorecard. Working paper, John F. Kennedy School of Government, Harvard University. https://www.hks.harvard.edu/publications/recognizing-public-value.