SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 1.1, (2026), pp. 1641-1671
Open Access. Online & Print

DOI: 10.5281/zenodo.11425220

PUBLIC POLICIES OF DIGITAL LITERACY AND CYBER HYGIENE FOR RISK REDUCTION IN EDUCATION

Yamileth Arteaga-Alcívar[1], Javier Guaña-Moya[2*], Santiago Criollo-C[3], Raúl Guillermo Zambrano Pontón[4], Diego Cajamarca-Carrazco[5], Edwin Edison Quinatoa Arequipa[6]

[1]Unidad de Investigación y Generación del Conocimiento, Instituto Superior Universitario Japón, Quito 170120, Ecuador, Email: yarteaga@itsjapon.edu.ec, https://orcid.org/0000-0002-0675-0203
[2]Carrera Sistemas de Información, Facultad de Hábitat, Infraestructura y Creatividad, Pontificia Universidad Católica del Ecuador, Quito 170523, Ecuador, Email: eguana953@puce.edu.ec, https://orcid.org/0000-0003-4296-0299
[3]Carrera de Ingeniería en Ciberseguridad, Facultad de Ingeniería y Ciencias Aplicadas, Universidad de Las Américas, Quito 170125, Ecuador, Email: luis.criollo@udla.edu.ec, https://orcid.org/0000-0001-7212-5513
[4]Carrera de Comunicación, Facultad de Ciencias Políticas y Administrativas, Universidad Nacional de Chimborazo, Riobamba 060110, Ecuador, Email: gzambrano@unach.edu.ec, https://orcid.org/0000-0002-4009-2726
[5]Carrera de Electrónica y Automatización, Facultad de Informática y Electrónica, Escuela Superior Politécnica de Chimborazo, Riobamba 060155, Ecuador, Email: diego.cajamarca@espoch.edu.ec, https://orcid.org/0000-0001-6619-0490
[6]Departamento de Ciencias de la Computación, Carrera de Ingeniería de Software, Universidad de las Fuerzas Armadas ESPE, Latacunga 050105, Ecuador, Email: eequinatoa3@espe.edu.ec https://orcid.org/0000-0001-9701-7463

Received: 10/10/2025
Accepted: 10/11/2025

Corresponding Author: Javier Guaña-Moya (eguana953@puce.edu.ec)

ABSTRACT

This study presents the first multinational systematic review that jointly examines digital literacy and cybersecurity from the perspective of Sen's Capability Approach. Following the PRISMA 2020 protocol, sixty-one studies published between 2020 and 2024 in diverse contexts, such as Uganda, Kazakhstan, Estonia, Indonesia, Latin America, and Ecuador, were analyzed. The review examines how structural, pedagogical, and sociocultural factors affect the effectiveness of digital literacy and online safety policies in fostering equity and sustainability in education. Key findings include: Digital literacy is a multidimensional construct (technical, cognitive, socio-emotional, and ethical), whose effectiveness depends on enabling factors such as infrastructure, teacher preparation, gender, and regulatory frameworks; policies achieve greater impact when they combine investment in infrastructure, teacher training, community engagement, and monitoring systems, while approaches focused solely on access remain insufficient; Persistent barriers such as the gender digital divide, rural-urban inequalities, and limited curricular integration of cybersecurity continue to restrict the transformation of digital resources into real educational opportunities. By synthesizing evidence from underrepresented contexts and applying robust quality assessment tools (ROBINS-I, CASP, GRADE), this review provides a holistic and context-sensitive framework. This framework repositions digital literacy as a

capability-enhancing construct. It also offers practical guidance for policymakers seeking to design inclusive, safe, and sustainable education systems.

KEYWORDS: Digital Literacy; Cyber Hygiene; Educational Equity; Public Policy; Sustainable Development.

1. INTRODUCTION

1.1. Presentation of The Problem

Digital literacy is recognized as an essential competence in contemporary education, but its conceptualization and justification require more rigorous and situational analysis. While there is an international consensus on its importance for equity and social sustainability, the literature shows that the adoption and impact of digital literacy vary dramatically according to structural, socio-economic and cultural contexts, and that generalizations may hide deep inequalities (Ancheta-Arrabal et al., 2021; Wang & Si, 2024).

In this study, the term digital literacy is consistently understood as a construct encompassing four interrelated dimensions—technical, cognitive, socio-emotional, and ethical—thus preventing a reductionist view limited to access or instrumental skills.

For example, in Gulu (Uganda), only 10% of secondary schools have computers and reliable internet access, severely limiting learning opportunities. In this context, students with higher digital proficiency achieve academic averages of up to 78%, compared to 60% of those with limited access, a difference of 18 points directly attributable to digital literacy (Abiodun Nafiu et al., 2024). However, these data cannot be extrapolated without nuance to other contexts. The literature on the digital divide in Latin America emphasizes that access is only one dimension and that inequalities in use and quality, determined by factors such as gender, educational level, income and geographic location, are equally decisive (Ancheta-Arrabal et al., 2021).

In Central Asia, the integration of digital resources into primary education in Kazakhstan has shown improvements in reading comprehension and logical thinking, but inequalities persist due to lack of infrastructure, teacher training and adequate educational resources. In Indonesia, although 98.5% of students use the internet for educational purposes, only 82.7% feel competent to assess the quality of information, revealing that access does not guarantee critical or ethical skills in the use of technology (Wang & Si, 2024).

Digital literacy therefore involves much more than technical skills: it extends to cognitive, socio-emotional and ethical competences such as critical thinking, information assessment and responsible communication in digital environments. For example, in Estonia, despite a high awareness of cyber risks, 36% of the population admits not changing their passwords regularly, reflecting a persistent gap between knowledge and safe practice. Cyber hygiene campaigns and the integration of cybersecurity in school curricula have succeeded in reducing cyberattacks, but challenges remain in teacher training and institutional culture (Wang & Si, 2024).

In Latin America, the gender digital divide is a structural challenge. Although there has been progress in infrastructure, public policies lack a comprehensive approach that incorporates gender perspective into digital literacy. This limits the effective participation of women and girls in the digital economy and perpetuates educational and social inequalities. Research highlights the need for inclusive policies that integrate gender-sensitive teacher education and digital training programs tailored to the needs of girls and adult women, as well as the urgency of having gender-disaggregated data to design evidence-based policies (Ancheta-Arrabal et al., 2021).

On the other hand, the relationship between digital literacy and social sustainability remains under-explored in many contexts. While international agencies and recent studies highlight the role of digital literacy in achieving the Sustainable Development Goals (SDGs), especially SDG 4 on quality and inclusive education, the literature points out that access to technology alone is not enough to reduce inequalities or ensure educational justice (Ancheta-Arrabal et al., 2021; Wang & Si, 2024). Structural and cultural barriers as well as regulatory and pedagogical frameworks need to be addressed if digital literacy is to contribute effectively to educational equity and sustainability.

This study addresses a critical gap in the literature by conducting the first multinational systematic review that simultaneously explores digital literacy and cyber hygiene across diverse global contexts (Uganda, Kazakhstan, Estonia, Indonesia, Latin America), using an integrated analytical framework. Prior studies have focused on isolated regions or single-dimension interventions; this research proposes a holistic understanding of digital competencies as essential capabilities for educational sustainability and social inclusion, applying for the first time Sen's Capability Approach to this field (Sen, 1987).

1.1.1. Novelty and contribution of the approach

As the first systematic review to combine cyber hygiene and digital literacy through the lens of the Capability Approach and across multiple under-researched national contexts, this study offers an original contribution by systematically positioning cyber hygiene as an essential dimension within the broader framework of digital literacy. Unlike prior works that have largely focused on the development of technical skills and equitable access, this review expands the concept to encompass risk management,

ethical digital citizenship, and behavioral change as fundamental components of educational practice.

Using a rigorous systematic review methodology, including PRISMA, ROBINS-I, CASP, and GRADE, the analysis draws on evidence from multiple national contexts and identifies six critical factors shaping impact: infrastructure, teacher preparedness, gender-responsive pedagogy, policy coherence, socio-emotional learning, and monitoring frameworks. What sets this study apart is its comparative approach to diverse regulatory and educational ecosystems, its identification of persistent gaps in teacher training and policy adaptation, and its formulation of actionable, context-sensitive recommendations aimed at fostering sustainable digital education and cyber resilience (Eliza et al., 2024; Ugwu et al., 2022; Fikry et al., 2024).

To date, most academic discourse on digital literacy has remained narrowly centered on access and basic skills acquisition, often neglecting the equally vital area of digital security and risk management in educational environments. This research introduces and substantiates, both theoretically and empirically, the integration of cyber hygiene as a complementary and necessary pillar of digital literacy. Defined as the set of practices, habits, and behaviors that promote digital safety and resilience, cyber hygiene provides the tools to address emerging challenges such as hyperconnectivity, cyberbullying, disinformation, and the ethical management of digital identities (Fonseca & Borges-Tiago, 2024; Eliza et al., 2024; Ugwu et al., 2022).

By merging both technical and security-oriented perspectives, this study not only broadens the conceptual and practical scope of digital literacy but also responds directly to documented gaps in the literature. It underscores the pressing need for educational policies and curricular frameworks that prepare individuals for safe, critical, and ethically responsible engagement in contemporary digital society.

1.2. Critical Justification of The Selected Cases

The selection of contexts such as Uganda, Kazakhstan, Estonia, Indonesia, and Latin America responds to the study's aim to provide the first comparative, evidence-based synthesis of how digital literacy and cyber hygiene interact under diverse structural, cultural, and policy environments. These cases were intentionally chosen to illustrate the variety of challenges and approaches observed globally, while avoiding simplistic generalizations.

The analysis highlights how structural barriers (such as access and infrastructure), cultural dynamics (including gender stereotypes and social uses), and political frameworks (such as regulatory policies and teacher training systems) shape the effectiveness and equity of educational policies and practices in each context (Ancheta-Arrabal et al., 2021; Wang & Si, 2024; Abiodun Nafiu et al., 2024).

In Uganda, the digital infrastructure gap is stark: only 10% of secondary schools have connectivity and equipment, directly impacting academic performance and equity (Abiodun Nafiu et al., 2024). In Kazakhstan, the integration of digital resources in primary education has improved functional literacy, yet inequalities persist due to insufficient teacher training and lack of adapted resources (Abildina et al., 2024). Estonia represents an advanced model of curricular integration of cyber hygiene and digital literacy, with national campaigns and ongoing training for teachers and librarians, resulting in reduced cybersecurity incidents and improved public awareness (Kont, 2023b).

Indonesia exemplifies a case of high access but low critical competence: while 98.5% of students use the internet for learning, only 82.7% feel capable of evaluating information quality, and disciplinary and gender gaps remain (Eliza et al., 2024; Wang & Si, 2024). Latin America, meanwhile, demonstrates that the gender digital divide and urban-rural inequalities remain structural, limiting the impact of public policies and the participation of women and vulnerable groups in the digital economy (Ancheta-Arrabal et al., 2021).

These cases are not intended to establish direct equivalences, but to show how the interplay of structural (access, infrastructure), cultural (gender stereotypes, social uses), and political (regulatory frameworks, teacher training) barriers requires contextualized responses and highlights the need for differentiated, comprehensive, and adaptive policies.

1.3. Definition Of The Research Problem

Based on the critical review of the literature and the analysis of selected cases, this study addresses the following central research problem:

How do structural, pedagogical, and sociocultural factors affect the effectiveness of digital literacy and cyber hygiene in promoting educational equity and sustainability in diverse contexts, and how can the integration of cyber hygiene strengthen educational justice and digital citizenship?

This research builds on Sen's Capability Approach, which highlights that access to resources (such as digital technologies) does not automatically translate into real opportunities for individuals to achieve valued educational outcomes (Sen, 1987). The study therefore explores how contextual conversion factors—including gender, geographic

location, institutional policies, and teacher training—either enable or constrain the development of digital capabilities.

The aim is to provide a holistic and comparative evidence base to inform the design of inclusive, secure, and context-sensitive educational policies and curricula that advance digital equity and resilience.

1.4. Review Of The State Of The Art And Relevance Of The Topic

A key conceptual expansion emerges from the reconceptualization of digital literacy, evolving from a merely technical skillset to a holistic construct encompassing technological, cognitive, socio-emotional, and ethical dimensions (Herwani & Pasiningsih, 2023). In line with this broader vision, this study consistently understands digital literacy as a multidimensional competence integrating technical proficiency (use of digital tools), cognitive abilities (critical thinking and information evaluation), socio-emotional skills (self-regulation, collaboration, empathy), and ethical responsibility (safe and responsible digital practices). This explicit differentiation prevents reducing the concept to instrumental access and ensures a comprehensive analytical framework.

Herwani and Pasiningsih (2023) argue that digital literacy includes not only technical proficiency but also critical thinking, emotional regulation, and civic responsibility in digital environments. This broader vision is echoed in the literature, which highlights that digital literacy in education now prepares future generations to think critically, communicate, collaborate, and be creative in a globalized, technology-driven society (Hadi Pradana et al., 2024).

This study further builds on Sen's Capability Approach (Sen, 1987), which offers a powerful lens to analyze digital inclusion and educational equity. The Capability Approach emphasizes that access to resources, such as digital technologies, does not automatically translate into real freedoms or opportunities for individuals to achieve valued educational outcomes. Instead, a range of conversion factors—including teacher preparedness, gender, geographic location, and policy coherence—determines whether resources can be transformed into actual capabilities. By adopting this framework, this review uniquely examines how the interaction of digital literacy and cyber hygiene influences the development of digital capabilities across diverse educational systems.

Structural inequalities remain a central concern in digital inclusion, particularly regarding gender and socio-economic gaps. For example, empirical findings from Uganda reveal that while digital access is expanding, only a minority of students and teachers regularly use digital tools for educational purposes, and those with higher digital literacy achieve significantly better academic outcomes (Abiodun Nafiu et al., 2024). The study also demonstrates that lack of infrastructure, insufficient teacher training, and curriculum misalignment are persistent barriers, with teachers lacking ICT training nearly ten times more likely to struggle with digital integration (Abiodun Nafiu et al., 2024). These findings underscore that access alone does not guarantee the development of critical or ethical digital competencies.

Public policy responses vary widely across national contexts. In India, large-scale initiatives such as Digital India have increased awareness and access, yet ongoing deficits in rural data protection and teacher training persist (Raut et al., 2022). In Indonesia, there is an urgent need for comprehensive legislation and multisectoral cooperation to address threats such as ransomware and to ensure that digital literacy is embedded in educational policy (Anastasya & Kansil, 2024). Meanwhile, systematic reviews in Indonesia and other contexts emphasize that the successful implementation of digital literacy programs depends on teacher motivation, ongoing professional development, and the adaptation of curricula to local needs (Hadi Pradana et al., 2024).

Cyber hygiene practices, understood as preventive behaviors and protocols to protect digital data and systems, are increasingly viewed as core components of digital literacy. Institutional frameworks that combine technical controls with ongoing training are relevant in both educational and defense sectors, as they ensure that digital literacy is not only about access but also safe and responsible use (Mednikarov et al., 2023). Comparative studies show discipline-specific disparities, such as business students outperforming accounting students in password management, suggesting the need for differentiated pedagogical strategies (Abiodun Nafiu et al., 2024).

The literature identifies three persistent gaps: (1) insufficient curricular integration between digital literacy and cyber hygiene; (2) widespread teacher underqualification, with many teachers lacking cybersecurity training; and (3) sluggish adaptation of regulatory frameworks to emergent technologies and digital threats (Hadi Pradana et al., 2024; Mednikarov et al., 2023). These limitations highlight structural weaknesses in educational and legislative systems that must be addressed to build resilient digital citizens.

Several paradigm cases offer instructive models. Estonia's integration of cyber hygiene into national

school curricula and India's large-scale awareness campaigns exemplify context-sensitive policy success (Raut et al., 2022). In Bulgaria, practical training programs featuring ransomware simulation led to a measurable reduction in vulnerabilities among military personnel (Mednikarov et al., 2023). However, replicability in other regions requires equitable infrastructure and culturally adapted methodologies.

The relevance of these issues for educational sustainability is particularly evident in the context of the Sustainable Development Goals, especially SDG 4. Studies confirm that fostering critical and socio-emotional competencies improves not only academic performance (e.g., a +18-point difference in Uganda) but also students' resilience to digital threats (Abiodun Nafiu et al., 2024). In line with this, the literature advocates for embedding digital identity management and ethical awareness into public policy to strike a balance between innovation and human rights protection (Herwani & Pasiningsih, 2023).

The reviewed literature underscores the urgent need for integrative frameworks that combine inclusive public policies, critical pedagogies, and adaptive regulations. However, previous reviews have focused predominantly on regional or single-country analyses (Ancheta-Arrabal et al., 2021; Kont, 2023b). This study offers a novel contribution by providing the first comparative systematic review that integrates digital literacy and cyber hygiene under the Capability Approach across diverse international contexts. Drawing lessons from models such as Estonia and India, and confronting structural inequalities, are critical for building sustainable educational systems in digitally interconnected societies (Sogalrey et al., 2024; Hadi Pradana et al., 2024).

In summary, although global literature acknowledges the relevance of digital literacy for achieving SDG 4, most studies focus on infrastructure or individual competencies without addressing how institutional contexts convert resources into actual opportunities. This review positions Sen's Capability Approach as a foundational lens to reconceptualize digital inequality not merely as a lack of access, but as the deprivation of the substantive freedom to participate, learn, and flourish in digital societies. By foregrounding conversion factors such as gender, rurality, policy coherence, and teacher readiness, this study advances a deeper analytical framework that bridges digital literacy and educational justice.

1.5. Research Questions

This study seeks to answer the following research questions, formulated on the basis of the identified gaps in literature and the theoretical framework of the Capability Approach:

1. Structural And Sociocultural Factors

What structural elements (such as infrastructure, public policies, and teacher training) and sociocultural factors (including gender, geographic location, and socioeconomic status) determine the effectiveness of digital literacy and cyber hygiene in vulnerable contexts?

2. Pedagogical Strategies and Competencies

Which pedagogical approaches and instructional strategies demonstrate the greatest impact on the development of critical digital competencies—such as information evaluation, cyber hygiene, and ethical digital behavior—across diverse educational environments?

3. Policy Integration and Equity

How can public policies effectively integrate digital literacy and cyber hygiene to reduce gender and socioeconomic gaps, ensuring educational equity, sustainability, and the development of real capabilities as conceptualized by Sen's framework?

These questions are designed not only to guide the systematic review but also to bridge theoretical constructions with empirical evidence, ensuring that digital literacy is analyzed as more than a matter of access. They emphasize the conditions under which resources can be converted into genuine opportunities for learners to participate, thrive, and achieve valued educational outcomes in digitally mediated societies.

1.6. Justification For The Use of PRISMA

This study adopts the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol to ensure methodological rigor, transparency, and reproducibility in the review process. The choice of PRISMA is justified by its widespread use and proven effectiveness in synthesizing complex research, originally in health sciences but increasingly applied to the field of education, particularly in reviews that examine digital literacy, technological integration, and policy impacts. Its structured reporting guidelines make it especially suitable for addressing multifactorial problems that involve both pedagogical and socio-technical dimensions.

PRISMA facilitates systematic identification, selection, and synthesis of evidence, reducing bias and strengthening the reliability of findings. In this study, it was essential for organizing the large body of literature on digital literacy and cyber hygiene,

which spans diverse contexts, populations, and methodological approaches. By following PRISMA, the review process was able to guarantee transparency in inclusion and exclusion criteria, consistency in data extraction, and comparability across studies, all of which are necessary for building an evidence base that can inform educational policies.

This systematic review was driven by the central research question: How do structural, pedagogical, and sociocultural factors affect the effectiveness of digital literacy in promoting equity and educational sustainability in varied settings, and how can the integration of cyber hygiene strengthen educational justice and digital citizenship? The adoption of the PRISMA 2020 protocol (Page et al., 2021) ensured methodological consistency, analytical rigor, and full reproducibility throughout the review process.

2. METHODS

This systematic review was conducted under the PRISMA 2020 protocol (Page et al., 2021), ensuring transparency, rigor, and reproducibility in the identification, selection, and synthesis of evidence on digital literacy, cyber hygiene, and public policy in educational contexts. The methodology was designed to directly address the research questions on the educational impact of digital literacy and the effectiveness of public policies for digital inclusion and online safety.

2.1. Inclusion And Exclusion Criteria

The inclusion and exclusion criteria were structured using the PICO framework, aligning the selection process with the study's objectives and ensuring consistency throughout.

The population of interest included students, teachers, and educational communities in vulnerable contexts (rural areas, socioeconomically disadvantaged groups, and regions with limited technological access). This focus was key to examining how structural and sociocultural factors condition educational outcomes.

Interventions included public policies, educational programs, and institutional strategies aimed at strengthening digital literacy, cyber hygiene, and online safety. Comparative studies contrasting regions (urban vs. rural) or approaches (infrastructure vs. teacher training) were prioritized, as these highlight structural conversion factors central to Sen's Capability Approach (Sen, 1987).

Outcomes selected were improvements in academic performance, narrowing of digital divides, enhancement of critical digital skills, and mitigation of cyber risks such as cyberbullying or online fraud.

The time frame was limited to 2020–2024, a period marked by pandemic-driven transformations in digital education and the rise of technologies such as AI and IoT.

Studies were included if published in English or Spanish, with exceptions for Ukrainian, Russian, and Indonesian when they offered distinctive contextual evidence.

Exclusion criteria covered non-peer-reviewed works, corporate-only contexts, opinion pieces, abstracts without full texts, and studies lacking measurable educational or cybersecurity outcomes. This safeguarded the quality and relevance of the sample.

2.2. Data Source

Searches were conducted across SCOPUS, Web of Science, Dimensions.ai, and Google Scholar to ensure comprehensiveness:

- SCOPUS for multidisciplinary peer-reviewed coverage, including non-Western perspectives.
- Web of Science for high-impact policy and educational technology literature.
- Dimensions.ai for emerging research, preprints, and regional studies are often absent in traditional indexes.
- Google Scholar for supplementary access to institutional reports and open-access studies, particularly from Latin America, Africa, and Asia.

This multi-source strategy allowed the review to capture both global frameworks and local case studies, in line with the Capability Approach, which emphasizes how structural and institutional contexts shape real opportunities for digital participation.

2.3. Search Strategy

Systematic research was conducted between June and November 2024. Boolean operators were applied to refine retrieval:

- SCOPUS / Dimensions.ai: "digital literacy" AND "cyber hygiene" AND "education" AND "policy" AND "sustainable".
- Web of Science: "cyber hygiene" AND "policy" AND "education".
- Google Scholar: "public policies" AND "digital literacy" AND "cyber hygiene" AND "education" AND "sustainable".

Reference lists of included studies were also manually reviewed. Full search strings, with filters and adaptations, are provided in Appendix A for reproducibility.

This combined strategy captured both high-impact and context-specific research, aligning with Sen's framework by including underrepresented contexts where conversion factors (infrastructure, teacher training, gender) condition outcomes.

2.4. Selection Process

The selection process for this systematic review was conducted in three stages, following the PRISMA 2020 guidelines (Page et al., 2021), to ensure both thematic relevance and methodological rigor.

- Identification: A total of 996 records were retrieved from SCOPUS, Web of Science, Dimensions.ai, and Google Scholar. After removing 50 duplicates, 946 unique studies were retained for screening.
- Screening: Titles and abstracts of these 946 records were reviewed. A total of 800 studies were excluded: 497 (62%) due to thematic irrelevance (e.g., corporate cybersecurity, general ICT without educational relevance, or medical informatics); 265 (28%) for lacking empirical foundation (e.g., commentaries, essays without data, abstracts without results); and 88 (10%) due to inaccessibility despite attempts through institutional subscriptions and author contact.
- Eligibility: Of 146 full-text articles assessed, 20 could not be retrieved. Among the 126 accessible studies, 71 were excluded: 40 for not aligning with the central focus on the intersection between digital literacy, cybersecurity/online safety, and educational outcomes or policy interventions; 20 for insufficient methodological quality; and 11 due to persistent inaccessibility.

The final sample comprised 61 studies meeting both thematic and methodological criteria. For quality control, all studies were assessed using ROBINS-I for non-randomized quantitative designs (Sterne et al., 2016), the CASP checklist for qualitative studies (CASP, 2020), and GRADE for systematic reviews and observational research (Guyatt et al., 2011). Studies below the thresholds (≥4/6 ROBINS-I, ≥70% CASP, or moderate certainty in GRADE) were excluded, unless justified by exceptional contextual relevance in underrepresented settings such as rural Sub-Saharan Africa or Central Asia.

Additionally, the Capability Approach (Sen, 1987) informed the inclusion logic by emphasizing not only the presence of digital tools or policies, but also whether structural and sociocultural conditions (e.g., gender, territorial disparity, institutional resources, pedagogical autonomy) enabled the transformation of those resources into real educational capabilities.

This selection process reinforced the review's commitment to contextual depth, methodological transparency, and theoretical coherence, ultimately contributing to a more inclusive understanding of how digital literacy and cyber hygiene affect educational equity and sustainability across varied contexts.

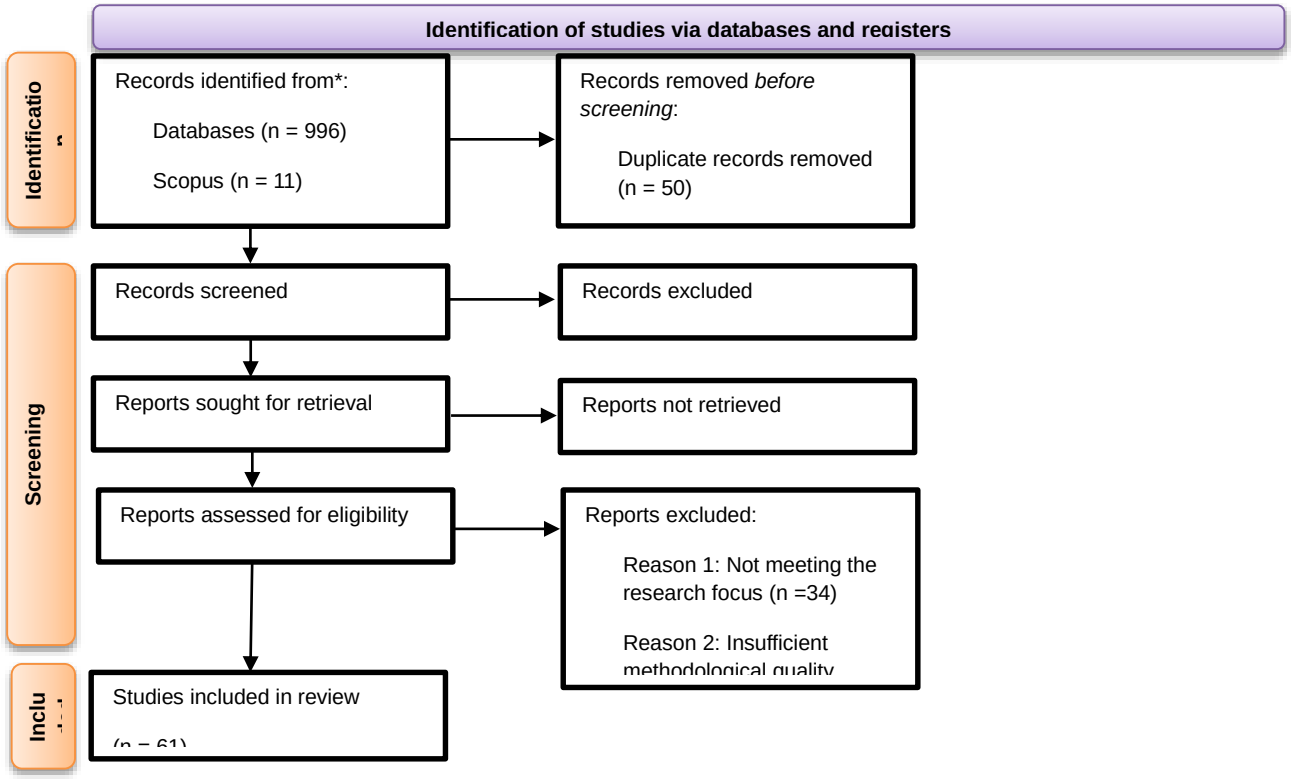

Figure 1: PRISMA 2020 Flow Diagram Showing Study Identification, Screening, Eligibility, And Inclusion (N = 61).

2.5. Data Extraction

For each study, data were collected on authorship, year, country, objectives, methodology, sample characteristics, key findings, and policy relevance. To facilitate comparative analysis, studies were grouped by intervention type (infrastructure, pedagogy, cyber hygiene) and by region.

To ensure methodological rigor and comparability, three internationally validated quality assessment tools were employed according to study design:

- ROBINS-I for non-randomized quantitative studies (Sterne et al., 2016). Studies were required to score at least ≥4/6 across bias domains such as confounding, participant selection, deviations from intended interventions, and outcome measurement.
- CASP Qualitative Checklist for qualitative research (CASP, 2020), with a minimum compliance threshold of 70 % to guarantee design clarity, ethical integrity, and analytical transparency.
- GRADE for systematic reviews and observational studies (Guyatt et al., 2011), evaluating risk of bias, inconsistency, indirectness, imprecision, and publication bias. Studies rated as low or very low certainty were excluded unless justified by exceptional contextual relevance.

The data extraction process was conceptually guided by Sen's Capability Approach (Sen, 1987). This framework emphasizes that access to digital technologies and learning resources alone does not guarantee real educational opportunities. The actualization of digital literacy and cyber hygiene as meaningful outcomes depends on conversion factors such as gender, teacher training, institutional infrastructure, and regulatory environments, which determine whether individuals can transform resources into real capabilities.

This conceptual framing enhanced the analytical coherence of the synthesis by stressing those public interventions, beyond providing access, must enable individuals to convert digital resources into meaningful learning achievements. It was particularly valuable for comparative policy evaluation, as it highlighted how contextual barriers—such as teacher underqualification or gendered digital norms—limit the real effectiveness of digital inclusion strategies.

2.6. Quality Assessment

To ensure the methodological soundness of the 61 studies included in this review, three internationally validated tools were applied according to study design:

- ROBINS-I for non-randomized quantitative studies (Sterne et al., 2016), assessing bias across six domains (confounding, participant selection, deviations from intended interventions, outcome measurement, etc.). Studies with "low" or "moderate" risk in at least four domains were included, following standards from previous reviews in educational technology.
- CASP Qualitative Checklist for qualitative research (CASP, 2020), focuses on design clarity, ethical integrity, recruitment strategy, data collection and analysis, and the transparency and value of results. A minimum of 70% compliance (14/20 points) was required for inclusion.
- GRADE for systematic reviews and observational studies (Guyatt et al., 2011), evaluating risk of bias, inconsistency, indirectness, imprecision, and publication bias. Studies with overall low or very low certainty were excluded unless offset by compelling contextual value.

Figure 2 provides a visual synthesis of the included studies, organized by bias tool, year, source database, and study type. The figure highlights the growing methodological variety of recent contributions (2020–2024), predominantly sourced from Dimensions.ai and SCOPUS.

Approximately 20% of the studies could not be classified under ROBINS-I, CASP, or GRADE due to their design. Examples include:

- Conceptual frameworks without empirical data (Skarga-Bandurova et al., 2021; Tello de la Torre et al., 2021).
- Structural modeling lacks sufficient reporting for ROBINS-I (Senarak, 2021).
- Use of aggregated national statistics without individual-level data (Azizbayov, 2024).
- Cross-national panel data modeling, statistically robust but not aligned with GRADE assumptions (Meiqi et al., 2024).
- Macro-level policy analyses focusing on structural risk profiling rather than intervention outcomes (Tokan et al., 2024; Căciulescu et al., 2024).

The presence of these unclassified studies reflects the limitations of existing evaluation instruments when applied to interdisciplinary research on digital literacy and cybersecurity. Their inclusion underscores the need to expand or adapt current bias-assessment frameworks to accommodate policy reviews, conceptual innovations, and large-scale modeling approaches.

This classification not only illustrates the methodological rigor of the review but also reveals the epistemological diversity of the literature. It affirms the importance of interdisciplinary approaches and the necessity of inclusive evaluative tools in advancing equitable and secure digital education systems

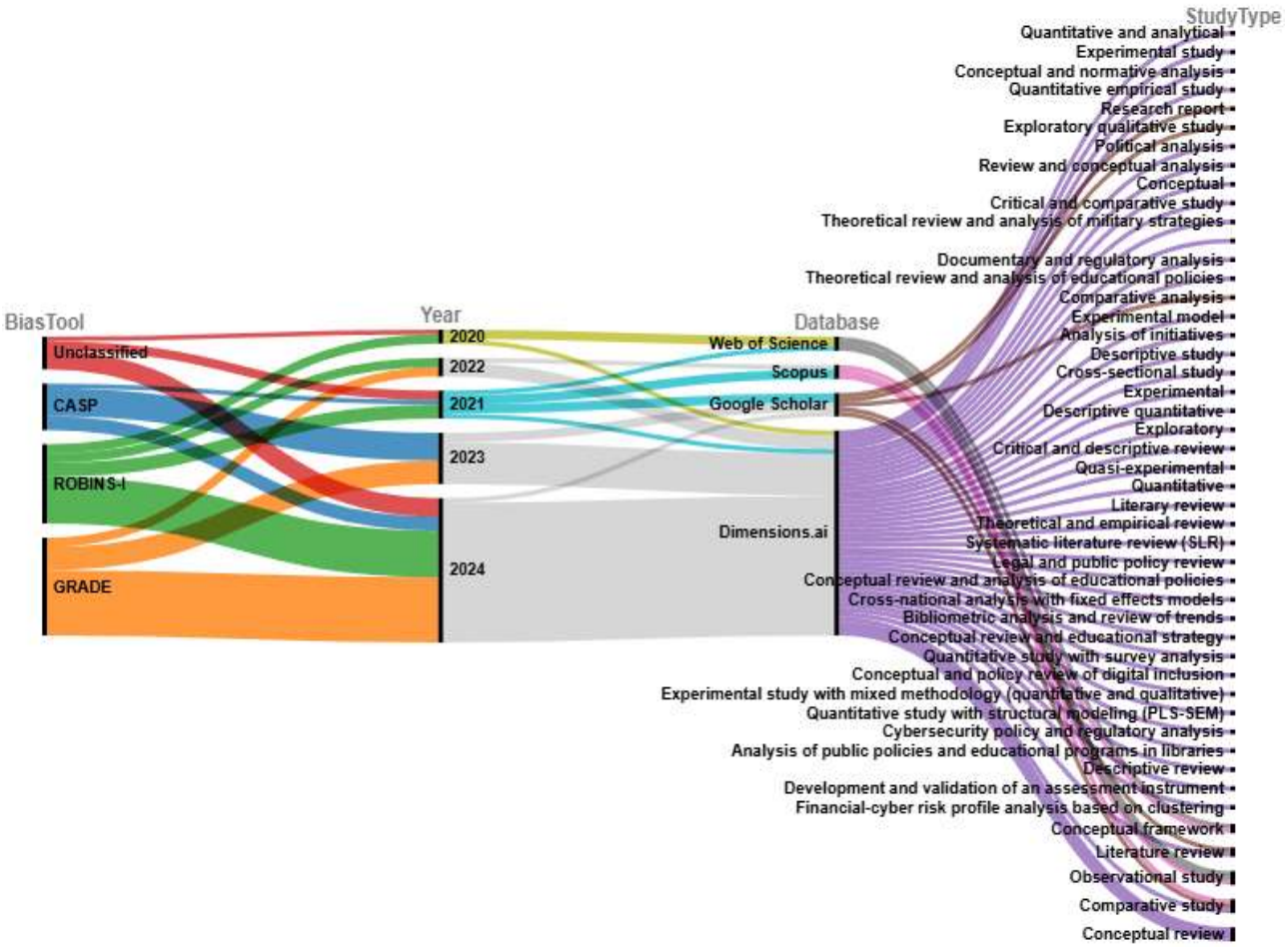

Figure 2: Distribution of The 61 Included Studies By Study Type, Year Of Publication, Source Database, And Quality Assessment Tool (ROBINS-I, CASP, GRADE), Visualized Through An Alluvial Diagram Created With Rawgraphs 2.0 (Https://App.Rawgraphs.Io/; Accessed May 1, 2025).

2.7. Limitations

This review acknowledges limitations. Restricting the time frame (2020–2024) and languages (English and Spanish, with few exceptions) may have excluded relevant perspectives. The exclusion of grey literature, while improving methodological rigor, may have reduced context-specific insights, particularly in low- and middle-income countries. The heterogeneity of study designs prevented meta-analysis and required narrative synthesis. Finally, the lack of granular subnational data limited deeper territorial comparisons (e.g., rural vs. urban in India or Latin America).

3. RESULTS

3.1. Structural And Sociocultural Factors In Educational Cybersecurity

3.1.1. Structural Frameworks and Maturity Models in Cyber Hygiene

The study by (Skarga-Bandurova et al., 2021) introduces the Cyber Hygiene Maturity Assessment Framework (CHMF), a three-dimensional model comprising infrastructure, organization, and personnel, designed to assess the maturity of cyber hygiene practices in critical sectors such as smart electrical grids. Their findings reveal substantial deficiencies: only 34 % of organizations in Eastern Europe reached advanced levels of cybersecurity infrastructure, largely due to outdated IoT firmware; additionally, 58 % lacked documented password management policies, increasing their vulnerability to ransomware attacks. The authors advocate for the adoption of the Plan-Do-Check-Act (PDCA) methodology as a standardized evaluative model to improve methodological consistency in

cybersecurity assessments. These results emphasize the need for formalized protocols and targeted workforce training, particularly in infrastructure-dependent sectors like energy and telecommunications.

Building on this institutional perspective, (Azizbayov, 2024) analyzes cyber hygiene practices within Azerbaijan's public administration. His study underscores the role of regulatory frameworks, specifically the Cybersecurity Law (2018) and Personal Data Protection Law (2019), in promoting compliance with ISO 27001 and GDPR standards. Notably, 62 % of Azerbaijani institutions reported improved incident response times following the implementation of structured cyber hygiene protocols. These findings support prior assertions by (Szczepaniuk & Szczepaniuk, 2022) on the critical importance of procedural rigor and regular audits, illustrating how legal backing can significantly enhance institutional resilience when aligned with international benchmarks.

In a different domain, (Senarak, 2021) examines port cybersecurity in Thailand, identifying three pillars: human, procedural, and technological. His research reveals that 74 % of port employees lacked anti-phishing training, while the implementation of ISO 27001 protocols led to a 65 % reduction in unauthorized access. Although these results are sector-specific, their implications are transferable to educational institutions facing similar challenges in data protection and identity spoofing, further reinforcing the argument for cross-sectoral adoption of maturity models.

From the West African context, (Ugwu et al., 2022) emphasize the role of human behavior in cybersecurity resilience. Based on a survey conducted in Nigeria, 86 % of respondents admitted to risky behaviors such as password reuse and outdated software usage. Despite awareness of cyber threats, behavior change remained insufficient, suggesting that technical safeguards must be complemented by sustained digital education. This aligns with (Mednikarov et al., 2023), whose ransomware simulation program in Bulgarian military and educational settings led to a 40 % reduction in vulnerabilities and a 65 % increase in phishing detection among pedagogy students. Their findings validate the effectiveness of experiential, simulation-based training over theoretical instruction alone.

Further supporting this pedagogical dimension, (Abildina et al., 2024) present evidence from Kazakhstan on the value of early cyber hygiene education. Their experimental study in primary schools showed that the integration of interactive platforms such as Kahoot and Exam.net resulted in a 30 % improvement in students' functional literacy. The intervention emphasized interdisciplinary learning in reading, mathematics, science, and information literacy through targeted digital activities and formative assessment. These results suggest that early-stage digital fluency is essential for long-term cybersecurity awareness and should be embedded within national education strategies.

A policy-oriented view is provided by (Ananin & Uvarkina, 2023), who analyze Ukraine's cyber education reforms in the aftermath of the 2022 geopolitical crisis. Through NATO-aligned initiatives like the Defense Education Enhancement Program (DEEP), cyber hygiene has become a central element of military curricula. This reinforces (Senarak, 2021) emphasis on procedural safeguards and (Szczepaniuk & Szczepaniuk, 2022) call for harmonized international standards, highlighting the role of political commitment and curriculum standardization in national cyber resilience.

Synthesizing these perspectives, (Szczepaniuk & Szczepaniuk, 2022) argue that achieving cyber hygiene maturity requires more than technological upgrades; it depends on a triad of safeguards: robust technical controls, institutionalized processes, and sustained human development. This conclusion is echoed in the successes observed in Azerbaijan's policy framework, Ukraine's military integration, and Kazakhstan's primary education initiatives.

In summary, effective cyber hygiene frameworks must combine technical mechanisms (such as IoT firmware updates), procedural systems (e.g., ISO 27001 compliance), and human-centered strategies (like anti-phishing training and foundational digital literacy programs). Case studies from Azerbaijan, Nigeria, Ukraine, and Kazakhstan demonstrate that national policy, legal structures, and educational reform are equally critical to building organizational and societal cyber resilience. Crucially, the development of digital maturity should begin at the earliest levels of formal education, ensuring that cybersecurity becomes a foundational competency of 21st-century learners.

3.1.2. Gender Gaps and Access in Vulnerable Contexts

The systematic review by (Ancheta-Arrabal et al., 2021) reveals a persistent digital gender divide across rural areas in Latin America. In Mexico and Colombia, only 35% of rural women have access to broadband, compared to 68% in urban settings. Although targeted programs have managed to improve girls' retention in STEM fields by 22%, implementation remains limited, reaching just 18% of schools. Moreover, the review notes that local realities are often overlooked, as non-peer-reviewed

sources such as government data and community reports are frequently excluded from formal analyses.

Similar challenges are observed in Uganda. (Abiodun Nafiu et al., 2024) demonstrate that students in digitally connected schools outperform their peers in mathematics by 18 points. Yet only 10% of rural schools have stable internet access. Notably, women in these communities are 50% less likely to engage with digital tools, even when devices are available. Cultural expectations, limited teacher training, and gendered norms continue to shape the unequal use of technology in educational spaces.

In Pakistan, (Naseer et al., 2023) point to a lack of Media and Information Literacy (MIL) in national education policies as a key factor perpetuating these disparities. Their analysis of frameworks from 1998 to 2020 reveals minimal integration of digital literacy, particularly in rural and conservative regions where cultural restrictions and limited infrastructure converge. While urban women may access informal training opportunities, rural women are often left without the institutional or technological support needed to acquire basic digital competencies. Without a strategic push to embed MIL into education policies, gender-based exclusion from the digital sphere is likely to persist.

Expanding the conversation to post-conflict environments, (Malik et al., 2023) study digital literacy initiatives in rural Afghanistan. They report a 40% increase in entrepreneurial activity among women participating in mobile-based learning programs. These initiatives have the potential to challenge restrictive gender roles. However, limited electricity, device availability, and connectivity still pose significant obstacles. Only 15% of rural women were able to maintain long-term engagement in these training programs, highlighting the infrastructural fragility that undermines progress.

The risks of digital exclusion extend beyond missed opportunities. (Septanto et al., 2024) emphasize how low digital literacy leaves rural women in Indonesia more exposed to online radicalization and cybercrime. Women with limited digital skills are three times more likely to encounter malicious content. Their findings call for digital literacy programs that are not only accessible but also include cybersecurity education to ensure both inclusion and protection.

Addressing these barriers requires more than infrastructure. (Herwani & Pasiningsih, 2023) document the success of community-led digital hubs in rural Java. Designed with flexible schedules and culturally appropriate content, these centers increased women's digital literacy by 35% within a year. Critical to their success were mentorship programs that paired urban technology professionals with rural learners and the use of local languages in digital training modules. This model demonstrates how localized, participatory approaches can bridge access gaps more effectively than one-size-fits-all solutions.

Across these cases, several cross-cutting insights emerge. First, successful digital inclusion strategies must combine infrastructure investment with cultural adaptation. (Malik et al., 2023) mobile learning programs and (Herwani & Pasiningsih, 2023) community hubs exemplify this dual approach. Second, cybersecurity must be integrated into digital literacy curricula, particularly for vulnerable populations, as highlighted by (Septanto et al., 2024). Third, data disaggregated by gender, including device ownership, internet usage, and digital skills, is essential to design responsive policies, as emphasized by (Naseer et al., 2023).

Based on these insights, targeted interventions are recommended. Subsidized device distribution programs for rural women, modeled after Indonesia's hubs, can address access. Comprehensive teacher training in gender-responsive digital pedagogy is also vital to overcome persistent sociocultural barriers. Finally, national MIL strategies should incorporate specific quotas for women's participation in STEM and digital policymaking to ensure long-term equity.

In sum, closing the gender digital divide requires coordinated action across education, infrastructure, and culture. Each of these elements must be addressed simultaneously to create inclusive digital ecosystems where women and girls are not only connected but empowered.

3.1.3. Disciplinary Differences and Formal Pedagogy

The study by (Eliza et al., 2024) in Indonesia reveals critical disciplinary disparities in cyber hygiene practices. While 74 % of business administration students managed passwords appropriately, only 40 % of accounting students exhibited similar behavior. Phishing simulations reduced vulnerability by 45 %, yet only 32 % of universities had adopted these practical tools. VOSviewer mapping further exposed curricular gaps in core areas like security configuration and data backup protocols, underscoring a disconnection between theoretical instruction and applied cybersecurity training.

(Tokan et al., 2024) expand on this by examining regulatory shortcomings across Southeast Asia, where 58 % of educational institutions lacked password management policies and just 34 % of rural teachers applied basic digital safety protocols like

HTTPS. These findings expose systemic weaknesses, especially in non-technical disciplines, and the urgent need for educational reforms that align with legal and cybersecurity standards.

(Raut et al., 2022), in the context of the Digital India initiative, highlight a similar urban-rural divide. In rural settings, only 34 % of trained teachers applied basic safety measures, versus 68 % in urban areas. Particularly in humanities programs, 62 % lacked modules on fraud prevention or password security. These gaps compromise the broader goal of digital resilience and reflect a lack of curricular coherence across disciplines and territories.

A psychosocial approach is proposed by (Madanu et al., 2024), whose service-learning program improved cyberpsychology literacy by 45 % and showed that students in social sciences practiced safer behaviors 30 % more than their technical counterparts. This suggests that digital resilience also requires socio-emotional strategies such as empathy and screen-time regulation, which are often missing in standard curricula.

In Albania, (Basholli et al., 2023) found that 70 % of teachers lacked formal cybersecurity training. Although GDPR implementation led to a 30 % rise in incident reporting, 41 % of institutions had no formal response protocols. These findings echo (Raut et al., 2022), demonstrating that normative advances often fail to translate into effective institutional practice.

In Ecuador, official frameworks like the Agenda de Transformación Digital 2022–2025 and the Estrategia Nacional de Ciberseguridad propose integrating digital competencies in education. However, the absence of cybersecurity law and the lack of curricular mandates in humanities and rural education hinder progress. The latest ENC data (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022) confirms that teachers in rural areas report significantly lower confidence in addressing digital risks, which reflects a deeper gap in formal pedagogical training.

These institutional gaps are further illuminated by (Ilbay Guaña, 2022), who highlights the need to adapt media literacy strategies to intercultural and vulnerable populations. Her review underscores that integrating critical and ethical literacy into the school curriculum, particularly for older adults, persons with disabilities, and rural learners—remains a pending challenge. In the same line, (Chancusig Ruiz, 2023) stresses the importance of digital tools like podcasts to foster analytical thinking and verification skills, revealing that inclusive and participatory media strategies significantly improve learners' interpretative abilities.

In higher education, (Pérez García et al., 2025) identify persistent tensions between policy discourse and teaching practice in Ecuadorian teacher education programs. Their findings show that while ICT-related policies exist, they are not systematically aligned with pedagogical training, leading to fragmented implementation and low impact on classroom innovation.

(Guana Moya et al., 2022) contribute further by revealing that although Ecuador's digital transformation has expanded infrastructure, its educational integration remains uneven. Their analysis points to a disconnect between technological availability and pedagogical adaptation, especially in humanities programs. A follow-up study by (Guaña Moya et al., 2022) reinforces this, emphasizing that national educational policies still fail to incorporate digital citizenship frameworks systematically, particularly in underserved institutions.

Finally, (Guaña-Moya et al., 2024) argue that the development of academic responsibility in digital environments requires not only policy but also context-sensitive pedagogical mediation. They advocate for teacher training models that integrate digital ethics, critical autonomy, and social inclusion to effectively nurture digital citizenship.

From a capability-oriented perspective (Sen, 1987), these cases show that access to technology is insufficient if not supported by curricular design and pedagogical models that allow individuals to develop the real freedom to act safely and critically in digital environments. The lack of disciplinary standardization constrains students' capabilities, particularly in non-STEM fields and underserved regions.

In summary, this review contributes to the field by illuminating how disciplinary silos, pedagogical inertia, and uneven regulatory uptake hinder the integration of cyber hygiene into education systems. The novelty lies in exposing how technical and socio-emotional competencies must converge to build sustainable digital citizenship. By highlighting both systemic gaps and promising interventions across varied national contexts, this subsection underscores the need for inclusive, capability-enhancing curricular reform

3.1.4. Integrated Strategies for Advancing Digital Literacy and Cybersecurity Policy.

(Baxto, 2024) offers an in-depth evaluation of Brazil's digital access policies in higher education. Despite high national connectivity rates, significant inequalities persist only 8.6 % of remote education enrollments between 2011 and 2021 occurred in public institutions, and 35 % of rural schools lacked stable broadband. Initiatives such as Reuni Digital and the Open University of Brazil (UaB) increased total enrollments by 474 % yet failed to bridge

structural gaps. The study identifies weak digital governance, insufficient inter-institutional coordination, and teacher training deficits as the main barriers. Proposed solutions include sustained infrastructure investment and the development of integrated digital governance strategies.

In the European Union, (Căciulescu et al., 2024) explore the link between financial literacy and cybersecurity practices. They find that individuals with higher financial literacy are significantly more likely to use protective measures such as multifactor authentication. However, 41 % of financial institutions lack comprehensive incident response protocols, and only 36 % of users regularly update their passwords. These gaps, even in advanced systems, underscore the need for regulatory frameworks that not only legislate but also promote behavioral change.

In India, (Behera & Deb, 2023) argue that digital literacy must go beyond technical skills to include critical thinking, ethical awareness, and socio-emotional competencies. Their analysis reveals that current curricula often fail to prepare students to handle cyberbullying, misinformation, and online risks. They recommend embedding digital citizenship principles across disciplines and educational levels.

Similarly, (Antunes et al., 2021) present an integrated cyber awareness strategy for Portuguese schools, based on diagnostic assessments, gamified lesson plans, and community engagement. Their research shows that older students tend to underestimate online risks, highlighting the need for continuous, age-sensitive interventions adapted to sociocultural realities.

In Ecuador, initiatives such as the Digital Transformation Agenda 2022–2025 and the National Cybersecurity Strategy 2022–2025 outline strategic goals for improving digital access, governance, and educational quality. However, the absence of a binding cybersecurity law and the lack of mandatory curricular guidelines for cyber hygiene limit effective implementation. The national strategy itself identifies education as one of the "critical sectors" with unresolved vulnerabilities (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022). Furthermore, poor coordination between national and local levels hinders scalability, especially in rural provinces, where many digital literacy programs depend on short-term donor-driven projects.

From the perspective of (Sen, 1987), these cases show that access to digital infrastructure is not sufficient. What truly determines meaningful participation is how public policies transform resources into real freedoms through regulatory coherence, teacher training, pedagogical design, and cultural adaptation. Where these elements are misaligned as is partially the case in Ecuador, Brazil, and certain EU countries digital strategies tend to reproduce existing inequalities rather than reduce them.

In conclusion, this review identifies that truly transformative strategies are those that integrate digital literacy, cybersecurity, and socio-emotional learning within holistic and context-sensitive policy frameworks. The novelty of this study lies in demonstrating how different countries operate this integration often inconsistently and how the combination of regulatory structure, pedagogical design, and community participation determines the long-term sustainability of digital inclusion. Beyond technological advancement, the focus must shift toward building capability-enhancing educational ecosystems that allow individuals to learn, protect themselves, and thrive in complex digital environments.

3.1.5. Implications For Educational Policies

To begin with, integrating frameworks such as the Cyber Hygiene Maturity Framework (CHMF) and ISO 27001 can play a crucial role in reducing technical vulnerabilities in educational environments. However, policy initiatives must extend beyond infrastructure by incorporating teacher training through practical simulations, as suggested by (Eliza et al., 2024), and embracing gender-inclusive approaches, as highlighted by (Ancheta-Arrabal et al., 2021). This is particularly critical in regions like Latin America and Sub-Saharan Africa, where poverty, gender inequality, and limited access to digital resources intersect to deepen existing educational gaps.

In support of this, (Kozyreva et al., 2022) note that in Russia, digital literacy and cyber hygiene are still not systematically embedded in the national curriculum. This disproportionately affects vulnerable groups such as the elderly and rural populations, who remain exposed to cyber threats. The authors advocate for embedding digital literacy, legal awareness, and information evaluation at all educational levels, alongside aligning national policies with international standards such as the EU's eIDAS regulation and the UK Digital Strategy.

Further illustrating the implementation gap, (Anastasya & Kansil, 2024) examine the Indonesian context, where despite the existence of key legal instruments like the Personal Data Protection Law and the Electronic Information and Transactions Law (UU ITE), enforcement remains inconsistent. Recent ransomware attacks on national data centers have exposed the fragility of the country's digital

infrastructure. The authors emphasize the urgency of inter-agency coordination, legal reform, and large-scale cybersecurity literacy campaigns to build a more resilient and informed digital society.

In the South African context, (Kritzinger, 2020) identifies severe shortcomings in cybersafety practices across 24 schools evaluated using the 360safe maturity tool. Areas such as staff training, parental involvement, and online safety education all scored above 4 on a 5-point non-compliance scale. In response, (Kritzinger, 2020) proposes a ten-phase model that begins with institutional self-assessment and concludes with post-evaluation. Her model highlights the importance of addressing not only technical dimensions but also behavioral and community-level factors.

Building on the need for localized capacity-building, (Omojemite & Cishe, 2024) demonstrate the effectiveness of cooperative learning strategies in cybersecurity training for pre-service teachers in Nigeria. Their quasi-experimental study shows that group-based simulations on ransomware led to a 40% reduction in vulnerabilities and a 65% improvement in phishing detection. The authors argue that collaborative, structured training enhances not only technical abilities but also encourages proactive attitudes. These results support integrating cooperative learning into national teacher certification systems, in line with ISO 27001's emphasis on continuous professional development.

Expanding this policy discussion, (Asimiyu, 2024) examines cyber resilience strategies for critical infrastructure in Nigeria. While the Cybercrimes Act (2015) establishes legal parameters, enforcement is weak in rural zones. (Asimiyu, 2024) calls for sector-specific policies modeled after the EU's NIS Directive and proposes subsidized training initiatives to address the 70% gap in teacher cybersecurity preparedness across Sub-Saharan Africa. Her work reinforces the importance of public-private collaboration and tailored workforce development strategies in regions with fragmented regulatory enforcement.

In contrast, (Kont, 2023b) presents Estonia as a model for early cybersecurity education and community-based outreach. National awareness campaigns and workshops hosted by public libraries have led to a 45% reduction in risky online behavior among rural populations. Estonia's national curriculum integrates cybersecurity from the primary school level, and tools such as the Cyber Hygiene Maturity Assessment Framework are used to evaluate librarian preparedness. (Kont, 2023b) reports that 62% of Estonian librarians received cybersecurity training, compared to just 27% in neighboring Lithuania, demonstrating the effectiveness of standardized, state-supported initiatives.

In brief, these diverse perspectives underscore the need for a comprehensive and adaptable approach to digital resilience in education. Systemic integration of digital literacy, as emphasized by (Kozyreva et al., 2022), and community engagement strategies, as proposed by (Kritzinger, 2020), must be complemented by targeted teacher training (Omojemite & Cishe, 2024), regulatory harmonization (Asimiyu, 2024), and inclusive public programs (Kont, 2023b). Aligning these efforts with international frameworks such as GDPR and eIDAS will be key to ensuring long-term digital security and inclusion in both developed and developing contexts.

Lastly,(Rasdiana et al., 2024) highlights the importance of aligning cybersecurity policy implementation with school culture and digital literacy levels. In her study of Indonesian secondary schools, she found that digital literacy acted as a mediating variable between institutional culture and student digital resilience. Schools with collaborative, trust-based environments and clear leadership structures were more effective in fostering responsible online behavior, particularly when digital literacy was embedded into daily practices rather than treated as an isolated subject. The findings suggest that policy frameworks must account for sociocultural variables within schools and provide resources to support context-sensitive implementations of cybersecurity curricula.

Complementing this perspective, (Srivastava et al., 2024) critically assesses existing cybersecurity awareness programs in Indian school education, pointing out that most initiatives suffer from a top-down, compliance-focused design. Through content analysis of national and regional programs, the author identifies a lack of contextual relevance, limited engagement with students' digital realities, and minimal focus on behavioral change. Srivastava argues for a shift toward participatory, experiential learning models that integrate local digital cultures and student agency. She recommends embedding cyber ethics, misinformation detection, and safe online communication skills into national frameworks, ensuring that awareness programs move beyond awareness-raising to transformative digital citizenship.

The following comparative table summarizes key national strategies in digital literacy and cybersecurity education across seven countries. By highlighting institutional frameworks, implementation gaps, and effective practices, this synthesis illustrates the diversity of policy responses and contextual challenges. It offers a clearer

understanding of how structural, pedagogical, and regulatory factors interact to shape digital inclusion outcomes, aligning with the study's capability-oriented approach.

Table 1: Comparative Synthesis of National Strategies in Digital Literacy and Cybersecurity Education.

Country	Institutional Framework	Identified Gaps	Good Practices	Contextual Notes
Brazil	Reuni Digital, UaB	Rural connectivity, digital governance	Massive enrollment programs (474 % increase)	Fragmented governance
India	Digital India, Kerala Mission	Rural implementation, legal enforcement	Community-based mentoring, peer learning	Strong subnational initiatives
Estonia	National Cybersecurity Strategy + CHMF	Library-sector disparities (e.g., Lithuania)	Cyber hygiene in primary school, 62 % librarian training	EU-aligned frameworks
South Africa	No national integration, 360safe tool	High non-compliance in schools	10-phase school model, local capacity-building	Deep urban-rural divide
Ecuador	Digital Transformation Agenda, ENCS	No cybersecurity law, low rural access	Inter-agency plans exist but lack enforcement	48.1 % rural internet access
Indonesia	Personal Data Law + UU ITE	Poor inter-agency coordination	Partial inclusion in curriculum	Frequent ransomware incidents
Nigeria	Cybercrimes Act, teacher training pilots	70 % gap in teacher preparedness	Simulation-based pedagogy with 65 % improvement	Weak enforcement in rural areas

Finally, what this study contributes is a multidimensional framework that integrates digital literacy, cyber hygiene, and pedagogical innovation into a typology of policy responses that are both capability-enabling and context-sensitive. This synthesis moves beyond sectoral or disciplinary boundaries by offering a holistic reading of how national strategies succeed or fail depending on their capacity to align technical, human, and regulatory components. It provides policymakers and educators with a map of actionable practices that foster sustainable, inclusive, and secure digital learning ecosystems, especially in countries like Ecuador facing persistent structural gaps.

3.2. Pedagogical Strategies And Educational Outcomes

3.2.1. Perception And Awareness in University and Library Contexts

(Piscikiene et al., 2021) examined the level of cybersecurity awareness within academic communities in Lithuania through a survey of 308 participants. The results were striking only 21% of respondents were familiar with basic terms such as "social engineering" or "phishing," and although 56.3% recognized the risks of using public Wi-Fi for sensitive transactions, 37.5% remained unaware of such vulnerabilities. The generational divide was particularly notable 78% of participants under 30 could identify dangerous websites, compared to just 22% of those over 50. These findings emphasize the urgent need to implement mandatory cybersecurity seminars and incorporate practical digital security modules into university curricula to close both generational and knowledge gaps.

In addition, (Kont, 2023a) expands the scope of this issue through a comparative analysis of public libraries in Estonia, Latvia, and Lithuania, involving 1,217 librarians and applying the HAIS-Q questionnaire. The study reveals considerable national differences: in Estonia, 62% of librarians had received formal cybersecurity training, compared to 40% in Lithuania. USB device safety practices and password management also varied only 27% of Lithuanian librarians routinely checked USB devices before use, versus 45% in Estonia. Furthermore, password manager usage was significantly higher in Estonia (87.5%) than in Latvia (52%). These disparities underscore the need for standardized cybersecurity protocols and compulsory certification for library professionals to ensure consistency and security in digital practices across public institutions.

Moreover, (Mastam et al., 2024) address another critical dimension of digital access by focusing on inclusive education in Malaysia. Their study brings attention to the challenges faced by students with disabilities and those from marginalized backgrounds, particularly in under-resourced rural schools. Despite initiatives such as the Digital Education Policy and the Digital Literacy Empowerment Program for Persons with Disabilities, many inclusive students still lack access to adaptive technologies and customized digital content. Interviews with teachers revealed that these gaps significantly hinder students' ability to develop foundational digital skills. The authors advocate for targeted investment in infrastructure, teacher training in inclusive digital pedagogies, and the creation of culturally relevant digital resources. Their findings call for a comprehensive strategy that addresses both technical access and pedagogical design to achieve genuine digital inclusion.

Similarly, (Basholli et al., 2023) explore the role of higher education in shaping cyber hygiene habits in Albania. Drawing from data collected at public and private universities, their study finds that although

technological access has increased, awareness and responsible usage remain insufficient. The absence of structured cybersecurity education especially in curriculum development and hands on training is identified as a major factor contributing to data breaches and security incidents. As a response, the authors propose integrating cyber hygiene content into academic programs, offering dedicated training for students and faculty, and launching awareness campaigns. They also highlight the value of partnerships between public institutions and private organizations, emphasizing that a collaborative approach is essential to fostering a broader culture of digital responsibility.

In conclusion, (Meiqi et al., 2024) provides a broader, cross-national perspective by analyzing digital literacy trends across 25 African countries. Their research shows that digital literacy is tightly linked to both the presence and affordability of ICT infrastructure, with marked gaps between urban and rural settings. However, the study also demonstrates that well-targeted inclusion policies can mitigate these disparities, especially when they prioritize women, the elderly, and rural communities. Importantly, Sun et al. find that higher national digital literacy rates correlate with reduced educational and income inequalities, even where infrastructure remains limited. They advocate for national strategies that integrate ICT infrastructure development, inclusive digital education, and focused policy interventions to ensure equitable digital access and opportunity across the continent.

In summary, these studies collectively highlight the multifaceted nature of digital literacy and cybersecurity awareness in educational and public institutions. Whether through targeted curricular reforms, inclusive teaching practices, or infrastructure investment, building digital resilience requires a coordinated and context-sensitive approach. From Europe to Africa and Southeast Asia, the evidence suggests that meaningful progress depends not only on technological deployment but also on how effectively institutions equip individuals to use it safely and inclusively.

3.2.2. Practical Simulations in Military and Educational Environments

Firstly, (Mednikarov et al., 2023) demonstrate the effectiveness of simulation-based training in both military and academic settings. In Bulgaria, their ransomware simulation program, which included scenarios such as "Brain Cipher," resulted in a 40% reduction in vulnerabilities among military personnel after 12 sessions and a 65% improvement in phishing detection among pedagogy students. The methodology, supported by quantitative measures like response times, was later adapted in Kazakhstan to train rural teachers, leading to a 30% increase in incident reporting. These outcomes highlight the scalability and practical value of immersive cybersecurity training in diverse educational contexts.

In parallel, (Malik et al., 2023) explore how innovation in higher education policy contributes to strengthening digital literacy in Indonesian universities. Their study shows that integrating tools such as digital libraries, online academic systems, and journal management platforms modernizes both teaching and administration. Moreover, it helps establish digital skills as foundational for students and faculty alike. The authors argue that infrastructure accessibility and continuous professional development are key to success, suggesting that institutions which prioritize systematic implementation of digital innovation are better prepared to adapt to technological change.

At the same time, (Septanto et al., 2024) examine digital literacy as a preventive strategy against the rise of online gambling, a rapidly growing cybercrime threat in Indonesia. Their analysis, based on a review of existing literature, emphasizes that digital literacy programs must extend beyond technical knowledge to include critical thinking, risk awareness, and personal data protection. They recommend embedding such content into school curricula and launching national awareness campaigns to empower vulnerable groups, especially youth and low-income populations, to recognize and resist digital threats.

Meanwhile, (Herwani & Pasiningsih, 2023) propose cyber pedagogy as a strategic approach to cultivate digital literacy in Indonesia's online learning environments. Their research underscores the importance of designing virtual classrooms that promote collaboration, critical thinking, and responsible technology use. By employing interactive platforms, digital storytelling, and peer learning networks, students gain practical skills for managing digital identities, evaluating online information, and participating safely in digital spaces. Their findings suggest that embedding cyber literacy into pedagogy is essential for equipping learners to navigate the complexities of the digital age.

Overall, these studies collectively highlight the importance of context-specific, practice-oriented strategies for advancing cybersecurity awareness and digital resilience in education. From simulation training (Mednikarov et al., 2023), to institutional innovation (Malik et al., 2023), crime prevention (Septanto et al., 2024), and pedagogical reform (Herwani & Pasiningsih, 2023), each contribution

demonstrates that effective digital literacy initiatives must be both adaptable and inclusive to meet the demands of a rapidly evolving technological landscape.

3.2.3. Digital Transformation in Higher Education: Lessons from Brazil

Initially, (Baxto, 2024) offers a detailed analysis of Brazil's digital transformation in higher education, focusing on programs such as Reuni Digital and the Open University of Brazil (UaB). Between 2011 and 2021, distance education enrollments increased by 474%, yet only 8.6% were in public institutions, reflecting persistent inequalities. Notable barriers included limited infrastructure 35% of rural schools lacked stable broadband and a lack of teacher training, with just 28% of educators in remote areas receiving instruction on digital platforms. To address these issues, (Baxto, 2024) recommends strategic partnerships with telecommunications companies to subsidize internet access and the inclusion of cybersecurity standards in national higher education policies.

Subsequently, (Fonseca & Borges-Tiago, 2024) extend the conversation by exploring how digital literacy intersects with cyberbullying prevention in university contexts. Their citation-based review emphasizes that digital literacy involves more than technical ability it requires ethical understanding, empathy, and critical thinking. They argue that integrating digital citizenship and cyberbullying awareness into university curricula can foster safer and more inclusive online environments. The authors also call for collaborative efforts among educators, librarians, and student support services, reinforcing (Baxto, 2024) argument that digital expansion must be accompanied by strong support structures for student well-being.

Equally important, (Fikry et al., 2024) examine the role of cyber hygiene in digital higher education, drawing lessons from the Malaysian experience during the COVID-19 pandemic. Their study reveals that remote learning intensified vulnerabilities in cyber practices at both institutional and individual levels. Unlike general cybersecurity, cyber hygiene refers to daily behaviors that protect digital systems. The authors stress the importance of incorporating cyber hygiene education into university policies and professional development programs, focusing on issues such as data privacy, device maintenance, and safe digital behavior recommendations that resonate strongly with Brazil's current digital transformation challenges.

In a related contribution, (Banitalebi et al., 2024) introduce the TALiDE instrument to assess digital assessment literacy among teachers in Iran. Their findings show a disconnect between instructors' positive attitudes toward digital tools and their actual implementation, largely due to training and resource limitations. The study highlights the need for targeted professional development and institutional support to ensure effective digital assessment practices. Their suggestions include the integration of assessment literacy into teacher education and ongoing, scenario-based training complement (Baxto, 2024) emphasis on systemic digital governance and underscore the importance of faculty empowerment in sustaining digital innovation.

Taken together, these studies demonstrate that digital transformation in higher education cannot rely solely on expanding access to technology. It must also include the development of human and institutional capacities. From (Baxto, 2024) call for equitable infrastructure and governance, to Fonseca's emphasis on ethical digital behavior, (Fikry et al., 2024) advocacy for cyber hygiene, and (Banitalebi et al., 2024) focus on assessment literacy, each contribution points to the need for holistic, context-aware strategies that align innovation with educational quality and digital security.

3.2.4. Strategic Convergence in Digital Literacy and Cybersecurity for Educational Resilience

Specifically, (Bhortake, 2024) presents a global overview of the evolving cybersecurity landscape, emphasizing the dual impact of digital connectivity: while it enhances learning and innovation, it simultaneously exposes educational systems to increasingly complex cyber threats. The study documents the shift from financially motivated hacking to more coordinated, state-sponsored cyberattacks, and highlights vulnerabilities introduced by the proliferation of IoT devices and social engineering tactics. (Bhortake, 2024) advocates for a multi-layered security approach that includes technical safeguards such as authentication, encryption, and backups, but also emphasizes the role of cyber hygiene, ethics, and continuous user education. The author underscores the importance of embedding cybersecurity education into curricula and building resilience through collaborative, cross-sectoral strategies.

Separately, (Bachtiar et al., 2024) focus on the transformative role of digital literacy in Indonesian secondary schools. Their empirical data show that students with stronger digital literacy skills not only perform better academically but also exhibit improved social interaction and greater confidence in navigating digital environments. Although 98.5% of students reported daily internet use for learning, notable gaps remain in areas like critical evaluation,

password security, and participation in structured digital training. (Bachtiar et al., 2024) and colleagues argue that digital literacy must be viewed as a multidimensional competency that includes cognitive, ethical, and socio-emotional elements. They recommend prioritizing institutional strategies that combine digital training with cybersecurity awareness, supported by inclusive and collaborative digital cultures, especially in under-resourced regions.

Based on these findings, several strategic recommendations can be drawn. First, digital literacy and cybersecurity must be holistically integrated across education systems, encompassing curriculum design, teacher development, and institutional policy. Second, institutions should implement layered defense strategies, pairing technical protections with scenario-based training, simulations, and awareness initiatives. Third, advancing equity and inclusion requires targeted investment in infrastructure and culturally responsive digital education, particularly for marginalized communities.

Fourth, the evidence underscores the need for continuous professional development for teachers and staff, including incentives for certification and access to peer-supported learning networks. Fifth, fostering collaborative ecosystems among education, government, industry, and civil society is essential for sharing intelligence, setting common standards, and coordinating responses to emerging risks. Last of all, educational programs must address the ethical and legal dimensions of digital participation, equipping students with the knowledge to engage responsibly and protect personal data in complex digital contexts.

In a nutshell, the work of (Bhortake, 2024) and (Bachtiar et al., 2024), alongside broader literature, demonstrates that digital transformation in education cannot succeed without simultaneously addressing cybersecurity and digital literacy. Institutions that invest in inclusive, adaptable, and ethically grounded strategies will not only improve academic outcomes but also strengthen the social fabric and digital resilience of their communities.

3.3. Public Policy And Regulatory Frameworks

3.3.1. Telecommunications Policy Review and Cyber Literacy

To begin with, (Szczepaniuk & Szczepaniuk, 2022) analyzed cybersecurity competencies within the context of telecommunications policies in Eastern Europe by proposing the Cyber Hygiene Maturity Assessment Framework. This model, grounded in the Plan-Do-Check-Act (PDCA) cycle, evaluates three key dimensions: infrastructure, organization, and people. The findings revealed that only 34% of organizations in Eastern Europe achieved advanced levels in cyber hygiene practices. This deficiency is largely attributed to outdated firmware in IoT devices and weak password management policies. Their study underscores the pressing need for standardized security protocols and targeted training for critical sectors such as energy and telecommunications.

Moreover, (Kont, 2023b) conducted a comparative study on public libraries in Estonia, Latvia, and Lithuania, identifying notable disparities in cybersecurity training. In Estonia, 62% of librarians had received cybersecurity training, compared to only 40% in Lithuania. Furthermore, USB device verification practices were more prevalent in Estonia (45%) than in Lithuania (27%). These contrasts point to the urgent need for harmonized European Union policies promoting mandatory certifications and standardized cybersecurity protocols, especially in regions with institutional capacity gaps.

3.3.2. Financial Literacy and Cybersecurity

Recent research confirms that financial literacy and cybersecurity are increasingly interdependent. (Căciulescu et al., 2024), drawing on Flash Eurobarometer 525 data, identify five citizen clusters across Europe including the "Cyber-Savvy Pragmatists" and "Digitally Hesitant At-Risk"each defined by varying levels of financial knowledge, digital confidence, and vulnerability. Alarmingly, only 18% of respondents demonstrate high financial literacy, with marked disparities by gender, age, and education. Those with low digital and financial skills face the highest exposure to fraud and identity theft, while even digitally confident individuals with poor financial judgment (the "Comfortably Naive") remain vulnerable to scams rooted in overconfidence.

Furthermore, the study shows that financial literacy alone is insufficient to mitigate cyber risk. Instead, digital financial literacy, the combined ability to manage financial decisions and recognize digital threats is essential. Although more financially literate individuals detect scams more readily, their increased engagement with online platforms can paradoxically raise exposure. Gender gaps are particularly significant: women are disproportionately represented in the most at-risk clusters, pointing to systemic deficits in financial and digital education. (Căciulescu et al., 2024) call for stratified, targeted interventions that address these intersecting vulnerabilities.

In a complementary analysis, (Popoola et al., 2024) compare cybersecurity education strategies in Africa

and the United States. They find that behavioral and constructivist approaches are most effective when adapted to context. In African settings, where digital literacy and infrastructure vary, community-based workshops and mobile platforms show strong results. In contrast, the U.S. relies more on simulation-based training, which must also address complacency among digitally active users. The authors advocate for closer integration between cybersecurity and financial literacy initiatives and promote cross-regional collaboration to tailor solutions to local needs.

At the educational level, (Nayyar & Gupta, 2024) stresses the importance of embedding cybersecurity principles into financial education, particularly within teacher training. She argues that educators must act as digital role models, incorporating password management, online safety, and cyber hygiene into routine instruction. As financial services become increasingly digital, education systems must not only provide access but also develop informed, security-conscious users.

(Adeleye et al., 2024) addresses the foundational issue of access. Her framework for technical literacy inclusion emphasizes universal infrastructure, teacher professional development, community-based digital hubs, and the integration of financial and digital literacy into education from early stages. She highlights that equity in access and culturally relevant content is essential for empowering marginalized populations and fostering long-term cyber resilience.

In conclusion, the intersection of financial literacy and cybersecurity demands multidimensional policy responses. The evidence underscores the need for integrated curricula, context-sensitive strategies, and targeted interventions particularly for women and underserved groups. Ensuring inclusive access, continuous teacher training, and cross-sector collaboration will be critical for preparing citizens to navigate and protect themselves within an increasingly digital financial ecosystem.

3.3.3. Libraries And Rural Digitalization as Inclusion Drivers

(Omidvar & Tavakoli, 2023) offer a critical review of rural digital literacy policies in Iran, revealing that national strategies have primarily benefited urban areas, while rural communities remain underserved. Their analysis of key policy documents including the Cyberspace Strategic Document, Digital Transformation Strategic Document, and the Sixth Development Plan shows that rural digital skills are often addressed in a fragmented manner. Although initiatives such as broadband expansion and e-government services are mentioned, essential elements like digital training for agricultural innovation, support for rural entrepreneurship, and development of local content are underemphasized. The authors recommend prioritizing rural-specific policies, targeted infrastructure investment, and community-driven digital service development to ensure more equitable and sustainable digital transformation.

In a similar vein, (Magunje & Chigona, 2024) examine the challenges faced by resource-constrained schools in South Africa, particularly in rural and marginalized urban contexts. Their qualitative research reveals that school management teams (SMTs) often lack both digital confidence and cybersecurity knowledge, leaving learners, educators, and families vulnerable to cyber threats. The absence of cybersecurity policies, limited training, and poor access to digital tools exacerbate these risks. The authors argue for continuous professional development for SMTs, localized cybersecurity frameworks, and dedicated investment in building human capital to support digital inclusion in these contexts.

Additionally, (Kont, 2023a) provides an Estonian case study that demonstrates how public libraries can function as strategic hubs for digital literacy and cyber awareness. Her findings show that 62% of Estonian librarians have received formal cybersecurity training, a reflection of the country's integrated national strategies. (Kont, 2023a) emphasizes that beyond access to digital tools, success depends on localized content, outreach programs, and training tailored to vulnerable populations such as the elderly, women, and rural residents. Her work illustrates how libraries, supported by national policies and local engagement, can effectively bridge digital divides.

Also, (Sogalrey et al., 2024) reinforce these perspectives through a global bibliometric review of over 3,000 publications. Their analysis highlights a growing emphasis in the literature on digital inclusion, critical thinking, and the importance of embedding local cultural elements into digital literacy curricula. The authors advocate for policies that recognize libraries and community centers as central actors in digital education, particularly in underserved rural areas.

Taken together, these studies converge on several strategic priorities. First, national digital policies must explicitly address rural realities, ensuring infrastructure development is accompanied by localized content and training. Second, libraries should be formally recognized and funded as digital inclusion hubs, with continuous staff development and community outreach programs. Third, building capacity among school and community leaders is

vital to foster cybersecurity awareness in low-resource settings. Fourth, digital literacy curricula must be context-sensitive, integrating local languages and cultural norms to engage vulnerable groups effectively. Fifth, cross-sector collaboration between governments, educational institutions, libraries, and civil society is essential to ensure scalable, equitable access to digital opportunities.

To put it briefly, advancing digital inclusion requires more than extending infrastructure it demands the strategic mobilization of community spaces like libraries, investment in human capital, and the creation of policies that are locally grounded and socially inclusive. Efforts targeting rural digitalization must be integrated, sustained, and adaptable to empower all citizens, particularly those in marginalized areas, to fully participate in the digital society.

3.3.4. Recommendations For Comprehensive Policies

(Johnson-Glenberg, 2018) offers a critical assessment from Western Australia, where integrating cybersecurity into school curricula remains a persistent challenge. Although national and state frameworks exist, Johnson identifies major implementation gaps due to limited teacher training, inconsistent curriculum standards, and a lack of resources. The study emphasizes that cybersecurity should not be treated as a peripheral topic, but rather as a foundational component of digital literacy. To achieve this, (Johnson-Glenberg, 2018) recommends comprehensive teacher professional development, curriculum alignment, and the establishment of continuous assessment mechanisms to ensure that all students acquire essential cyber hygiene competencies.

In contrast, (Anandraj et al., 2024) draws from the success of the Total Digital Literacy Mission in Kerala, India, highlighting how community-based models can drive widespread digital inclusion. His findings reveal that localized initiatives anchored in peer mentoring, local-language instruction, and strong public-private partnerships have significantly improved digital literacy among women, older adults, and rural populations. (Anandraj et al., 2024) recommends that national strategies formally integrate and fund such grassroots efforts, leveraging civil society and existing community networks to extend reach and impact, particularly among marginalized groups.

Likewise, (Wang & Si, 2024) explore how libraries in China act as critical agents for digital literacy, especially in underserved regions. Their mixed-methods study underscores that both public and academic libraries can function as hubs for digital inclusion, offering training, content access, and lifelong learning opportunities. To maximize their potential, the authors call for greater resource allocation, policy support, and cross-sectoral coordination, arguing that libraries must be equipped to meet diverse community needs.

In a broader ethical frame, (Tello de la Torre et al., 2021) urge policymakers to consider not only technical skills but also the psychological and ethical dimensions of digital engagement. They advocate for integrating digital ethics, critical thinking, and personal data protection into digital literacy programs. Their holistic approach to digital citizenship stresses the importance of balancing innovation with individual rights, autonomy, and digital well-being.

From a risk-based perspective, (Nzeakor & Nwoke, 2024) present data from Nigeria showing a direct link between poor digital hygiene and increased cybercrime victimization. They propose embedding digital safety modules into school and civil service curricula, supported by community-based ambassadors and incentive-driven programs that promote safe digital practices at the individual and collective levels.

Besides, (Căciulescu et al., 2024) highlight the need for data-driven, stratified digital and financial literacy policies across populations with varying risk profiles. Their research identifies gender disparities and other vulnerabilities, calling for targeted educational interventions that combine cybersecurity and financial literacy within harmonized regulatory frameworks. They argue that tailoring content to specific user groups is key to reducing systemic digital risks.

At the same time, (Abdizhadil et al., 2024) and (Hadi et al., 2023) underscore the urgency of introducing digital literacy from early childhood through to higher education. Their studies emphasize innovative, practice-oriented methods and support curriculum reform, teacher training, and adaptable learning models that reflect local realities. These approaches aim to build strong digital foundations across age groups and socio-economic contexts.

In summary, a comprehensive digital policy agenda should include: empowering libraries and community centers as pillars of digital inclusion (Wang & Si, 2024); embedding good digital hygiene practices through education and behavioral strategies (Nzeakor & Nwoke, 2024); designing gender-sensitive, risk-responsive literacy programs (Căciulescu et al., 2024); integrating ethics and cybersecurity into all levels of education with updated curricula and faculty development (Abdizhadil et al., 2024) (Hadi et al., 2023);

addressing the psychological and ethical aspects of digital engagement (Tello de la Torre et al., 2021); prioritizing teacher training and curriculum coherence in cybersecurity education (Johnson-Glenberg, 2018); and supporting sustained, community-led initiatives for inclusive digital learning (Anandraj et al., 2024).

Ultimately, by aligning national strategies with these multidimensional priorities, policymakers and educators can foster digital ecosystems that are not only innovative and inclusive, but also secure, ethical, and resilient in the face of ongoing technological change.

4. DISCUSSION

This systematic review critically examines the impact of digital literacy on educational outcomes and assesses the effectiveness of public policies aimed at promoting online safety and social inclusion across diverse global contexts. The findings confirm that digital literacy is a multifaceted construct—encompassing technical, cognitive, socio-emotional, and ethical competencies—that correlates with improved academic performance, equity, and educational resilience. Interpreted through Sen's Capability Approach, the evidence suggests that access to digital resources is only a starting point; outcomes ultimately depend on conversion factors such as infrastructure, teacher preparedness, gender, and policy coherence, which condition whether resources become real opportunities for learners. At the same time, persistent gaps in infrastructure, teacher training, regulatory frameworks, and policy implementation continue to hinder the realization of inclusive and sustainable digital education.

4.1. Synthesis And Interpretation of Key Findings

The evidence shows that digital literacy interventions can yield substantial academic and social benefits, but these are highly context dependent. For instance, in Uganda, students with higher digital engagement achieved grades 18 points higher than their peers, yet only 10% of secondary schools had reliable internet and computer access—underscoring the critical role of infrastructure (Abiodun Nafiu et al., 2024). In Kazakhstan, the integration of digital platforms in primary education improved functional literacy, but similar gains were not observed in regions lacking teacher training or sufficient resources (Abildina et al., 2024). Read through the lens of the Capability Approach, these patterns illustrate how infrastructure and teacher preparedness operate as conversion factors that mediate the translation of digital inputs into capabilities and learning outcomes.

Access alone does not guarantee the development of critical or ethical digital competencies. In Indonesia, while 98.5% of students reported using the internet for learning, only 82.7% felt competent to evaluate information quality, and gaps persisted in cyber hygiene practices (Wang & Si, 2024). Similarly, in Estonia, despite widespread awareness of cyber risks, more than one third of the population reported not changing passwords regularly signaling a persistent distance between knowledge and safe practice. These observations align with the literature's call for policies that integrate digital literacy and cyber hygiene, moving beyond instrumental skills to cultivate critical thinking, digital citizenship, and responsible online behavior.

Gender and socioeconomic disparities remain structural barriers to digital inclusion. In Latin America, only 35% of rural women have broadband access, compared to 68% in urban areas, and targeted STEM initiatives have reached just 18% of schools (Ancheta-Arrabal et al., 2021). In Pakistan and Indonesia, sociocultural norms and limited institutional support further restrict women's access to digital skills training (Naseer et al., 2023; Septanto et al., 2024). In capability terms, gender, place of residence, and institutional supports function as decisive conversion factors: even when access is available, these dimensions can constrain the transformation of resources into substantive freedoms to learn and participate.

4.2. Policy Effectiveness And Implementation Gaps

The review identifies several policy models with demonstrable success, such as India's Total Digital Literacy Mission and Estonia's integration of cyber hygiene into national curricula. Kerala's community-driven approach in India, for example, mobilized over 50,000 learners supported by more than 2,000 volunteers (Anandraj et al., 2024). These initiatives demonstrate how community participation and institutional commitment can expand individual opportunities, turning available resources into genuine capabilities. Yet even in these cases, structural inequalities persist, particularly in rural and marginalized communities, underscoring that infrastructure and institutional support remain decisive conversion factors in Sen's framework.

Against this global backdrop, Ecuador has taken important steps toward establishing a strategic framework for cybersecurity and digital transformation, notably with the adoption of the National Cybersecurity Strategy 2022–2025 and the Digital Transformation Agenda 2022–2025. These instruments outline six critical pillars: governance, cyber resilience, combatting cybercrime, cyber

defense, capacity building, and international cooperation. Despite these advancements, challenges remain in standardizing protocols and protecting key sectors such as education and health. Compared to international models like Estonia's Cybersecurity Act (2018) or the European Union's NIS2 Directive, Ecuador's regulatory framework is still fragmented and lacks binding cybersecurity legislation (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022; Terán & Guevara Ruales, 2025).

The Organic Law on Personal Data Protection (2021) and the National Digital Development Plan 2022–2025 provide general guidelines on digital security. However, Ecuador's absence of a dedicated cybersecurity law hampers the integration of sectoral obligations and critical infrastructure protection. The National Cybersecurity Strategy aims to fill this gap by proposing the creation of a National Cybersecurity Committee and mandatory protocols for essential service providers. Yet its effectiveness ultimately depends on the establishment of a solid legal framework (Universidad Internacional de Valencia, 2025; Terán & Guevara Ruales, 2025).

In parallel, Ecuador has also advanced in the education sector. The Digital Education Program has improved access to devices and connectivity in schools. However, training on cyber hygiene remains inconsistent and is not systematically integrated into curricula. In contrast, Estonia reports 62% of library staff trained in digital security, and Bulgaria has successfully reduced vulnerabilities through regular simulations. Ecuador continues to face persistent fragmentation in teacher training and lacks standardized metrics to assess outcomes. Rural internet access remains a critical issue: only 48.1% of rural households have an internet connection, compared to 73.6% in urban areas (Instituto Nacional de Estadística y Censos [INEC], 2024). Although the national gender gap in internet use is relatively small (85.1% of men vs. 81.8% of women), there are no official disaggregated data available for rural areas (Ancheta-Arrabal et al., 2021; Baxto, 2024; INEC, 2024).

Drawing from international best practices, four key recommendations emerge for Ecuador:

1. Adopt a cybersecurity law aligned with the EU NIS2 Directive, focusing on critical infrastructure protection and mandatory audits.
2. Integrate digital citizenship and cyber hygiene modules across all education levels, inspired by Estonia's continuous teacher training model and ISO 27001 certification standards.
3. Expand rural connectivity through public-private partnerships, emulating India's Kerala Digital Literacy Mission and the establishment of gender-focused community digital centers.
4. Implement a national monitoring system disaggregated by region and gender, following the European Cyber Hygiene Maturity Framework (CHMF) model to evaluate public policies (Baxto, 2024; Skarga-Bandurova et al., 2021; Anandraj et al., 2024).

The case of Indonesia illustrates that even with a robust legal framework, such as the Electronic Transactions Law (2008), poor inter-institutional coordination can increase vulnerability to ransomware and other cyber threats. In Ecuador, this risk is partially mitigated by the ECU-CERT, though its operational capacity and integration with predictive cyber intelligence protocols must be significantly strengthened (Tokan et al., 2024).

In conclusion, Ecuador must prioritize synergy between its Digital Transformation Agenda and National Cybersecurity Strategy, closing legal gaps and fostering an inclusive digital culture. Only through these coordinated efforts can the country improve its standing in the Global Cybersecurity Index, where it ranked 119th out of 182 countries in the 2020 edition (International Telecommunication Union [ITU], 2020). These findings confirm that policies only translate into real freedoms when they are supported by coherent regulations, local adaptation, and institutional capacity—key conversion factors in the Capability Approach.

4.3. The Capability Approach And Empirical Findings

The findings of this review can be more fully understood when interpreted through Sen's Capability Approach, which highlights that access to resources does not automatically translate into substantive opportunities. Instead, outcomes depend on conversion factors—structural, institutional, and sociocultural—that determine whether resources can be transformed into real freedoms to achieve valued goals.

In Uganda, for example, the availability of computers in only 10% of schools (Abiodun Nafiu et al., 2024) shows how limited infrastructure severely restricts students' capabilities, even when individual motivation is high. In Kazakhstan, although digital platforms improved functional literacy, the absence of adequate teacher training hindered the conversion of access into sustained learning outcomes (Abildina et al., 2024). These cases illustrate how infrastructure and teacher preparedness act as conversion factors: without them, resources remain underutilized, and inequality persists.

Estonia has shown a contrasting scenario. National campaigns and the integration of cyber hygiene into curricula have resulted in 62% of library

staff being trained in digital security (Kont, 2023b). In this case, supportive institutional policies function as enabling conversion factors, expanding digital capabilities across both educators and learners. Conversely, in Indonesia, despite nearly universal access (98.5% of students use the internet for education), only 82.7% felt confident evaluating information quality (Wang & Si, 2024). Here, sociocultural norms and limited teacher preparation operate as restrictive conversion factors, preventing access from becoming critical and ethical digital competence.

In Latin America, gender and rurality emerge as persistent constraints. Broadband access remains heavily skewed toward urban populations and men (Ancheta-Arrabal et al., 2021; Baxto, 2024), and initiatives targeted at women in STEM reach only a small fraction of schools. These findings confirm that gender and geographic location are decisive conversion factors, determining whether digital literacy policies translate into equitable participation in the digital economy.

By applying Sen's framework to these diverse contexts, this review shows that digital literacy and cyber hygiene cannot be evaluated solely by metrics of access or technical provision. Instead, their effectiveness must be assessed by the extent to which policies and practices expand individuals' substantive freedoms—such as the freedom to learn safely, to participate equitably in education, and to develop critical, ethical, and socio-emotional competencies for life in digital societies.

4.4. Theoretical And Practical Contributions

This review advances the field by moving beyond a purely technical or access-based understanding of digital literacy. It synthesizes evidence showing that digital literacy should be conceptualized as an integrated set of competencies—critical thinking, information evaluation, digital ethics, and cyber hygiene—that are essential for educational sustainability and social justice. From a capability perspective, these findings demonstrate that digital literacy is not only a catalyst for academic achievement but also a foundation for equitable participation in the digital economy and society.

The analysis also underscores the importance of differentiated pedagogical strategies. Empirical evidence reveals that business students outperform accounting students in password management, while social science students tend to adopt safer practices than their technical counterparts (Eliza et al., 2024; Madanu et al., 2024). These results suggest that discipline-specific curricula and psycho-social interventions are necessary to ensure that conversion factors—such as prior knowledge, professional orientation, and disciplinary culture—do not become barriers to capability expansion.

In practical terms, this review highlights that educational systems must integrate cyber hygiene and digital ethics into the core of digital literacy frameworks. This integration ensures that access to technology and the development of technical skills are accompanied by the cultivation of resilience, responsible communication, and risk awareness. Such a holistic approach directly responds to the need for policies that transform digital resources into substantive freedoms, a key principle of Sen's Capability Approach.

By aligning theoretical insights with empirical evidence, this review provides a conceptual and practical foundation for context-sensitive policies and curricula. The theoretical contribution lies in positioning digital literacy as a capability-enhancing construct rather than a technical skillset. The practical contribution lies in identifying actionable strategies—teacher training, discipline-specific curricula, and continuous cyber hygiene education—that can enable equitable and sustainable digital inclusion.

4.5. Implications And Future Directions

The findings underscore the need for comprehensive, evidence-based, and forward-looking digital policies. In capability terms, policies should not only provide resources but also create the conditions that convert those resources into real opportunities for learners and educators. Policymakers should prioritize:

1. Integrated frameworks that align infrastructure investment with teacher training and adaptive curricula, ensuring that connectivity and devices are transformed into sustained learning outcomes.
2. Gender-responsive and intersectional approaches to address persistent disparities across gender, rural–urban location, socioeconomic status, and disability, supported by targeted incentives and outreach.
3. Continuous professional development for teachers, with clear competency standards, certification pathways, mentoring, and peer-learning opportunities to consolidate safe and critical digital practices.
4. Community-driven and locally adapted initiatives that leverage schools, libraries, and civil society networks to ensure relevance, trust, and long-term sustainability.
5. Robust monitoring and evaluation systems, with interoperable data, regular audits, and disaggregation by gender, region, and school

type. Indicators should capture not only access and usage but also critical competencies and safe practices.

International collaboration and knowledge exchange are equally essential. Successful models—such as Estonia's systemic integration of cyber hygiene, Kerala's community mobilization, and the EU's data-protection standards—offer valuable lessons but must be adapted to local realities of institutional capacity, culture, and legal frameworks. Policy transfer should therefore proceed through pilot projects and formative evaluation before nationwide scaling.

Future research should explore: (i) the long-term impacts of digital literacy and cyber hygiene programs on academic achievement and behavioral resilience; (ii) the implications of emerging technologies (e.g., AI, IoT) for classroom practice, equity, and online safety; (iii) the effectiveness of cross-sectoral partnerships (education, telecommunications, social policy, justice) in strengthening digital resilience; and (iv) the development of capability-based indicators to assess whether policies expand learners' substantive freedoms to participate, learn, and act safely in digital environments. Mixed-methods and longitudinal designs, with subnational and gender-disaggregated analyses, will be critical to guide adaptive policy cycles and ensure accountability.

4.6. Novelty And Contribution

This study distinguishes itself from previous reviews by systematically integrating cyber hygiene as a core dimension of digital literacy and by critically analyzing policy effectiveness across multiple regions and educational levels. Unlike prior works that narrowly focused on access or basic skills, this review positions digital literacy as a capability-enhancing construct, aligning technical proficiency with cognitive, socio-emotional, and ethical dimensions.

Methodologically, the study applies the PRISMA protocol alongside rigorous quality assessment tools such as ROBINS-I, CASP, and GRADE, ensuring transparency, reproducibility, and analytical depth. This combination provides a more robust synthesis than previous regional or single-focus reviews, offering a comprehensive evidence base for cross-national comparison.

The principal contribution lies in proposing a holistic, context-sensitive framework that demonstrates how digital literacy and cyber hygiene jointly shape educational equity, social inclusion, and sustainable development. By explicitly incorporating Sen's Capability Approach, the review reframes digital literacy not merely as a resource to be delivered but as a set of substantive freedoms that individuals can exercise to participate, learn, and thrive in digital societies.

Through this lens, the originality of the study lies in its ability to bridge theoretical innovation with practical policy guidance: identifying conversion factors that explain disparities across contexts and outlining actionable strategies for policymakers and educators. This dual emphasis ensures that the study contributes both to academic debates on digital literacy and to the design of effective, equitable, and sustainable educational policies.

4.7. Limitations And Future Research

This review provides a comprehensive and comparative synthesis of digital literacy and cybersecurity policies across diverse global contexts; however, certain limitations must be acknowledged. The study's scope was confined to peer-reviewed literature published between 2020 and 2024 in English and Spanish, which may have excluded relevant grey literature and policy documents. While this decision ensured methodological rigor and consistency, it may have limited the inclusion of context-specific insights, especially from countries where governmental or community-driven initiatives are more often documented outside academic outlets.

Although the adoption of the PRISMA 2020 protocol guaranteed transparency in the selection process, the heterogeneity of study designs—ranging from simulation trials and conceptual frameworks to policy evaluations and qualitative case studies—limited the feasibility of conducting meta-analyses and posed challenges for quality assessment using ROBINS-I, CASP, and GRADE. Moreover, the absence of granular subnational data constrained the analysis of territorial disparities in implementation. This was particularly evident in countries such as Ecuador, Nigeria, and Indonesia, where national strategies often obscure urban–rural inequalities and institutional fragmentation.

A further limitation relates to potential selection bias, as the exclusion of grey literature may have disproportionately excluded innovative but unpublished interventions from low- and middle-income regions. This restricts the scope of the review and suggests that future studies should incorporate structured searches of grey literature and non-English sources to ensure a more inclusive evidence base.

To address these gaps, future research should:

1. Integrate grey literature and local-language sources, especially in regions where academic output is limited but community-driven programs are well documented.

2. Adopt mixed methods approaches that combine policy analysis with ethnographic or participatory research to capture the lived realities of digital exclusion.
3. Develop longitudinal studies to assess the enduring impact of cybersecurity and digital literacy education on behavioral resilience.
4. Incorporate capability-based indicators, rooted in Sen's framework; to evaluate how digital literacy policies not only deliver access but also expand individuals' real freedoms to learn, participate, and thrive in digital societies.

By addressing these limitations, future studies can generate a richer, more context-sensitive understanding of what makes digital inclusion policy truly effective, equitable, and sustainable across both the Global North and South.

5. CONCLUSIONS

This systematic review draws on 61 studies conducted between 2020 and 2024 across multiple global contexts to analyze the impact of digital literacy on educational outcomes and evaluate the effectiveness of public policies promoting online safety and social inclusion. The evidence confirms that digital literacy is not limited to technical proficiency; rather, it encompasses cognitive, socio-emotional, and ethical competencies that shape how individuals interact with digital environments. While the correlation between digital literacy and academic performance is evident, as shown by an 18-point difference in math scores in Uganda and a 30 percent improvement in functional literacy in Kazakhstan, these benefits depend on how effectively structural, pedagogical, and sociocultural barriers are addressed.

From a structural and policy perspective, the review identifies persistent infrastructure deficits in rural and marginalized areas. For instance, only 10 percent of schools in Uganda have access to stable internet, limiting equitable learning opportunities. In contrast, countries such as Estonia and India offer promising models. Estonia's integration of cyber hygiene into the national curriculum and India's community-driven digital literacy missions illustrate the importance of aligning infrastructure investment with localized, inclusive strategies that engage schools, families, and communities.

Moreover, teacher preparedness emerges as a critical bottleneck in the integration of digital skills and cybersecurity into education. Studies from South Africa and Pakistan report that approximately 70 percent of teachers lack basic cybersecurity training, undermining their ability to transfer knowledge or promote safe online practices. Solutions include implementing mandatory certifications, promoting practical training through simulations, and offering incentives for continuous professional development to build a more resilient teaching workforce.

In terms of sociocultural equity, gender and socioeconomic disparities remain deeply entrenched. In Latin America, rural women face a 33 percent broadband access gap compared to their urban counterparts. Similarly, in Pakistan, entrenched cultural norms continue to restrict girls' participation in digital education. The review highlights the need for policies that incorporate gender-sensitive pedagogies, subsidized device programs, and the development of inclusive community hubs that serve as accessible points of entry into the digital world for underrepresented groups.

Equally important, cyber hygiene integration has shown measurable success in reducing exposure to digital threats. Case studies from Bulgaria and Nigeria demonstrate that ransomware simulations and password management training can reduce vulnerabilities by 40 to 65 percent. However, awareness alone is insufficient. Lasting behavioral change requires institutionalized protocols such as ISO 27001 compliance and regular reinforcement through structured programs and policy mandates.

Despite these insights, the review acknowledges several limitations. First, the focus on studies published between 2020 and 2024 and restricted to English and Spanish may exclude region-specific gray literature and longer-term trends. Second, methodological inconsistencies across studies, particularly the lack of standardized tools for measuring digital literacy and cybersecurity maturity, limited the potential for comparative analysis. Future research should prioritize the development of common evaluation metrics and the inclusion of localized data from underrepresented regions.

In response to these findings, a set of strategic policy recommendations is proposed. National curricula should integrate digital literacy and cyber hygiene as core competencies, emphasizing critical thinking, responsible behavior, and ethical engagement. Rural broadband expansion must be prioritized through public-private partnerships, drawing lessons from Kerala's Total Digital Literacy Mission. Additionally, teacher training should be institutionalized through mandatory cybersecurity programs and collaborative, practice-based models such as Nigeria's simulation-driven initiatives. Gender-inclusive strategies are also essential, including gender-disaggregated data monitoring and quotas to ensure women's participation in STEM education and digital governance.

From a broader perspective, this study contributes to the field by framing cyber hygiene as a

key component of digital citizenship. It highlights the intersection of technical, human, and procedural dimensions in building resilient and equitable educational systems. Aligning digital literacy policy with Sustainable Development Goal 4 on inclusive and quality education allows governments to foster transformation that is innovative and socially inclusive.

In conclusion, the global evidence presented in this review calls for coordinated, context-sensitive policymaking. Only through collaborative and evidence-based strategies can digital literacy become a true driver of educational equity and sustainable development in an increasingly interconnected world.

By reconceptualizing digital literacy through the lens of Sen's Capability Approach, this study offers a paradigm shift from metrics of access to frameworks of opportunity, paving the way for future equity-oriented digital education reforms.

Acknowledgement: We wish to express our sincere gratitude to the Pontificia Universidad Católica del Ecuador for their support of our research, which was conducted as part of the activities of the Applied Information Systems and Technologies research group (SITECIA), registered under GI-Quito-071-2022. Furthermore, we extend our heartfelt appreciation to the Anonymous Reviewers whose thoughtful and constructive recommendations greatly enhanced the quality of this paper. Their expertise and feedback played a pivotal role in refining our research and ensuring its rigor and credibility.

REFERENCES

Abdizhadil, Y., Moldassan, K., Tekesbayeva, A., Massimbayeva, A., & Sembayeva, A. (2024). Development of digital literacy of a future educational psychologist in the process of professional training. *Scientific Herald of Uzhhorod University. Series Physics, 56*, 1326–1338. https://doi.org/10.54919/physics/56.2024.132eh6

Abildina, S., Dusembinova, R., Sarsekeyeva, Z., Mukhametzhanova, A., & Aidarbekova, K. (2024). Functional literacy development of junior schoolchildren based on digital educational resources. *Scientific Herald of Uzhhorod University. Series Physics, 56*, 1295–1305. https://doi.org/10.54919/physics/56.2024.129ej5

Abiodun Nafiu, L., Julius, A., Hadiijah, N., & Nafiu Lukman Abiodun, P. (2024). Digital literacy and educational outcomes: A case study of secondary schools in Gulu. *Metropolitan Journal of Social and Educational Research, 3*(1), 1–12. Retrieved from https://www.researchgate.net/publication/385217888

Adeleye, O. O., Eden, C. A., & Adeniyi, I. S. (2024). Educational technology and the digital divide: A conceptual framework for technical literacy inclusion. *International Journal of Science and Research Archive, 12*(1), 150–156. https://doi.org/10.30574/ijsra.2024.12.1.0405

Anandraj, K. C., Vattikulla, B., & Aravind, S. (2024). Total digital literacy initiatives in Kerala: A study of the Educational Digital Awareness Mission. *International Journal of Innovative Research in Technology, 11*(5), 1518–1523. https://doi.org/10.2139/ssrn.5001019

Ananin, V., & Uvarkina, O. (2023). Political visions of cyber education. *National Technical University of Ukraine Journal: Political Science. Sociology. Law, 1*(57), 35–39. https://doi.org/10.20535/2308-5053.2023.1(57).280780

Anastasya, V., & Kansil, C. S. T. (2024). Efektivitas hukum dan kebijakan publik dalam menghadapi ancaman siber terhadap keamanan negara. *Qistina: Jurnal Multidisiplin Indonesia, 3*(2), 1–15. Retrieved from https://www.kemhan.go.id/pothan/2024/07/15/keamanan-siber-dan-kebutuhan-sistem-digital-di-dunia-maya.html

Ancheta-Arrabal, A., Pulido-Montes, C., & Carvajal-Mardones, V. (2021). Gender digital divide and education in Latin America: A literature review. *Education Sciences, 11*(12), 804. https://doi.org/10.3390/educsci11120804

Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. *Applied Sciences, 11*(23), 11269. https://doi.org/10.3390/app112311269

Asimiyu, Z. (2024). Policy pathways for cyber ecosystem resilience: National security approaches in the digital era. *ResearchGate Preprint*. Retrieved from https://www.researchgate.net/publication/385681683

Azizbayov, E. I. (2024). Cyber hygiene in public administration of Azerbaijan: Ensuring data security. *Journal of Modern Technology and Engineering, 9*(1), 94–101. https://doi.org/10.62476/jmte9294

Bachtiar, W., Priatna, W. B., Santoso, H., Wijaya, A. S., & Nugroho, D. R. (2024). The importance of digital literacy in enhancing the quality of education and social harmony. *International Journal of Multidisciplinary Research and Analysis, 7*(11), 5310–5317. https://doi.org/10.47191/ijmra/v7-i11-43

Banitalebi, Z., Estaji, M., & Brown, G. T. L. (2024). Measuring teacher assessment literacy in digital

environments: Development and validation of a scenario-based instrument. *[Manuscript in preparation]*.

Basholli, A., Mema, B., Basholli, F., Hyka, D., & Salillari, D. (2023). The role of education in cyber hygiene. In *Advanced Engineering Days* (Vol. 7, pp. 1–5). Retrieved from https://www.researchgate.net/publication/373077128

Baxto, W. (2024). Public policy and digital transformation in higher education. In *EAI/Springer Innovations in Communication and Computing* (pp. 59–85). Springer. https://doi.org/10.1007/978-3-031-52296-3_4

Behera, C., & Deb, J. P. (2023). An overview of digital literacy and cyber socialization in the educational scenario of the 21st century. *Asian Journal of Multidisciplinary Research & Review, 8*(2), 70–79. Retrieved from https://www.researchgate.net/publication/372725326

Bhortake, J. (2024). Securing the digital realm: Navigating cyber threats, risks, and resilience. *ResearchGate Preprint*. https://doi.org/10.13140/RG.2.2.15044.60808

Căciulescu, A. R., Răzvan, R., Țurcanu, D., & Radovici, A. (2024). Mapping cyber-financial risk profiles: Implications for European cybersecurity and financial literacy. *Risks, 12*(12), 200. https://doi.org/10.3390/risks12120200

CASP. (2020). *CASP qualitative studies checklist*. https://casp-uk.net/casp-tools-checklists/qualitative-studies-checklist/

Chancusig Ruiz, F. (2023). Herramientas digitales para fomentar la alfabetización mediática en la era digital. *Revista Ingenio Global, 2*(1), 35–45. https://doi.org/10.62943/rig.v2n1.2023.60

Eliza, F., Fadli, R., Hidayah, Y., Ramadhan, M. A., Yassin, A., & Bhanu Setyawan, M. (2024). Building a secure digital future: Investigating cyber hygiene levels of accounting, finance, and business students. *Data and Metadata, 3*, 544. https://doi.org/10.56294/dm2024.544

Fikry, A., Hamzah, M. I., Hussein, Z., Abdul, A. J., & Abu Bakar, K. A. (2024). Defining the beauty of cyber hygiene: A retrospective look. *IEEE Engineering Management Review, 52*(2), 174–180. https://doi.org/10.1109/EMR.2024.3361023

Fonseca, J., & Borges-Tiago, T. (2024). Digital literacy education and cyberbullying combat: Scope and perspectives. In *Springer Proceedings in Business and Economics* (pp. 157–164). Springer. https://doi.org/10.1007/978-3-031-51038-0_18

Guaña Moya, J., Acosta Vargas, P., Arteaga Alcívar, Y. A., & Begnini Domínguez, L. F. (2022). Impact of ICTs on academic development and the creation of educational public policies in times of pandemic. In *Proceedings of the 17th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–6). IEEE. https://doi.org/10.23919/CISTI54924.2022.9820096

Guana Moya, J., Arteaga Alcivar, Y. A., Chiluisa Chiluisa, M., & Begnini Dominguez, L. F. (2022). Evolution of information and communication technologies in education. In *Proceedings of the 3rd International Conference on Information Systems and Software Technologies (ICI2ST)* (pp. 138–144). IEEE. https://doi.org/10.1109/ICI2ST57350.2022.00027

Guaña-Moya, J., Arteaga-Alcívar, Y., Criollo-C, S., & Cajamarca-Carrazco, D. (2024). Use of interactive technologies to increase motivation in university online courses. *Education Sciences, 14*(12), 1406. https://doi.org/10.3390/educsci14121406

Guyatt, G. H., Oxman, A. D., Vist, G., Kunz, R., Brozek, J., Alonso-Coello, P., Montori, V., Akl, E. A., Djulbegovic, B., Falck-Ytter, Y., Norris, S. L., Williams, J. W. L., Atkins, D., Meerpohl, J., & Schünemann, H. (2011). GRADE guidelines: 4. Rating the quality of evidence—study limitations (risk of bias). *Journal of Clinical Epidemiology, 64*(4), 407–415. https://doi.org/10.1016/j.jclinepi.2010.07.017

Hadi Pradana, P., Ketut Agustini, G., Dantes, G. R., & Sudatha, I. G. W. (2024). The urgency of digital literacy learning in educational units: Systematic literature review. *Child Education Journal, 6*(1), 25–33. https://doi.org/10.33086/cej.v6i1.6100

Hadi, M., Martel, C., Huayta, F., Rojas, R., & Arias, J. (2023). *Metodología de la investigación: Guía para el proyecto de tesis*. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú. https://doi.org/10.35622/inudi.b.073

Herwani, S., & Pasiningsih, P. (2023). Digital literacy: A new culture of learning in the era of digitalization through cyber pedagogy strategies. *IJTIMAIYA: Journal of Social Science Teaching, 7*(2), 151–160. https://doi.org/10.21043/ji.v7i2.22913

Ilbay Guaña, E. L. (2022). Estrategias para promover la alfabetización mediática en la era digital. *Bastcorp International Journal, 1*(1), 14–22. https://doi.org/10.62943/bij.v1n1.2022.19

Instituto Nacional de Estadística y Censos (INEC). (2024). *Tecnologías de la información y comunicación*. Quito, Ecuador: INEC.

International Telecommunication Union (ITU). (2020). *Global Cybersecurity Index 2020: Measuring commitment to*

cybersecurity. Geneva, Switzerland: ITU.

Johnson-Glenberg, M. (2018). Immersive VR and education: Embodied design principles that include gesture and hand controls. *Frontiers in Robotics and AI, 5*, 81. https://doi.org/10.3389/frobt.2018.00081

Kont, K. R. (2023a). Cyber literacy skills of Estonians: Activities and policies for encouraging knowledge-based cybersecurity attitudes. *Information and Media, 96*, 80–94. https://doi.org/10.15388/im.2023.96.67

Kont, K. R. (2023b). Information security awareness of librarians in the Baltic countries: A comparative analysis. *Baltic Journal of Modern Computing, 11*(3), 450–474. https://doi.org/10.22364/bjmc.2023.11.3.07

Kozyreva, A., Rustikova, G., Pirozhkova, T., Shelmenkov, V., & Belyavskiy, A. (2022). Legal support of information security of the individual in the conditions of digital transformation of society. *SHS Web of Conferences, 134*, 00043. https://doi.org/10.1051/shsconf/202213400043

Kritzinger, E. (2020). Improving cybersafety maturity of South African schools. *Information, 11*(10), 465. https://doi.org/10.3390/info11100471

Madanu, P., Reddy, G. K., & B. J., A. (2024). Enhancing cyber psychology literacy in the digital age through a service-learning approach for students in India. *Help: Journal of Community Service, 1*(3), 187–197. https://doi.org/10.62569/hjcs.v1i3.81

Magunje, C., & Chigona, W. (2024). Perceptions of school management on cyber threats: The case of resource-constrained schools in South Africa. *EPiC Series in Education Science, 6*, 53–65.

Malik, M. T., Nurhikmah, H., Azmi, M., & Kurniati, K. (2023). Educational innovation policy for improving digital literacy capabilities in higher education. *Al-Musannif, 5*(1), 63–74. https://doi.org/10.56324/al-musannif.v5i1.81

Mastam, N. M., Mokhtar, K., & Zaharudin, R. (2024). Bridging the digital divide in Malaysia: Enhancing digital literacy for inclusive students in educational systems. *Asia Pacific Journal of Youth Studies, 15*(2), 128–150. https://doi.org/10.56390/apjys2024.15.2.128

Mednikarov, B., Tsonev, Y., Nikolov, B., & Lazarov, A. (2023). Characteristics and components of the cyber hygiene as a subclass of cybersecurity in military environment and educational issues. *Strategies for Policy in Science and Education, 31*(2), 154–169. https://doi.org/10.53656/str2023-2-3-cha

Meiqi, S., Jiaqi, L., & Jia, L. (2024). Digital literacy in Africa: Exploring its relationship with infrastructure, policy, and social inequality. *African Journalism Studies, 44*(1), 1–225. https://doi.org/10.1080/23743670.2024.2329705

Ministerio de Telecomunicaciones y Sociedad de la Información. (2022). *Estrategia nacional de ciberseguridad del Ecuador 2022–2025*. Quito, Ecuador: MINTEL.

Naseer, M., Bibi, T., & Aziz, S. (2023). Exploring educational policies of Pakistan for media information literacy. *Human Nature Journal of Social Sciences, 4*(2), 212–222. http://hnpublisher.com

Nayyar, S., & Gupta, K. K. (2024). Cyber security awareness: Safeguarding the digital future in education. In *Digital narratives in education* (pp. 198–205). OrangeBooks Publication. Retrieved from https://www.researchgate.net/publication/383206159

Nzeakor, O. F., & Nwoke, C. N. (2024). A study of the pattern of digital hygiene and cyberattacks in Abia State, Nigeria. *Journal of Criminology and Security Studies, 3*(1), 298–316. Retrieved from https://www.researchgate.net/publication/385044155

Omidvar, N., & Tavakoli, M. (2023). Analysis of the rural digital literacy policy in Iran. *Journal of Research and Rural Planning, 12*(1), 95–109. https://doi.org/10.22067/jrrp.v12i1.2110-1028

Omojemite, M. D., & Cishe, E. N. (2024). The influence of cooperative learning strategy on social studies pre-service teachers' attitudes towards cybercrime prevention. *Journal of Social Studies, 20*(2), 75–90. https://doi.org/10.21831/jss.v20i2.76782

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Pérez García, E. A., Arellano Vega, A. I., & López Meraz, Ó. F. (2025). Formación docente en TIC: Convergencias, ausencias y tensiones entre la práctica y la política. Caso de la UASLP. *Revista Científica Kosmos, 4*(1), 462–483. https://doi.org/10.62943/rck.v4n1.2025.279

Piscikiene, I., Romeikiene, J., & Šustickienė, B. (2021). Cyber vulnerability in light of online learning reality. In *Society. Integration. Education: Proceedings of the International Scientific Conference, 5* (pp. 426–435). https://doi.org/10.17770/sie2021vol5.6367

Popoola, O. A., Akinsanya, M. O., Nzeako, G., Chukwurah, E. G., & Okeke, C. D. (2024). Exploring theoretical

constructs of cybersecurity awareness and training programs: Comparative analysis of African and U.S. initiatives. *International Journal of Applied Research in Social Sciences, 6*(5), 819–827. https://doi.org/10.51594/ijarss.v6i5.1104

Rasdiana, R., Mauludin, I., Yahya, A., Putri, D. E., Machrus, M. A., Marbun, M., Sholikhah, A. M., Sinusi, N. S., Fathonah, S., Salmayda, S., Pawartani, T., & Ridwan, A. (2024). Mediation of digital literacy in investigating the effect of school culture on teacher performance: Implication for educational policy. *Journal of Infrastructure, Policy and Development, 8*(12), 9117. https://doi.org/10.24294/jipd.v8i12.9117

Raut, S. D., Shinde, A. R., & Patil, M. K. (2022). Cyber security awareness: A movement of digital literacy towards making of Digital India. *IBMRD's Journal of Management & Research, 11*(2), 174–180. https://doi.org/10.17697/ibmrd/2022/v11i2/172617

Sen, A. (1987). *Commodities and capabilities*. Oxford University Press.

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. *Asian Journal of Shipping and Logistics, 37*(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001

Septanto, H., Rusmawan, U., Yuliadi, B., & Hidayatullah, A. (2024). Study of the role of digital literacy in mitigating the spread of online gambling as a popular cyber crime in Indonesia. *DIJEFA: Dinastic International Journal of Economics, Finance & Accounting, 5*(5), 5048–5054. https://doi.org/10.38035/dijefa.v5i5

Skarga-Bandurova, I., Kotsiuba, I., & Velasco, E. R. (2021). Cyber hygiene maturity assessment framework for smart grid scenarios. *Frontiers in Computer Science, 3*, 614337. https://doi.org/10.3389/fcomp.2021.614337

Sogalrey, F. A. M., Safitri, F., Tijow, M. A., Sembiring, D. A. K., & Risamasu, P. E. G. (2024). Digital literacy research in education: Trends and insights. *Jurnal Kependidikan: Jurnal Hasil Penelitian dan Kajian Kepustakaan di Bidang Pendidikan, Pengajaran dan Pembelajaran, 10*(3), 1169–1180. https://doi.org/10.33394/jk.v10i3.12490

Srivastava, A. K., Singh, A. V., & Som, S. (2024). Critical analysis of cybersecurity awareness programs in school education. *Library Progress International, 44*(3), 18282–182303.

Sterne, J. A., Hernán, M. A., Reeves, B. C., Savović, J., Berkman, N. D., Viswanathan, M., Henry, D., Altman, D. G., Ansari, M. T., Boutron, I., Carpenter, J. R., Chan, A.-W., Churchill, R., Deeks, J. J., Hróbjartsson, A., Kirkham, J., Jüni, P., Loke, Y. K., Pigott, T. D., … Higgins, J. P. (2016). Stratification of risk for hospital admissions for injury related to fall: Cohort study. *BMJ, 355*, i4919. https://doi.org/10.1136/bmj.i4919

Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy, 46*(3), 102282. https://doi.org/10.1016/j.telpol.2021.102282

Tello de la Torre, C., Perez, V., & Juan José, M.-N. (2021). Digital human assets and psycho-digital risks: Concept and recommendations. *Revista Venezolana de Gerencia, 26*(Special Issue 6), 12–28. https://doi.org/10.52080/rvgluz.26.e6.2

Terán, A., & Guevara Ruales, N. (2025, February 24). Rumbo a 2025: Perspectivas tecnológicas para Ecuador. *Revista Industrias*. https://revistaindustrias.com/rumbo-a-2025-perspectivas-tecnologicas-para-ecuador/

Tokan, K., Amin, M. E., Syaufi, A., & Mispansyah. (2024). Protecting digital society: Policies for criminalizing illegal smartphone applications through cyber law frameworks. *West Science Law and Human Rights, 2*(3), 1–12.

Ugwu, C., Kingston, C., Ani, C., Ezema, M., Asogwa, C., Ani, C., Ome, U., Obayi, A., Ebem, D., Atanda, A., & Ukwandu, E. (2022). Towards determining the effect of age and educational level on cyber-hygiene. In *Proceedings of the IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)* (pp. 1–6). IEEE. https://doi.org/10.1109/NIGERCON54645.2022.9803154

Universidad Internacional de Valencia. (2025, March 13). Ciberseguridad en Ecuador: Actualidad y mejores prácticas. Retrieved from https://www.universidadviu.com/ec/actualidad/nuestros-expertos/ciberseguridad-en-ecuador

Wang, C., & Si, L. (2024). The intersection of public policy and public access: Digital inclusion, digital literacy education, and libraries. *Sustainability, 16*(5), 51878. https://doi.org/10.3390/su16051878