VISUAL REVIEW | Vol. 18, No. 8, 2026 | ISSN 2695-9631

International Visual Culture Review / Revista Internacional de Cultura Visual

https://doi.org/ 10.62161/revvisual.v18.6485

DIGITAL SECURITY AND CYBERSECURITY IN JOURNALISM

Risks and challenges: The Cases of Ecuador and Perú

KRUZKAYA ORDÓÑEZ [1]
kordonez@utpl.edu.ec
LUIS-ROLANDO ALARCÓN-LLONTOP[2],
luis.alarcon@upn.edu.pe
ABEL SUING [3],
arsuing@utpl.edu.ec
LUIS ORDÓÑEZ PINEDA[4]
loordonez@utpl.edu.ec
[1,3,4] Universidad Técnica Particular de Loja, Ecuador
[2]Universidad Privada del Norte, Perú

KEYWORDS

Journalism
Cybersecurity
Digital security
Cyberviolence
Data protection

ABSTRACT

Journalists face a digital environment linked to cyberattacks, threats, data theft, and online extortion. This prompted a study in Ecuador and Peru to investigate the challenges journalists face and what cybersecurity measures they are implementing. The methodology is mixed, using a survey designed on the basis of Cybersecurity Strategies and Personal Data Protection Laws, and a supplementary interview. The results show greater pressure and vulnerability for journalism, and cybersecurity and data protection are becoming a structural dimension of journalism.

Recibido: 03/ 07 / 2026
Aceptado: 20/ 10 / 2026

1. Introduction

Digital security and cybersecurity require special attention because all activities, and in this case journalism, are closely linked to the digital world, a space in which large amounts of information are generated that require observation and investigation and through which journalists and people in general navigate. Therefore, identifying risks in the case of journalists becomes a fundamental action due to growing threats ranging from cyberattacks, with detection, inspection, and repair being important preventive processes. This also includes data theft, online harassment and extortion (Phillips, et. al. 2025), and even the manipulation of information, situations that affect "media freedom and the safety of journalists [who suffer] a dangerous regression in almost every region of the world." For Pauner Chulvi, this regression is accentuated:

> […] in non-democratic environments where media professionals face increased intimidation through the misuse of laws and measures taken by public authorities to discredit their work. […] The number of threats, digital espionage attacks, and pressure against them has increased in recent years, seriously damaging their working environment (2024, p. 190).

The digital risks faced by journalists begin with daily activities that rely heavily on messaging using systems such as computers and mobile devices, on which they rarely use security or data encryption systems, according to a survey conducted by Freedom House and the International Center for Journalists in Mexico City. Based on these results, it is recommended that studies be conducted in each territory to gauge the state of digital security and the incorporation of cybersecurity measures in order to take actions that contribute to "minimizing the vulnerability of journalists and bloggers who cover high-risk topics such as drug trafficking, organized crime, corruption, violence, abuses, and human rights violations." (Sierra, 2013, p.14).

Regarding human rights violations, a report published by the Latin American Observatory of Digital Threats (2025) highlights that in Ecuador in 2023 there were more than 300 cyberattacks, particularly against the news website Indómita Media, which publishes articles related to the deterioration of the human rights situation. These follow-up reports are carried out in Ecuador by Fundamedios, a foundation that has been recording a series of attacks, such as the presidential elections in the same year, in which 23 journalists and media outlets were attacked by digital swarms through a troll center:

> which tend to be activated at certain times, when they need to establish a narrative or attack an opposing message. They were activated in October 2019, during the coronavirus pandemic, to spread misinformation; during the release of former president Jorge Glas—convicted of corruption—in April 2022; during the national strike in June 2022 and [...] on the eve of the local elections, with a clear objective: to position Correísmo and attack those who go against its narrative construction (2022, p.12).

In Peru, the scenario is similar. The media, journalists, and strategic sectors (manufacturing, telecommunications, healthcare, and financial services) are no longer collateral victims, but primary targets of cybercriminals seeking to disrupt essential services and steal sensitive data. In this scenario, artificial intelligence (AI) has become a double-edged sword: "attackers use FraundGPT or WormGPT systems to create extremely realistic phishing emails, automate social engineering campaigns, and map attack surfaces" (Meza Capcha, 2025).

Furthermore, the situation is exacerbated by the fact that only 27% of the Peruvian population chooses a career related to cybersecurity and AI, compared to 31% of companies that face difficulties in the digital sphere due to a lack of professionals with skills in these areas, including media companies (Forbes, 2025).

Digital violence is spreading rapidly, with attacks on network infrastructure and the use of digital technology to harm individuals and organizations (Setyowati, 2023), actions from which the media and journalists are not exempt. It is therefore necessary for them to have a high level of

understanding of the importance of cybersecurity in order to avoid becoming targets of attacks and minimize risk.

With reference to this last point, Di Salvo (2022), in his work Information Security and Journalism, brings up the revelations made in 2013 by Edward Snowden that highlighted the serious implications of mass surveillance and digital threats to the safety of journalists and their sources.

Among the best-known threats is the sophisticated Pegasus spyware and surveillance software, "an application commonly known as spyware [installed on mobile phones] via a link that exploits vulnerabilities in the operating system and remains active in the background to enable remote spying" via cell phones or computers (Xataka, 2022). With this Israeli-made software, thousands of journalists and opponents around the world have been spied on by governments.

What Bradshaw and Howard refer to as cyber troops are conceptualized as "government, military, or political party teams committed to manipulating public opinion through social media" (2017, p. 3), a widespread and global phenomenon that responds to interests of political and economic dominance and, above all, power. According to the authors, digital attacks pursue objectives depending on the political regime, with some aimed at controlling public opinion.

In this sense, the risks and challenges for journalists are imminent, depending on how news is produced and disseminated in the global digital landscape, as documented by Joyanes Aguilar in his work dedicated to collecting "news of cyberattacks on citizens, organizations, and companies, and even critical facilities in countries such as chemical power plants, nuclear power plants, or factories of various kinds," topics that have become commonplace on the front pages of various media outlets, "not only in print but also on radio, television, and, of course, electronic media on the Internet" (2011, p. 15). Given this adverse scenario, journalism plays a fundamental role due to the information it generates. In addition, journalists have integrated digital devices and actions into their work, which means that their work focuses on thinking about the digital security of journalists, media, and sources.

Likewise, "new technologies not only enable commercial and state surveillance, but also offer new opportunities for users to protect themselves from surveillance" (Tsui and Lee, 2019) with actions such as data encryption. These actions, which are available to the general public, "raise questions about journalists' awareness and knowledge of how to use these tools to communicate privately and securely with sources, colleagues, and editors" (Tsui & Lee, 2019). Additionally, journalists state in the study published by Waters (2018) that vulnerability, real or perceived threats of mass government surveillance, has led to changes in the way they work, which hinders their work and impairs their communication with sources. It is important to recognize the extent to which journalists have digital freedom.

1.1. Cybersecurity and data protection

Cybersecurity in journalism has been studied academically and scientifically from different perspectives. In the region, the research by Ordoñez et al. (2024) on the legal landscape of data protection in relation to journalism and that of Ordoñez et al. (2024) on the strategies implemented by states to guarantee cybersecurity for the profession are particularly important. Other works have explored the issue of cybersecurity in relation to disinformation, which is seen as a threat to democracy (Rodríguez Fernández, 2020). Montañez Ramírez (2023) also addresses a study on preventive cybersecurity measures, as do Mendoza Michilot, Dejo Vásquez, and Najar-Ortega (2025), who investigate the role of the media in the face of computer fraud, dissemination, prevention, and literacy. These reviews confirm the importance of hearing the voices of journalists themselves. However, they have not been called upon to express their views on their own cybersecurity, which opens up an interesting and important gap to be filled by this research.

When talking about cybersecurity, a direct link is established with data protection, and these issues are crucial in the digital landscape because understanding and implementing the principles for using and utilizing emerging technologies ensures the security of digital assets and sensitive and confidential information.

> Cybersecurity aims to establish measures to prevent the execution of unauthorized processes whose effects could compromise an organization's computer system. In other words, it seeks to shield the technological infrastructures that support the operations of an organization that uses hardware and software (Hernández Bejarano & Baquero Rey, 2025, p. 6).

Cybersecurity involves strategies and measures to protect information, devices, and people from attacks, breaches, and information theft. This action leads to the establishment of principles such as authentication and access control, encryption and threat detection, measures and practices designed to protect cloud resources from unauthorized access, data leaks, and other malicious activities (Tiwari, et al., 2024).

Emerging technologies are incorporated into this process: AI and blockchain, which drive growth and have significant strengths in "continuous threat analysis for anomaly detection, fraud elimination, and predictive modeling of cyber events" that goes beyond "reactive compensation and focuses on proactive risk reduction and automatic claims processing" (Viji Gripsy, et al. 2026).

But security is not only focused on protection from attacks; it also focuses on defending the rights of individuals, journalists, and their networks, as well as freedom of expression. This last point is questionable because some states have absolute control over networks and data.

From a legal standpoint, the cybersecurity of journalists in both Andean countries covered by this study is protected by laws aimed at the general protection of personal data. Enacted in 2011, Law No. 29733, the Personal Data Protection Law (LPDP) in Peru, regulates the issue for all citizens without distinction and, by extension, for journalists (Congress of the Republic of Peru, 2011). The law includes regulations with measures that have been implemented gradually, and in its 15 years of existence, it has undergone some amendments, most of which have been in line with the accommodation of progressive digital capabilities. A decade later, Ecuador approved the Organic Law on Personal Data Protection, guaranteeing citizens the right to control their personal information by extending its regulation to the collection and use of data, establishing principles and rights regarding access, rectification, and deletion, and obligations for those responsible for processing, applying the Regulation issued three years (2023) after the law came into force.

Given this context, this research aims to investigate the risks and challenges journalists face in the face of attacks and cyberviolence, and what cybersecurity measures they are implementing with regard to equipment and data. The results will serve not only to establish a frame of reference on the issue, but also to enable the journalistic community itself, as well as the government, academia, and civil society organizations, to discuss the current situation and propose integrated improvements.

2. Methodology

The research is based on the socio-critical paradigm, which combines quantitative and qualitative perspectives, marking the evolution of the latter beyond the exclusively quantitative (Finol de Franco & Vera Solórzano, 2020). The approach is therefore mixed: it merges the aforementioned perspectives, allowing them to interact and enhancing them (Arispe et al., 2020). From a quantitative perspective, the descriptive scope focused on identifying, describing, and analyzing the characteristics of a phenomenon (Hernández-Sampieri & Mendoza Torres, 2023). Qualitatively, the phenomenological typology involved investigating this phenomenon from the subjects' experience (Castillo, Romero & Mínguez, 2022). The general design is non-experimental and cross-sectional, as there was no intervention in the study variables at any time (Chuquiruna & Benites, 2019). The specific design was mixed, quantitative with qualitative output to better address a problem (Creswell, 2014; Cabrera, 2023). The specific type of mixed design was sequential explanatory, which is used when the researcher has a general idea of the phenomenon and seeks to delve into possible causal aspects (Barreto & Lezcano, 2023).

The unit of analysis, "an abstract/theoretical/tautological concept representing an analytical category, not a specific case," which forms a trilogy with the unit of observation and the unit of information (Barriga & Henríquez, 2011, p. 64), was the group of Ecuadorian and Peruvian

journalists. This represents a non-finite population, given the lax characteristics of the exercise in general. For the study, official data from two recognized associations in both countries were used, provided by both the Communication Council of Ecuador (2025) and the College of Journalists of Peru (2025): 983 in the first case and 11,696 in the second. The samples were non-probabilistic for convenience and criteria, respectively close to the researchers and under viable selection guidelines (Benites & Villanueva, 2015). The inclusion criteria were: 1) being a fully practicing journalist, 2) representing a media outlet directly or indirectly, and 3) having independence from functions that could pose conflicts of interest with the profession. The exclusion criteria were: 1) being subject to disciplinary or administrative sanctions by any professional association, and 2) being the author or co-author of studies similar to this one.

The sample consisted of 358 journalists: 203 from Ecuador and 155 from Peru. No distinction was made between genders in the data collection, as the research focused on the profession itself.

The quantitative technique used to collect data was a survey, which, in the words of Wilson et al. (2024), "seeks to generate practical data that informs and promotes educational practices, policies, and future research" (p. 1389). The instrument was an online questionnaire, via Google Forms, which is valid, modern, and useful in these times (Arias, 2021). The instrument consists of 12 questions grouped into thematic blocks: a) Cyberviolence attacks, b) Knowledge and challenges with cybersecurity, c) Knowledge and implementation of the Personal Data Law, d) Treatment of sensitive information. The instrument was based on Cybersecurity Strategies and the following laws: Peru's Data Protection Law, No. 29733; and Ecuador's Organic Law on Data Protection (May 21, 2021).

There were two versions of the same instrument that allowed for comparisons validated in content by the judgment of three experts, and criterion validity was achieved—the original shares features with similar instruments—as well as construct validity—it is supported by a broad theoretical basis. After applying a pilot test to 12 subjects with characteristics similar to the population, it was subjected to a reliability test for consistency using Cronbach's alpha, which gave an index greater than 0.7, acceptable according to the literature.

The qualitative section was based on the interview, followed by the survey, a technique that relied on open conversation with specific objectives (Armijo et al., 2021); and particularly useful in social science and humanities research to expand on a researched topic (Lopezosa, Codina & Freixa, 2022). For this research, the interview guide set three anchor questions that revolved around: 1) safeguarding the confidentiality of information from sources; 2) measures taken to protect the personal data of sources, collaborators, and people involved in journalistic work; and 3) the implementation of measures to prevent the loss, unauthorized access, or misuse of sensitive data.

Descriptive statistics were used to analyze the information obtained from the quantitative phase, such as measures of position, central tendency, and dispersion (Armijo et al., 2021). To analyze the qualitative phase, a narrative analysis approach was followed (Arispe et al., 2020). Regarding the dimensions and categories of analysis, applying triangulation strategies, as required for mixed studies, the data were integrated, which allowed for discussion of the findings and drawing of conclusions.

The study complies with the ethical aspects prescribed in the three principles of ethics in research with human subjects: 1) respect for persons, respecting their autonomy and self-determination to decide whether or not to collaborate with the study; 2) beneficence, or non-maleficence, participation does not involve any risk of harm; and 3) justice, as the selection of participants was as equitable as possible in terms of origin, social strata, gender, etc. (Álvarez Viera, 2018).

2. Results and Discussion

After applying the methodology and refining the results, a comparative analysis of the information collected was carried out, applying descriptive statistics with measures of position and central tendency represented by the mode (most frequent category) and the measure of dispersion by

absolute and relative count. The quantitative analysis was applied by grouping the questions into four thematic blocks (questions 1 to 12). It was complemented by a qualitative analysis of the open-ended interview (questions 13, 14, and 15) to gather the journalists' opinions.

The initial results of the count identified that hybrid media (traditional and digital) predominate in this study, with 119 (58.62%) in Ecuador and 97 (62.58%) in Peru, while digital natives accounted for 84 (41.38%) and 58 (37.42%) respectively. This shows that journalists' spaces for expression continue to recognize the coexistence of traditional and digital media as channels for amplifying information, validating their actions and credibility in the environment in which they operate. Anonymization was applied for security reasons.

Once the type of media was identified, the thematic analysis was organized into four blocks. The first category of study is cyberviolence, to account for the attacks and threats faced by journalists in Ecuador and Peru (Table 1). The results indicate that in Ecuador there is a greater perception of all options (48%)—digital attacks, personal data breaches, information theft, and extortion—compared to Peru (46%).

Table 1. Cyberviolence registry

Category 1: Registration	Ecuador		Perú	
	F	%	F	%
Digital attacks	47	23%	46	30%
Personal data breach	28	14%	12	8%
Information theft	16	8%	16	10%
Extortion	15	7%	10	7%
All options	97	48%	71	46%
	203	100%	155	100%

Source: Own elaboration.

Among the types of digital attacks, the most commonly reported in Ecuador are threats (37.9%), followed by data theft (30.5%). This precision allows for the identification of specific attacks associated with intimidation, extortion, or loss of information; the latter considered a valuable digital asset in the field of journalism. In Peru, the results indicate that the category "none" (27.1%), followed by blockages (25.8%), results from a lower perception and identification of digital attacks in relation to the higher perception and actual incidence of attacks recorded in Ecuador. This suggests greater exposure of Ecuadorian journalists or, alternatively, a higher level of awareness and ability to classify digital attacks, compared to a lower perception or identification of attacks by Peruvian journalists. This does not necessarily mean that incidents do not occur, but rather that there are gaps in perception, knowledge, or reporting mechanisms applied in newsrooms.

Table 2. Type of digital attack

Category 1: Type	Ecuador		Perú	
	F	%	F	%
Threats	77	37,9%	35	22,5%
Data theft	62	30,5%	35	22,5%
Blocking	45	22,1%	40	25,8%
Attempted attacks	6	2,9%	3	1,9%
None	13	6,4%	42	27,1%
	203	100%	155	100%

Source: Own elaboration.

The second category of analysis examines the level of cybersecurity awareness (Table 3) and the challenges posed by the digital transformation era in different fields of professional practice (Table 4). Specifically, in the field of journalism, cybersecurity is presented as a technical and legal element that contributes to digital security, as opposed to information processing. "A clear example of this is the 2016 publication of a journalistic investigation entitled 'Panama Papers,' in which private databases were used to reveal information of public interest" (Ramírez, 2020, p. 48). From this perspective, based on the results obtained, it is important to have a high level of

knowledge related to cybersecurity, considering the levels of digitization currently applied by the media.

With this suggestive assessment, the results indicate that journalists in both countries claim to have knowledge on the subject (Table 3). However, among the main challenges identified (Table 4) is the lack of continuous and specialized training in Ecuador (47.78%) and Peru (36.77%), which in some cases limits effective management for the prevention of digital risks that arise with: government surveillance and persecution of organized crime, which in Ecuador and Peru are recorded at 21%, evidencing a shared concern.

Another challenge observed and reported in both countries, with 21%, is technological management that is not necessarily adequate and appropriate for every type of situation, reflecting technical limitations, insufficient infrastructure, and a lack of specialized personnel in both contexts.

On the other hand, journalists were asked if they had access to resources and clear, timely information that would enable them to learn about cybersecurity. The data show that there is greater difficulty in Peru (9%) than in Ecuador (4.93%). The results determine the need to organize and establish interdisciplinary teams, to a greater extent in Peru (10.97%) than in Ecuador (4.43%). This leads to the conclusion that in Peru there is a high level of concern about integrating specialized technical professionals and strategists in cybersecurity management, as well as professionals specializing in law and data protection.

Across both countries, there is concern mainly about the surveillance of organized crime and the lack of adequate training and technological management, which in turn become significant challenges, reinforcing the notion that cybersecurity is not an individual problem but a structural phenomenon that requires the integration of technical and organizational capabilities. These results partially confirm that lack of training is not the main or only challenge facing the journalism sector.

These challenges are related to actions that must be implemented by the media institutions themselves. In this regard, from the perspective of shared responsibility, compliance is important as a theory that requires institutions to adopt preventive measures, including education and training in technical areas related to information processing. Naturally, in this vein, the role of the State in repressing possible attacks on journalistic activity is highlighted as a third assumption.

Table 3. Cybersecurity Knowledge

Category 2: knowledge	Yes		No	
	F	%	F	%
Ecuador	146	71,92%	57	28,08%
Perú	121	78.06 %	34	21,94%

Source: Own elaboration

Table 4. Challenges faced

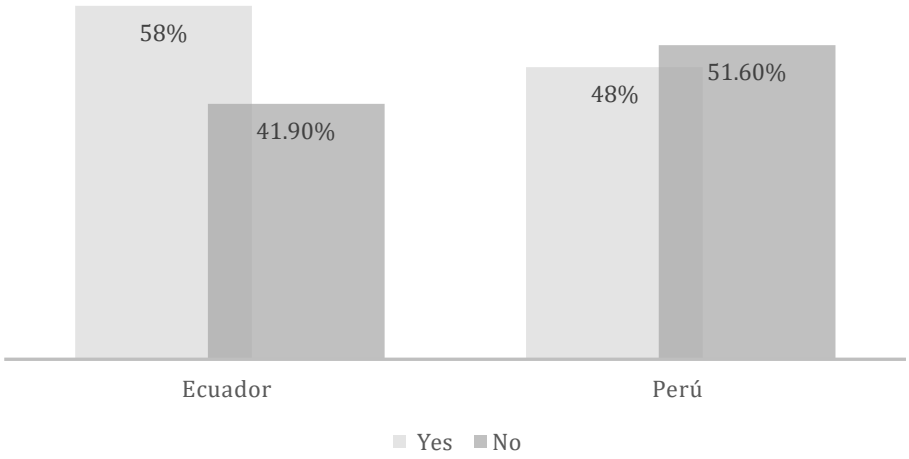
Categoría 2: Challenges	Ecuador		Perú	
	F	%	F	%
Lack of training	97	47,78	57	36.77
Surveillance and prosecution of organized crime	44	21,67	34	21,94
Lack of adequate technological management	43	21,18	33	21,29
Access to information on cybersecurity	10	4,93	14	9,03
Need for organization with interdisciplinary teams	9	4,43	17	10,97

Source: Own elaboration.

The third category relates to knowledge of the Organic Law on Personal Data Protection (LOPDP-Ecuador and LPDP-Peru). The results indicate that opinions are relatively divided regarding knowledge of the law (Figure 1). In Ecuador, 58% are aware of the law, compared to 41.9% who are unaware. However, it is striking that ignorance prevails in Peru, with 51.6% of journalists unaware of the law compared to 48% who are aware, considering that the Personal

Data Protection Law No. 29733 was enacted in 2011. In this regard, it should be noted that the supervisory authority has an important role to play, as it is responsible for "promoting awareness and advocacy campaigns on personal data protection" (Article 33). The regional gap is almost 10 percentage points in favor of Ecuador.

Figure 1. Awareness of the Data Protection Act



Source: Own elaboration.

Continuing with the inquiry, questions were asked about the implementation of Personal Data Protection Laws in media companies (Table 5). The results, based on the ordinal Likert scale, evaluate implementation actions in accordance with the provisions of the law. The data reveal a consensus in the responses of journalists from Ecuador and Peru, with the percentages of those who strongly agree and agree combined approaching 100%. This trend represents averages between 4.0 and 4.58 for "agree" and "strongly agree" responses, with a low standard deviation. This pattern consolidates acceptance of the implementation of the LOPDP-Ecuador and LPDP-Peru and rules out significant ambivalence, as no averages close to the neutral point of 3 were observed.

Among the priority issues for Ecuadorian journalists is the implementation of personal data protection policy (68.47%), with Article 13 mentioning the publication of privacy policies as a way of complying with the duty to inform the data subject, ensuring clarity in data processing. This is in line with the second most frequently mentioned issue, training in data management, as a direct measure for security and regulatory compliance (63.05%).

Aspects of the LODP	Strongly agree EC	Agree EC	Disagree EC	Strongly agree PE	Agree PE	Disagree PE
Data Protection Policy	68.47%	30.05%	1.48%	45.81%	52.90%	1.29%
Information Security Policy	60.59%	38.92%	0.49%	49.03%	49.68%	1.29%
Data Use Consent	55.67%	38.42%	5.91%	43.23%	54.19%	2.58%
Information Clauses	55.17%	38.42%	6.40%	43.87%	47.74%	8.39%
Complaint Filing	50.74%	42.86%	6.40%	42.58%	52.90%	4.52%
Technical Measures	61.08%	37.44%	1.48%	41.29%	53.55%	5.16%
Data Protection Clauses	49.26%	46.80%	3.94%	40.00%	50.97%	9.03%
Notifications	54.19%	41.38%	4.43%	40.65%	53.55%	5.81%
Data Impact Assessment	50.74%	44.83%	4.43%	40.65%	55.48%	3.87%
Data Management Training	63.05%	34.98%	1.97%	47.10%	49.03%	3.87%

Table 5. Comparative table of implementation of LOPDP (Ecuador) and LPDP (Peru)
Source: Own elaboration.

In Peru, the results are geared toward implementing measures to assess the impact of data processing (55.48%). Article 13 states that policies must include mechanisms for evaluating processing in order to protect the rights of the data subject. Likewise, 53.55% of journalists agree with the adoption of technical, organizational, and security measures to protect data. Article 39 of the LPDP describes access controls, activity logs, and technological protection mechanisms that overlap with the criterion of security breach notifications, which includes the obligation to take measures in the event of risks or vulnerabilities in data processing (Article 16).

In relation to questions 11 and 12, which inquired about the tools and procedures used by journalists to protect sensitive data and information, the results of the comparative analysis of 10 free-choice response alternatives indicate that hardware- and software-based security in Ecuador is carried out using external hard drives to back up sensitive information, combined with authentication and control (secure passwords) and not answering calls from unknown numbers. These tools, combined with procedures such as source verification, which is considered a priority, followed by not opening strange emails and constantly changing passwords, confirm that there is a significant parallel between cybersecurity knowledge and risk perception. The perception of digital risk is latent because these teams are vigilant about government monitoring and the prosecution of organized crime (22%), a finding that results from the analysis of the cyberviolence category. Added to this is concern about possible loss or theft of information.

Table 6. Comparative table of cybersecurity tool and procedure implementation

Protective equipment	Ecuador	Perú
Passwords / Secure Keys (Authentication)	**69**	**59**
Backup on External Drives / Backup	58	40
Do not answer calls/Unknown numbers (Awareness)	**29**	**16**
Access Control/Limit Access	14	3
Cloud storage	**14**	**3**
Proxy server with two-step authentication and vulnerability scanning	10	1
Encryption	**4**	**24**
Firewall application	4	8
Others	**2**	**0**

Procedures		
Source verification	**77**	**26**
Do not open strange emails/links (phishing)	56	46
Control of access to information (permissions)	**32**	**32**
Installation of antivirus software	12	4
Analysis of email origin	**11**	**30**
Double layer of security	8	6
Avoid contact with external networks	**7**	**11**

Source: Own elaboration.

In Peru, software and hardware security measures are combined with the use of external hard drives for data backup, authentication and access control (secure passwords), and encryption (data encryption on computers) applied by media outlets and journalists to enhance the protection of sensitive data and information (Table 6). Among the procedures for protecting sensitive data and information, as in Ecuador, Peru highlights the action of not opening strange emails and controlling access to information (permissions), with a third step being the verification of sources.

It is worth noting that in both Ecuador and Peru, advanced security tools such as working with a proxy server with two-step authentication and vulnerability scanning, as well as encrypted cloud backup with endpoint encryption, firewall application, and shared access limitation, have a lower registration rate. This shows that procedures with security tools have a basic connotation. However, it should be noted that source verification is as important as access control, suggesting that journalists integrate data security with their essential work of protecting sources.

Finally, this section concludes with the qualitative perception of journalists (open questions 13, 14, and 15). The qualitative analysis offers relevant findings in both countries. With regard to confidentiality strategies, in addition to verifying sources, an essential first step in journalistic practice, and basic security controls, they resort to anonymization and data minimization, especially in Peruvian journalism teams, which favors the confidentiality of sources' identities. In addition, they intentionally omit personal data and share sensitive information as a protection mechanism. These practices reduce the risk of compromising sources' information and documents, as well as tracking their digital footprint or paper trail. These actions are applied in hostile or high-surveillance scenarios.

An important point to note is that in both countries, advanced security mechanisms are marginal, despite the risks to which they say they are exposed and the need, indicated at least by journalists in Peru, to adopt adequate technical and organizational measures.

Likewise, journalists in Ecuador and Peru acknowledge that they do not apply formal strategies for the protection of sensitive data, limiting themselves to controlling information on a personal basis based on individual or team trust.

The qualitative results as a whole present a positive scenario that translates into a high level of awareness of the importance of personal data protection, source confidentiality, and the misuse of sensitive data and documents. This reflects a level of digital maturity combined with traditional practices that in some cases limit the expansion of cybersecurity in the field of journalism.

3. Conclusions

It is important to note that, in the quantitative and qualitative data analyzed, journalists in Ecuador and Peru who work in hybrid media such as digital media are exposed to risks related to digital attacks, cyberviolence, and vulnerabilities related to equipment and data.

In Ecuador, journalists have greater digital exposure compared to their peers in Peru: this result confirms that journalists in Ecuador face greater cyberviolence than in Peru. The evidence is the reporting of threats, data theft, and attacks associated with intimidation and extortion or loss of information, suggesting a context of greater pressure and vulnerability for the practice of journalism. Given this scenario, cybersecurity and its direct relationship with data protection become a structural dimension of journalism, especially in environments marked by risks

associated with surveillance and systematic persecution derived from public exposure, which set the tone for the implementation of digital security protocols.

With regard to specialized cybersecurity training, which is seen as a challenge in both countries, journalists and media outlets acknowledge the absence of a culture and processes for continuous and specialized training, which leads to self-taught and informal learning. This reality is exacerbated by the scarcity of institutional resources and the low level of cybersecurity knowledge, which in some cases limits effective management for the prevention of digital risks, making these issues central concerns in journalism.

On the other hand, with regard to knowledge and application of personal data protection laws, it is striking that Peruvian journalists remain largely unaware of these laws, considering that the LPDP was approved in 2011, which represents an advantage over Ecuador, whose LOPDP was issued in 2021. However, it should be noted that journalists in both countries are aware of the inclusion of data protection policies, technical measures, impact assessment, and data management training, regulations that are in line with hardware and software cybersecurity measures, as well as the procedures they implement, including source and document verification and access control, which suggests that Ecuadorian journalists value data security and source protection. In Peru, these appropriation procedures are also considered relevant, although the trend there is toward equipment security and protection. Finally, the implementation of advanced security procedures is suggested to reduce risks and vulnerabilities in the practice of journalism.

This research finds its strengths both in the choice of topic addressed, which is of utmost importance because it deals with guarantees first and then practices to uphold those guarantees with regard to the practice of journalism itself in the realm of digital security at a time when digitality itself is perhaps experiencing its most intense moments; as well as in offering an initial methodology that aspires to a mixed approach, from a sociocritical paradigm, based on a quantitative methodology at the outset, to be completed with qualitative contributions scrutinized on the protagonists of the journalistic work itself, the journalists, in an interesting sample of the countries studied. However, the study acknowledges limitations, such as the impossibility of generalizing the results obtained 100% due to having worked with a non-probabilistic sample, or the absence of other techniques, such as documentary analysis, for example, which could have cross-referenced the information provided by journalists and thus contributed to a more comprehensive reading of the issue. It is up to other researchers to overcome these points and continue to contribute to the lines of research that emerge from digital security in general and journalistic cybersecurity in particular.

4. Acknowledgments

This text was written within the framework of the lines of research maintained by the Research Group on Communication and Audiovisual Culture at the Technical University of Loja.

References

Alvarez Viera, P. (2018). Ética e investigación. *Boletín Redipe* [Internet], 7 (2), 122-149. https://goo.su/QeaMUG

Arias Gonzales, J. L. (2021). *Métodos de investigación on line. Herramientas digitales para recolectar datos*. Enfoques Consulting EIRL.

Arispe Alburqueque, C. M., Yangali Vicente, J. S., Guerrero Bejarano, M. A., Rivera Lozada de Bonilla, O., Acuña Gamboa, L. A., & Arellano Sacramento, C. (2020). *La Investigación científica. Una aproximación para los estudios de posgrado.* Universidad Internacional del Ecuador.

Armijo, I., Aspíllaga, C., Bustos, C., Calderón, A., Cortés, C., Fossa, P. et al. (2021). Manual de metodología de la investigación 2021. Universidad del Desarrollo, 2021.

Asamblea Nacional del Ecuador (2021, 26 de marzo). *Ley Orgánica de Protección de Datos Personales.* Documento de acceso abierto en línea. https://short.do/kiLtUC

Barreto, J., & Lezcano, A. (2023). Análisis y fundamentación de los diseños de investigación: explorando los enfoques cuantitativos, cualitativos y mixtos basados en Creswell & Creswell (2018). *Revista Unida Científica, 7*(8), 110-117. https://goo.su/HWbRfH

Barriga, O.A. & Henríquez A., G. (2011). La relación Unidad de Análisis-Unidad de Observación-Unidad de Información: Una ampliación de la noción de la Matriz de Datos propuesta por Samaja. *Revista Latinoamericana de Metodología de la Investigación Social,* (1), 61-69. https://goo.su/zQJUEqg

Benites Romero, S. H., & Villanueva López, L. (2015). *Retroceder investigando ¡Nunca! Rendirse con la tesis ¡Jamás!* Fondo Editorial Cultura Peruana E.I.R.L.

Bradshaw, S. & Howard, F. (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. University of Oxford. https://goo.su/OlaCrK

Cabrera, P. (2023). Nueva organización de los diseños de investigación. *South American Research Journal, 3*(1), 37-51. https://doi.org/10.5281/zenodo.8050508

Castillo López, M., Romero Sánchez, E., & Mínguez Vallejos, R. (2022). El método fenomenológico en investigación educativa: una revisión sistemática. *Latinoamericana de Estudios Educativos, 18*(2), 241–267. https://doi.org/10.17151/rlee.2023.18.2.11

Chuquiruna León, A. & Benites Romero, S. (2019*). Investigue. Usted también puede. Reseña de trabajos que cambiaron el mundo.* Imprenta Hesse EIRL.

Colegio de Periodistas del Perú (08 de febrero de 2025). *Data total colegiados a nivel nacional*. Documento respuesta ante pedido específico.

Congreso de la República del Perú. (2011, 03 de julio) Ley Nº 29733. Ley de Protección de datos personales. Diario Oficial El Peruano. https://goo.su/EBxMR

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.

Di Salvo, P. (2022). Seguridad de la información y periodismo: mapeo de un campo de investigación naciente. *Sociology Compass, 16*(3). https://doi.org/10.1111/soc4.12961

Finol de Franco, M. & Vera Solórzano, J.L. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. *Mundo Recursivo, 3*(1), 1-24. https://goo.su/JJp2

Forbes (8 de mayo de 2025). *El 76% de empleadores en el mundo no encuentran talento en IA y ciberseguridad.* https://goo.su/BezBRQe

Fundamedios (Publicación 2 de agosto de 2022). *Un troll center vuelve a hacer de las suyas en el país*. https://goo.su/7co19

Hernández Bejarano, M. & Baquero Rey, L. E. (2025). *Fundamentos de la ciberseguridad.* Escuela Tecnológica Instituto Técnico Central. https://goo.su/UhKlFd

Hernández-Sampieri, R. &Mendoza Torres, C. (2023). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill.

Joyanes Aguilar, L. (2011). Introducción. Estado del arte de la ciberseguridad. *Cuadernos de estrategia*, (149),11-46. https://goo.su/fyKw12C

Lopezosa, C.; Codina, L. & Freixa, P. (2022) *ATLAS.ti para entrevistas semiestructuradas: Guía de uso para un análisis cualitativo eficaz*. DigiDoc Research Group / Pompeu Fabra University, https://goo.su/tsaLBkg

Meza Capcha, E. (27 de agosto de 2025). *Ciberataques en Perú superan los 748 millones de intentos en lo que va del 2025*. Infobae. https://goo.su/2Z6gZX

Mendoza Michilot, M., Dejo Vásquez, M., & Najar-Ortega, R. (2025). El papel de los medios frente al fraude informático. Difusión, prevención y alfabetización. Contratexto, 43, 221-248. https://doi.org/10.26439/contratexto2025.n43.7160

Montañez Ramírez, C. (2023). *Medidas preventivas de ciberseguridad que debe tener un adulto mayor en Colombia para acceder a los servicios de internet y sus servicios [Proyecto de Grado para optar el título de Especialista en Seguridad Informática,* Universidad Nacional Abierta y a Distancia]. Repositorio institucional de UNAD. https://goo.su/OkW5pn1

Observatorio Latinoamericano de Amenazas Digitales (2025). *En la mira: seguridad y principales amenazas digitales en América Latina.* OLAD https://goo.su/zHSTH57

OECD (2018). Manual Oslo 2018 Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition. https://doi.org/10.1787/9789264304604-en

Ordóñez, K., Suing, A., Punín, M. I., Carpio, L. (2024). Ciberseguridad y Periodismo: Estrategias para garantizar la seguridad de la información. Revista Ibérica de Sistemas e Tecnologías RISTI. 382-392. https://short.do/9mXqzS

Ordóñez, K., Puertas, L., Suing, A. (2024). *Los datos sus usos e implicaciones en espacios democráticos.* Revista Ibérica de Sistemas e Tecnologías. RISTI, 102-114. https://short.do/DosHwl

Pauner Chulvi, C. (2024). La protección de las fuentes periodísticas en la era digital y el impulso regulatorio de la Unión Europea. *Teoría y Realidad Constitucional*, (54), 189-216. https://goo.su/XFoy

Phillips, S., Hansen, M., Matsilele, A. (2025). Análisis de alcance: El panorama de riesgos digitales y soluciones de ciberseguridad para periodistas. En N. Clarke & S. Furnell (eds.) Aspectos humanos de la seguridad y garantía de la información. *HAISA 2024. IFIP Avances en Tecnologías de la Información y la Comunicación, 721.* Springer, Cham. https://doi.org/10.1007/978-3-031-72559-3_3

Ramírez, D. (2020). *La inherente tensión entre los datos personales y el periodismo*. En: INAI. (eds.) Periodismo y la protección de los datos personales (págs. 43-61). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://short.do/hwHV9Z

Rodríguez Fernández, L. (2025) Desinformación y Ciberseguridad: Impacto en las organizaciones españolas 2025. En Sierra, J., Rodrigo Martín, J. , Muñoz de Luna, A. (2025). Realidades conectadas:Medios, cultura y sociedad en la era digital, 309, McGrawHill. https://short.do/XY1RCn

Setyowati, M. S, Desila Utami, N., Habib Saragih, A. & Hendrawan, A. (2023). Strategic factors in implementing blockchain technology in Indonesia's value-added tax system. *Technology in Society*. *72*, e102169. https://doi.org/10.1016/j.techsoc.2022.102169

Sierra, J. L. (2013). *Seguridad Digital y Móvil para periodistas y Blogueros. Resultados de la encuesta entre periodistas y blogueros mexicanos*. Freedom House y ICFJ Knight International Journalism Fellow. https://goo.su/DN27Yjt

Tejero, J. (2021) Técnicas de investigación cualitativa en los ámbitos sanitario y sociosanitario. Ediciones de la Universidad de Castilla – La Mancha. https://goo.su/0zs2j

Tiwari, M., Tiwari, T., Ticku, A., Dadhwall, H. & Singh, T. (2024). Metodologías y Desafíos de las Técnicas de Ciberseguridad en el Entorno de Computación en la Nube. *ICIMMI '23: Actas de la 5ª Conferencia Internacional sobre Gestión de la Información e Inteligencia Artificial*, (182), 1 – 7. https://doi.org/10.1145/3647444.3652492

Tsui, L. & Lee, F. (2019). Cómo los periodistas comprenden las amenazas y oportunidades de las nuevas tecnologías: Un estudio de las mentalidades de seguridad y sus implicaciones para la libertad de prensa. *Periodismo, 22* (6), 1317-1339. https://doi.org/10.1177/1464884919849418

Viji Gripsy, J., Lukose, B., Sheeba, L., Mesia Dhas, JT, Jayasree, R. & Brindha, NV (2026). Mejora del seguro de ciberseguridad a través de IA y Blockchain para una gestión proactiva de riesgos. En M. Alawida, A. Almomani & M. Alauthman (Eds.), *Innovaciones y marcos de seguros de ciberseguridad en la era de la IA* (págs. 349-376). Publicaciones científicas globales IGI. https://doi.org/10.4018/979-8-3373-1977-3.ch012

Waters, S. (2018). Los efectos de la vigilancia masiva en las relaciones de los periodistas con fuentes confidenciales: Un estudio comparativo constante. *Periodismo Digital, 6*(10), 1294–1313. https://doi.org/10.1080/21670811.2017.1365616

Wilson, A. B., Bay, B. H., Byram, J. N., Carroll, M. A., Finn, G. M., Hammer, N., Hildebrandt, S., Krebs, C., Wisco, J. J. & Organ, J. M. (2024). *Journal recommended guidelines for survey-based research. Anatomical Sciences Education, 17*(7), 1389–1391. https://doi.org/10.1002/ase.2499

Xataka (2 de mayo de 2024) *Qué es Pegasus: cómo se infecta, qué puede hacer y cómo detectarlo*. https://goo.su/fntY