Would you Steal me a Like? Undercover Operations in Digital Environments within the Peruvian National Police

Carlos Aliaga[1], Alexis Ravello[2], Darlys Sares[3] and Marcelo Leon[3,*]

[1]Escuela de Posgrado de la Policia Nacional del Peru, Lima, Peru
[2]Centro de Altos Estudios Nacionales, Lima, Peru
[3]Universidad Ecotec, Samborondon, Ecuador

Abstract

The study analyzed how undercover police operations are carried out within digital environments in the fight against organized crime in the city of Metropolitan Lima. The approach used was qualitative and the hermeneutical phenomenological method. Data saturation was achieved with 16 participants, including active police officers and experts in digital evidence analysis in organized crime investigations. The study employed interviews and documentary analysis as data collection techniques. The data were analyzed using discursive analysis and the technological tool ATLAS.ti. Undercover police operations in digital environments involve officers adopting fictitious digital identities and fabricated personas to infiltrate criminal organizations. "Based on the results, we conclude that undercover police operations in digital environments are effective in combating organized crime tools, such as specialized hardware and software, are pillars in the effectiveness of operations; the police profile personnel assigned to operations must integrate values, advanced cybersecurity skills, digital infiltration techniques and in- depth knowledge of the regulatory framework; the legal framework that regulates operations must be permanently updated, under agile management perspective; it es necessary to work with standardized processes to deliver valid evidence in criminal proceedings; The creation of the Police specialty Computer Engineering es urgent, to have officers professionally prepared for combat organized Crime in a digital world that es updated quickly and relentlessly.

Keywords

Undercover police operations, Digital environments, Organized crime, Special investigation techniques, Digital evidence

1. Introduction

Criminal organizations (COs) increasingly and efficiently use technology and digital environments [1]. In addition to their enormous availability of technological resources and scarce bureaucracy, COs have been achieving high degrees of impunity and capillarity, both at the global [2], regional, and local levels. In response, the signatory states of the United Nations Convention against Organized Crime, United Nations [3] have incorporated the so-called special investigation techniques into their legislation. Undercover operations in digital environments, hereinafter (OED), are one of those that require the greatest resources due to the constant growth of cybercrime [4, 5, 6].

In the fight against COs, Law enforcement officials face challenges in gathering evidence that can be used as admissible proof in criminal proceedings [7]. This problem becomes more complex when it comes to crimes in digital environments, because their attacks are covert, anonymous, and compartmentalized, which makes the work of law enforcement difficult [8].

According to the General Office of Planning and Budget of the Ministry of the Interior of Peru [9], in 2022, cybercrimes were the most frequent and showed an alarming increase of 277% compared to 2019, as shown in table 1

ICAIW 2025: Workshops at the 8th International Conference on Applied Informatics 2025, October 8–11, 2025, Ben Guerir, Morocco
*Corresponding author.
caliagaa1820@gmail.com (C. Aliaga); aravellojoo@yahoo.com (A. Ravello); darlyssares@hotmail.com (D. Sares); marceloleon11@hotmail.com (M. Leon)
0000-0002-3270-3507 (C. Aliaga); 0000-0003-4001-0142 (A. Ravello); 0009-0000-3488-2951 (D. Sares); 0000-0001-6303-6615 (M. Leon)

Table 1
Crimes with the highest incidence linked to OC in Peru 2019-2022.

Crimes	2019	2022	Variation
Computer Crimes	7,807	21,618	277%
Extortion	3,633	12,179	335%
Hitman	362	897	248%

Considering the problem described, the present study has the following objectives: (i) to describe how undercover operations are carried out in digital environments in the fight against organized crime in the city of Metropolitan Lima; (ii) to identify the contribution of undercover operations within digital environments in the fight against organized crime; (iii) to describe the digital environments, platforms and computer applications used by organized crime; (iv) to describe the tools in virtual media that police personnel use in OEDs; (v) to describe the legal framework that regulates the use of OEDs; (vi) to determine the profile that police personnel must have to execute OEDs; and based on the findings (vii) to propose improvements to this special investigation technique, in addition to serving as a background for future scientific research and proposals to improve police action.

2. Methodology

This study employed a qualitative approach using the hermeneutic phenomenological method [10]. Data saturation was achieved with 16 participants [11], all of whom were active police officers.

Officers involved in organized crime investigations in Metropolitan Lima over the past two years. To collect the data, the following techniques and instruments were used: the interview with its instrument, the semi-structured interview guide [12]; documentary analysis with its instrument, the data sheet [13, 14]; and a survey to collect the opinion of police investigators about specific aspects of the research phenomenon. To protect personal data, individual codes were used, in addition, informed consent was explained and given. For data processing, discursive analysis, and the software ATLAS.ti.

3. Results

The data obtained through interviews and documentary analysis formed the categories described in Table 2.

Table 2
Categories of study.

Category	Subcategory
Covert operations within digital environments	Special investigation techniques
	Computing platforms and applications Computer tools
	Legal framework Professional profile
	Protective measures (emergency)

Regarding the first objective, the findings reveal that EOs are gaining relevance because criminals have moved a significant part of their activities to the virtual space, taking advantage of digital platforms, social networks, and instant messaging systems to plan, coordinate, and execute illicit actions. To counteract these attacks, law enforcement agencies, in particular the Peruvian National Police (PNP), have been adapting, using new technologies and investigation methods that allow them to infiltrate criminal networks to obtain and collect relevant information.

Respondents noted that EOIs are considered an effective technique in the fight against COs. The analysis revealed that, where EOIs were properly developed, they were instrumental in dismantling criminal networks, especially in cases involving extortion, computer fraud, and online sexual crimes. However, they also mentioned that the use of EOIs is still limited.

Effective undercover operations require a combination of strong ethical principles, advanced technical skills, and a deep understanding of the legal framework governing digital crime investigations. In this sense, police officers create identities and adopt fictitious digital personality profiles to infiltrate the depths of the digital networks of COs. The fictitious digital identity is a key tool that allows direct interaction with criminals, who are unaware that they are dealing with an undercover police officer.

An updated and agile legal framework is another essential component in the development of these operations. Peruvian regulations establish the bases for the implementation of special investigation techniques in digital environments, in order to ensure that digital evidence collected during undercover operations is admissible in a judicial process. Law 30077 against organized crime and Article 341-A of the criminal procedure code are the legal framework for the development of undercover operations in digital environments.

The interviewees mentioned that technology plays a fundamental role in this type of operation. Computer tools such as monitoring software, digital search, and real-time data analysis are used by digital agents to track criminals' communications, obtain digital evidence, and ensure the integrity of the evidence obtained. It is worth mentioning that COs also make use of the same technologies and even more advanced tools, such as encryption systems, to hinder access to their information and protect their illicit operations. COs have shown a remarkable ability to quickly adapt to new technologies and digital environments, using platforms such as the Deep Web, social networks, and encrypted messaging systems to carry out crimes such as extortion, computer fraud, online sexual crimes, crimes against sexual freedom, virtual kidnapping, and money laundering, among others.

The interviews revealed that agents involved in undercover operations within digital environments require a high degree of values and ethics, specialization in cybersecurity; management of digital platforms; knowledge of the most advanced computer tools; use of social networks; knowledge of the English language; knowledge of the legislation that regulates the special technique; and the ability to interpret the profile of the acquired fictitious identity. In this sense, continuous specialized training is key to the success of these operations.

Figure 1 shows how covert operations are implemented and fictitious digital identities are created.

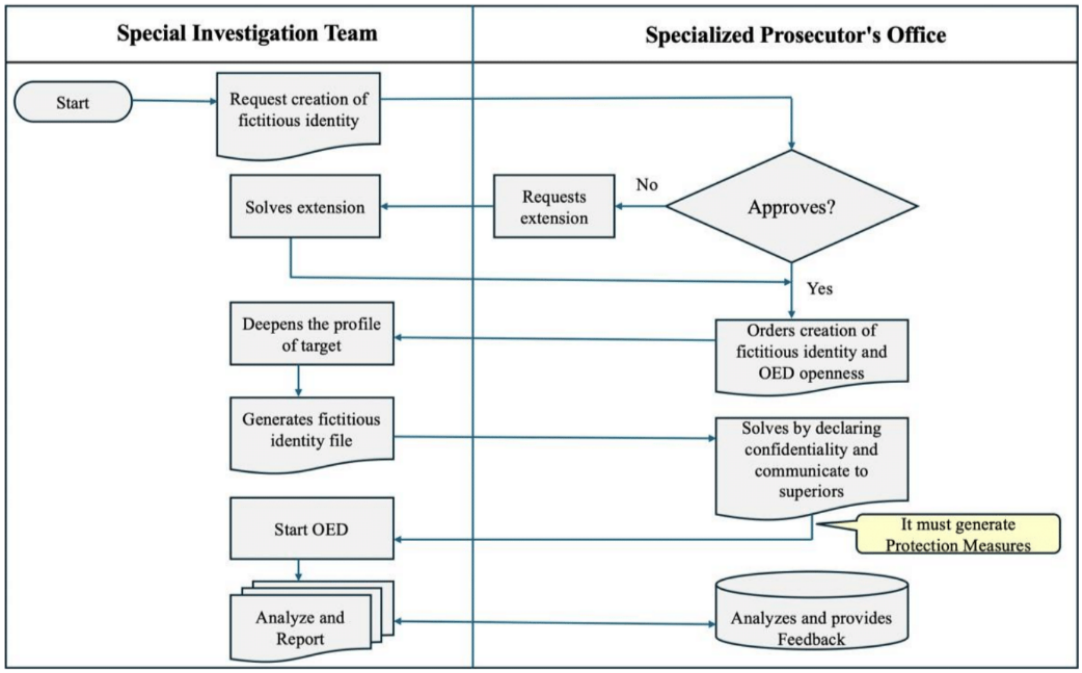

Figure 1: Flowchart for OED implementation and creation of fictitious digital identity.

Note: The flowchart shows the coordination between the special investigation teams with OC investigation functions and the Specialized Prosecutor's Offices Against Organized Crime (FECOR).

Regarding the second objective, the interviewees pointed out that EOs make an important contribution to the fight against criminal structures because they allow justice operators to infiltrate criminal networks that operate on digital platforms. The ability to access these environments through fictitious identities, avatars, and profiles facilitates obtaining crucial evidence to dismantle OCs.

The use of digital tools in EOIs has made it possible to trace illegal communications and transactions that were previously inaccessible through traditional methods. However, to ensure the effectiveness of these techniques, it is essential that investigators are trained in the use of advanced technologies and understand the modus operandi of criminals in cyberspace.

Undercover operations have made it possible to identify and track OC leaders. According to those interviewed, the OEDs contribute significantly to the fight against OCs because they contribute to the theory of the case; provide evidence in the process; and allow for an eventual conviction, thus achieving the objective of dismantling the OCs. The results of a survey applied to 30 agents of the highly complex crimes division revealed that 87% of those surveyed considered that these operations are effective in the fight against organized crime.

Regarding the third objective, the findings indicate that, in Peru, OCs have adopted digital environments as part of their modus operandi, using platforms such as Facebook, WhatsApp, Instagram, Telegram and anonymous networks such as the Dark Web to coordinate and execute their illicit activities. These tools allow criminal groups to operate efficiently and anonymously, making it difficult for authorities to intervene through techniques such as encryption and data deletion, which complicates the detection and tracking of their activities.

Digital environments offer a key infrastructure for COs, where the use of specialized software, such as encryption tools and malware, allows criminals to protect their communications and hide evidence. These platforms, especially encrypted messaging platforms, create barriers to accessing critical information in investigations, highlighting the need for the PNP to update its tools with advanced technology. To counter CO activities, data preservation methods, such as HASH codes, are required, which strengthen the ability of law enforcement to dismantle these criminal networks. Table three shows the digital places where COs operate, according to what was indicated by the interviewees.

Table 3
Digital environments, platforms and software used by OCs.

Digital environments	Platforms	Softwares
DarkWeb	Facebook	Malwares
	WhatsApp	Spies
	Instagram	
	Telegram	

Note: Malware software infects computer equipment and Spies even allow cloning of telephone and computer equipment.

Regarding the fourth objective, police personnel use a variety of tools in virtual media to carry out undercover operations against organized crime, taking advantage of technological tools that allow tracking, collecting and preserving digital evidence. However, the same technology or more current versions are used by COs to carry out their illicit activities. Table 4 presents a summary of the opinion of 48 specialized police officers surveyed in this study.

Table 4
Opinion on the computer update of the PNP and the OC.

Question Description	Disagree %	Neutral %	%
PNP quickly upgrades its IT technology to run OED.	36%	30%	34%
OCs are rapidly updating their skills in using IT tools to operate in digital environments.	12%	2%	86%

As can be seen, the majority of respondents, 86%, indicated that the OCs quickly update their computer tools, while only one third, 34%, considered that the PNP updates as quickly. The OCs,

from the perspective of PNP officers, are technologically ahead, which would give them an important advantage over law enforcement. The computer tools used by the authorities include programs that allow the creation of mirror copies of digital devices, guaranteeing the preservation of evidence without altering it, and using preservation mechanisms by creating forensic images with HASH codes. However, the lack of adequate technological resources and insufficient training of police personnel in the use of these tools have been identified as important deficiencies. The lack of updating and renewal of the technological tools used by the PNP also delays the progress of investigations, especially when the OCs use more advanced technology.

Regarding the fifth objective, the legal framework that regulates the use of undercover operations in the fight against OC in digital environments, the documentary analysis and the interviewees pointed out that, at the core of these laws, are Law 30077 against Organized Crime, and article 341-A of the criminal procedure code. Both norms provide the bases for the specialized units of the PNP to carry out undercover operations, with the objective of combating serious crimes such as extortion, computer fraud, online sexual crimes, crimes against sexual freedom, virtual kidnapping, money laundering, illegal mining, among others.

Law 30077 defines the guidelines for intervention in organized crime activities, allowing the PNP and other justice operators to act against these criminal networks. For its part, Article 341-A of the Criminal Procedure Code establishes the legal framework for the execution of OEDs.

However, despite this framework, those interviewed pointed out that the regulations lack the specificity and agility necessary for the execution of police operations and make it difficult for the digital evidence collected to be admissible in criminal courts. Another barrier is the inadequate coordination between the entities in charge of the administration of justice. Another key element to consider is the protection of individual rights and the protection of the data of people not related to crimes who interact with the OCs during the OEDs, which imposes additional limitations on the authorities.

Regarding the sixth objective, the interviewees pointed out that the profile of the agents who carry out OEDs is one of the most complex in the police field. Because it requires a fusion of solid moral and personal characteristics, advanced technical skills, and a solid legal knowledge, allowing them to develop the OEDs effectively and in accordance with the law. In this sense, a key element for success in infiltration tasks is ethics or integrity, due to the need to blend in with the psychological profiles of the members of the OCs. As revealed in the interviews, staying on the right side during and after the digital interaction with criminals (in a thin border of anonymous interrelation) is crucial for undercover operations to translate into successful criminal proceedings that end in the conviction and dismantling of the OCs.

Undercover digital investigators must undergo extensive training in computer technology to counteract the sophisticated methods used by criminals. However, experts stressed that the level of training of personnel does not cover the technical computer gaps compared to the technological prowess of the COs, which limits the PNP's ability to obtain and preserve digital evidence.

Table 5 below describes the ideal profile of the digital researcher.

Finally, based on the results of the study, we propose, as an improvement to the special investigation technique, the standardization of the main procedures for the execution of the OED through an easy-to-use guide in simple language, thinking about police operational work (see Appendix I, where the developed guide can be found).

3.1. Emerging Category: Protective Measures

A procedural protection measure is a legal action implemented within a criminal process to safeguard the rights and security of the persons involved, especially in investigations of organized crime or complex crimes. These measures are intended to protect victims, witnesses, and agents involved in obtaining and presenting evidence, guaranteeing their physical, psychological, and legal integrity during the development of the judicial procedure and after it [15].

It is urgent to include undercover agents, revealing agents, witnesses, and digital collaborators in procedural protection measures to reduce the risks of violent reprisals by COs. This action would

Table 5
Ideal profile of the digital researcher.

General Aspects			
Sex: Male or female			
Age: 20 – 40 years			
Police rank: Indistinct			
		Levels	
Generic Competencies	Half	High	Very High
Ethics			X
Booking			X
Emotional intelligence			X
Patience			X
Effective communication			X
Police Competencies	Half	High	Very High
Camouflage			X
Infiltration			X
Report			X
Police procedures			X
Technical skills		Levels	
Handling of main software and applications	Half	High	Very High
Single file		X	
Nimbus screenshot			X
HashMyFiles			X
Programming		X	
Social networks (user)		X	
Information Technology			X
Criminal Code		X	
English Language	X		

allow investigations to be conducted under strict security and confidentiality standards, ensuring the fulfillment of justice. Such measures may include mechanisms to preserve identity and the use of secure protocols in the management of information and custody of digital evidence.

3.2. Discussion

Our results confirm that Peru and Latin America are not immune to the significant increase in cybercrime, largely as a result of the new criminal modalities adopted by the OC during the COVID-19 pandemic [16, 17, 18].

In contrast to international studies, the use of digital undercover operations in Peru is still limited, which negatively affects the fight against OC, especially in the increasing number of crimes that are carried out or committed in digital environments. The low number of PNP personnel who have the appropriate profile to use digital tools or execute special investigation techniques, such as undercover operations and video surveillance, reflects a weakness in the implementation of effective strategies against OC. In this regard, De Paoli et al. [4], in their study carried out in Europe and Canada, pointed out that traditional police skills are inadequate for the digital environment, which is why the hiring of civilian specialists was required to cover these deficiencies. Naturally, Peruvian police culture is influenced by national culture and its state bureaucracy. It is worth mentioning that Peruvian culture is characterized by traditional values, Ravello and Llaque, [19], that are far from those of digital culture, which would make it difficult for the PNP to adopt values, strategies, techniques, and tools of digital culture [20].

According to the findings of related international research, COs, compared to police forces, are more agile in adopting new technologies [21, 22]. This situation is critical in Peru, because 18.3% of the economy comes from informal sources; 58.7% of jobs are informal [23]; and there are complex COs dedicated to crimes with high monetary returns. Such as informal mining and drug trafficking that

have the capacity to infiltrate and corrupt the different levels of power and the depth of the social fabric. It is important to highlight that the large profits of these COs would allow them to acquire cutting-edge technological resources and professional operators.

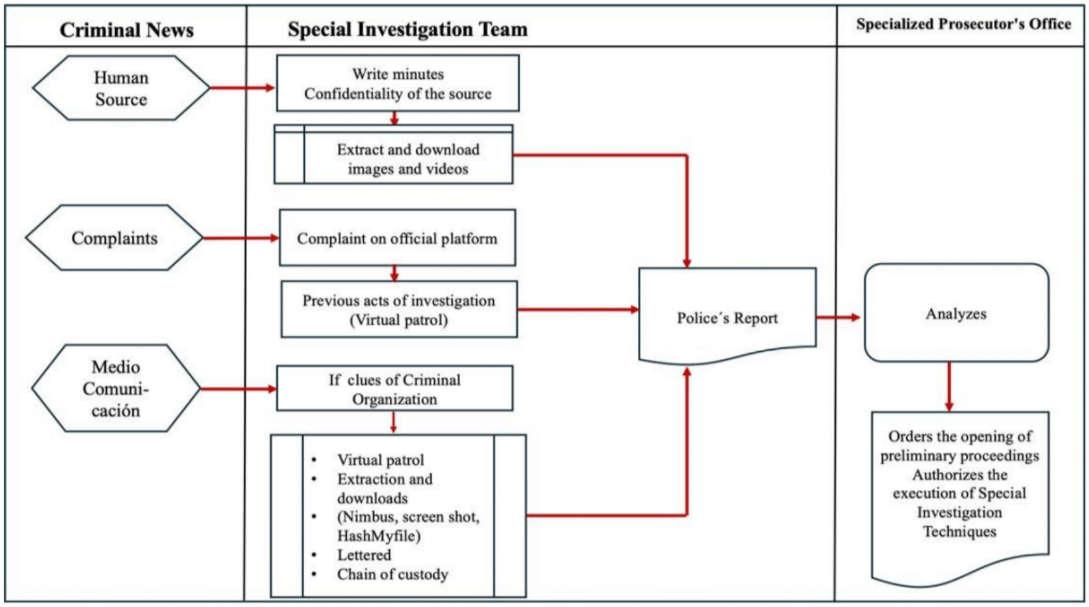

Figure 2: Procedure upon learning of a criminal act and opening of a prosecutor's file on the investigation into a criminal organization.

The findings show that the constant technological and computer evolution requires police personnel trained in updated tools for the collection and preservation of the integrity and authenticity of digital evidence, which will be part of the criminal process. This underlines the need to train police personnel to achieve the ideal profile of digital investigators (see table 4). Our evidence reinforces the findings of Kassem and Erken [24] in the United Kingdom, who pointed out that inadequate training in digital skills and advanced technologies is a major challenge for police officers. Taking into consideration the gap in the digital culture of the PNP, the majority traditional profile of the agents, and the growing and urgent need for training in technology and computer science, we consider it imperative to create the specialty of police computer engineering from police training schools. In this way, the technological gap between the OC and the PNP could be shortened in the medium term. Additionally, the PNP would be better prepared for the inevitable wave of crimes leveraged by new technologies and the global disruptive Artificial Intelligence (AI).

Regarding the legal framework that supports the OEDS in Peru, it is very generic and outdated. Because it is updated under the vision of the traditional legal system, it is archaic to combat COs in digital environments. Therefore, it is necessary to propose amendments to both Law No. 30077 against organized crime and Article 341-A of the Criminal Procedure Code. Our results are consistent with those of [25], who in her study in the European Community pointed out that contemporary criminal investigation calls into question; the law in general; the scientific validity of digital findings, because old procedural guarantees do not adapt to processes with digital evidence; and the criminal legal system, due to the need to update the laws, regulations and procedures for validating digital evidence to protect all parties involved in the criminal process.

Due to its complex nature, huge resources, multiple offensive channels, evasive operation, and serious damage to the social fabric, it is urgent to start involving more community actors in the fight against OC in digital environments. These include hardware, software, technology services, telecommunications providers, and local representatives of digital platforms and social networks. The efforts of traditional law enforcement agencies, such as the prosecution, police, and judiciary, are insufficient to combat OCs operating in digital environments. The findings of our study support what Montasari [26] pointed out in his research in the United States of America and the United Kingdom, who stated that collaboration

between technology companies and institutions that oversee justice is crucial to combat cyberterrorism and improve national and citizen cybersecurity.

Finally, the study was not free of limitations that were overcome during the research process. On the one hand, the small number of professionals specialized in OEDD to carry out the data collection was very challenging. The scarce academic literature on OEDD in the country convinced us of the need to work only with international articles from journals indexed in quartiles one to two of the Scopus database. Future research should delve deeper into the implications of the emerging category of protection measures, the use of AI by the OC and law enforcement for OEDD, and develop actions at a theoretical and/or practical level.

4. Conclusion

The EOD is an effective technique in the fight against organized crime, allowing the obtaining of evidence for criminal proceedings and the subsequent dismantling of OCs.

Tools, such as specialized hardware and software, are pillars of the effectiveness of OEDs. Constant updating of these tools is essential to cope with the sophistication of the techniques used by OCs.

It is crucial to develop standardized operating procedures that allow detectives or digital investigators to act effectively in these environments.

The professional profile of police personnel assigned to OED must integrate values, advanced skills in cybersecurity, digital infiltration techniques, and in-depth knowledge of the applicable regulatory framework.

The legal framework that regulates EOs must be constantly updated, from a perspective of agile management, not only from a legal perspective, due to the enormous difference in the speed of attacks and sophistication of OCs and the reaction of justice operators.

Authorization to use disguised identities and manipulate aspects of legal dealings must be strictly regulated to protect both the integrity of the evidence and the rights of the individuals involved.

There is an urgent need to create a specialty in police computer engineering at the PNP officers' school in order to have professionals prepared to combat OC on equal terms, in terms of updating capabilities, hardware, and software, and at the same time, not to depend on temporary experts who do not understand the institutional culture.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] G. A. J. Díaz Samper, A. L. Molina Garzón, L. E. Serrador Osorio, Approaching the cybercriminal from a perspective of social control, Revista Criminalidad 65 (2023) 81–95.

[2] M. Diaz, P. Rangel, National challenges facing cybersecurity in the global scenario: an analysis for colombia, 2020.

[3] Nations United, United nations convention against transnational organized crime and its protocols, U. Nations. Palermo, Italy (2000).

[4] S. De Paoli, J. Johnstone, N. Coull, I. Ferguson, G. Sinclair, P. Tomkins, M. Brown, R. Martin, A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists, Policing: A Journal of Policy and Practice 15 (2021) 1429–1445.

[5] O. A. Fonseca-Herrera, A. E. Rojas, H. Florez, A model of an information security management system based on ntc-iso/iec 27001 standard, IAENG Int. J. Comput. Sci 48 (2021) 213–222.

[6] S. A. Ajagbe, J. B. Awotunde, H. Florez, Ensuring intrusion detection for iot services through an improved cnn, SN Computer Science 5 (2023) 49.

[7] S. Lannier, Infiltrating virtual worlds. the regulation of undercover agents through fundamental rights, Revista Brasileira de Direito Processual Penal 10 (2024) e1066.
[8] Ombudsman's Office, Ombudsman's report no. 001-2023-dp/adhpd. cybercrime in peru: State strategies and challenges, 2023.
[9] General Office of Planning and Budget of the Ministry of the Interior, Implementation of budget program 0086 "improvement of the services of the criminal justice system, 2023.
[10] J. W. Creswell, V. L. P. Clark, Designing and conducting mixed methods research, Sage publications, 2017.
[11] S. J. Gentles, C. Charles, J. Ploeg, K. A. McKibbon, et al., Sampling in qualitative research: Insights from an overview of the methods literature, The qualitative report 20 (2015) 1772–1789.
[12] M. Z. Cohen, D. L. Kahn, R. H. Steeves, Hermeneutic phenomenological research: A practical guide for nurse researchers, Sage Publications, 2000.
[13] R. K. Yin, Case study research: design and methods (ed.), Thousand Oaks (2003).
[14] A. Morante, M. del Pilar Villamil, H. Florez, Framework for supporting the creation of marketing strategies, International Information Institute (Tokyo). Information 20 (2017) 7371–7378.
[15] Ministry of Justice, Supreme decree no. 020-2001-jus. approves the regulations on protection measures for collaborators, witnesses, experts and victims, as referred to in law no. 27378, 2001.
[16] N. Aliane, H. Gharbi, Y. Semlali, The role of artificial intelligence, digital capabilities and digital awareness on supply chain management: moderating role of organizational readiness and digital organizational culture, Transformations in Business and Economics 22 (2023) 832–852.
[17] T. Kliestik, E. Nica, P. Durana, G. H. Popescu, Artificial intelligence-based predictive maintenance, time-sensitive networking, and big data-driven algorithmic decision-making in the economics of industrial internet of things, Oeconomia Copernicana 14 (2023) 1097–1138.
[18] A. Kuzior, I. Tiutiunyk, A. Zielińska, R. Kelemen, Cybersecurity and cybercrime: Current trends and threats., Journal of International Studies (2071-8330) 17 (2024).
[19] A. Ravello, A. Llaque, Moderation of national culture between empowerment and resilience in job performance, 2023.
[20] World Economic Forum, Digital culture: The driving force of digital transformation, 2021.
[21] L. Hadlington, K. Lumsden, A. Black, F. Ferra, A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime, Policing: A Journal of Policy and Practice 15 (2021) 34–43.
[22] S. Kethineni, R. D. Jackson, Cybercrime and cryptocurrency as new challenges for the police, in: Exploring Contemporary Police Challenges, Routledge, 2022, pp. 181–192.
[23] National Institute of Statistics and Informatics, Production and informal employment in peru. satellite account of the informal economy, 2023.
[24] R. Kassem, E. Erken, In their own words: Police officers' insights on identifying and overcoming contemporary policing challenges, International review of administrative sciences 91 (2025) 130–149.
[25] R. Stoykova, Digital evidence: Unaddressed threats to fairness and the presumption of innocence, Computer Law & Security Review 42 (2021) 105575.
[26] R. Montasari, Countering cyberterrorism: The confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity, volume 101, Springer Nature, 2023.