

LEGISLATIVE COMMENTARY

The undercover digital agent in Mendoza's criminal legislation

El agente digital encubierto en la legislación penal de Mendoza

Patricia A. Cozzo¹  • Jesús C. Salas² 

Received: 11 April 2024 / Accepted: 07 June 2024 / Published online: 07 July 2024

© The Author(s) 2024

Abstract This paper examined the incorporation of the undercover digital agent into the criminal process of the Province of Mendoza, Argentina, following the reform introduced by Law 9510 to the Code of Criminal Procedure. The objective was to analyze this concept's normative, procedural, and constitutional aspects in the context of combating organized crime and complex crimes committed in digital environments. The scope of the new legal articles regulating the role of the undercover digital agent was studied, along with other digital investigation tools such as data security and computer systems analysis. This concept's risks to fundamental rights such as privacy and the right to freedom from self-incrimination were also assessed. The methodology critically analyzed current regulations, specialized doctrine, and relevant jurisprudence. Among the main findings, a tension was identified between the need for investigative effectiveness and the protection of constitutional guarantees. In conclusion, it was argued that the legitimacy of the use of digital undercover agents depends on their rigorous implementation, with strict judicial oversight, defined time limits, and safeguards that ensure respect for due process and fundamental rights.


Keywords digital undercover agent, criminal proceedings, organized crime, fundamental rights, non-self-incrimination.

Resumen Este trabajo examinó la incorporación del agente digital encubierto al proceso penal de la Provincia de Mendoza, Argentina, a partir de la reforma introducida por la Ley 9510 al Código Procesal Penal. El objetivo fue analizar los aspectos normativos, procesales y constitucionales de esta figura en el contexto del combate a la criminalidad organizada y los delitos complejos cometidos en entornos digitales. Se estudió el alcance de los nuevos artículos legales que regulan la actuación del agente encubierto digital, junto con otras herramientas de investigación digital como el aseguramiento de datos y el análisis de sistemas informáticos. Asimismo, se evaluaron los riesgos que esta figura representa para derechos fundamentales como la intimidad y la no autoincriminación. La metodología consistió en el análisis crítico de la normativa vigente, la doctrina especializada y la jurisprudencia relevante. Entre los principales hallazgos se identificó una tensión entre la necesidad de eficacia investigativa y la protección de garantías constitucionales. Como conclusión, se sostuvo que la legitimidad del uso del agente encubierto digital depende de su implementación rigurosa, con control judicial estricto, límites temporales definidos y salvaguardas que aseguren el respeto al debido proceso y a los derechos fundamentales.

Palabras clave agente encubierto digital, proceso penal, criminalidad organizada, derechos fundamentales, no autoincriminación.

How to cite

Cozzo, P. A., & Salas, C. J. (2024). The undercover digital agent in Mendoza's criminal legislation. *Journal of Law and Epistemic Studies*, 2(2), 13-17. <https://doi.org/10.5281/zenodo.14868646>

 Patricia A. Cozzo
pcv.abog@gmail.com

¹Universidad Nacional Tres de Febrero, Argentina.

²Instituto Universitario de Tecnología Los Andes y FUJA, Venezuela.

Universidad Nacional Tres de Febrero, Argentina.

Introduction

This paper analyzes the concept of the undercover digital agent in the criminal legislation of the Province of Mendoza, Argentina, and its incorporation into the provincial Criminal Procedure Code (Law 6730) through Law 9510. The objective is to examine the legal, procedural, and constitutional implications of this concept, particularly in combating organized crime and using digital technologies for criminal investigation.

The emergence of new forms of crime linked to technology has required States to adapt their investigative tools. In this context, the digital undercover agent emerges as a device that allows for covert infiltration into virtual environments, especially in networks where highly complex crimes are committed, such as the corruption of minors, sex tourism, or the distribution of child pornography. When carried out in virtual spaces, these criminal practices present particular challenges for criminal law, particularly regarding access to evidence, the preservation of fundamental rights, and the delimitation of state actions.

The figure of the undercover agent has traditionally been controversial, as their inherently secretive and deceptive actions straddle a conflict zone between the effectiveness of the criminal process and unrestricted respect for individual rights. The digitalization of this role sharpens the debate, introducing new dilemmas regarding legality, judicial oversight, and the scope of state intervention in private life.

The right to privacy protects individuals' private spheres from arbitrary interference by the State. The figure of the undercover digital agent, by infiltrating closed virtual spaces, even in environments that simulate personal or confidential relationships, can imply access to extremely sensitive information without the affected person's knowledge or opportunity to defend themselves, reproducing what Márquez (2004) describes as a surveillance architecture that threatens to dissolve the boundary between public and private.

Finally, critical observations are included regarding the practical scope of this tool, its legitimacy in a state governed by the rule of law, and its compatibility with a guarantee-based conception of the criminal process.

Regulatory framework of the Mendoza reform

Law 9510 of the Province of Mendoza modifies and incorporates various articles into the local Code of Criminal Procedure (Law 6730) to adapt criminal investigation tools to the new challenges of crimes committed in digital environments. This reform introduces the concept of the digital undercover agent and other mechanisms related to securing, accessing, and safeguarding computer data.

The law establishes the incorporation of Articles 29 bis,

224 bis, 224 ter, and 228 bis and the amendment of Article 226 of the Code of Criminal Procedure. Article 29 bis regulates the concept of the digital undercover agent for the first time, establishing the formal requirements for their actions, the crimes in which they may be involved, the duration of the measure, and the guarantees to prevent abuse.

The text provides that the prosecutor may, with justification, request an agent's undercover action on digital platforms before the Criminal Court when investigating complex crimes, especially those provided for in Articles 128 and 131 of the Criminal Code. Authorization will be granted by reasoned decree and for a maximum period of 180 days, extendable in justified cases.

Furthermore, the law establishes that the digital profiles used may not include real images of individuals and must be created by qualified technical personnel under the prosecutor's supervision. Information related to the profile used and the authorized activities must be stored in a safe deposit box, ensuring traceability and judicial oversight.

The law also provides an officer with an exemption from criminal liability when his or her actions are proportional, necessary, and do not constitute provocation to commit a crime. This seeks to strike a balance between investigative effectiveness and respect for constitutional guarantees.

Along with this provision, the reform regulates new powers for the prosecutor to order the seizure of computer data (Article 224 ter), the presentation of data by suppliers and third parties (Article 224 bis), the seizure and analysis of computer systems (Article 228 bis), and the disposal of seized devices (Article 226). These provisions form a system of tools for digital investigation and the fight against cybercrime and organized crime.

It should be noted that these tools also contemplate the possibility of operating extraterritorially, under certain conditions, when the data is located in connected systems outside the provincial jurisdiction. Mechanisms for rapid judicial authorization in urgent cases and criteria for preserving the chain of custody are included, which seek to grant evidentiary validity to the data obtained during the execution of these measures.

Thus, the reform's regulatory framework not only introduces an innovative concept, such as the undercover digital agent but also articulates a set of instruments designed to strengthen the Public Prosecutor's Office's capacity to prosecute complex crimes while ensuring certain controls and limits against potential excesses of punitive power (Barja et al., 2019).

Organized crime and investigative tools

Organized crime represents one of the most complex chal-

lenges for contemporary criminal justice systems. Its hierarchical structure, transnational nature, intensive use of technology, and capacity for institutional corruption often make traditional criminal prosecution tools insufficient (Anarte & Ferré, 1999; Hefendehl, 2004).

Faced with this reality, States have been compelled to provide the Public Prosecutor's Office with more effective mechanisms to address highly complex crimes, such as human trafficking, money laundering, drug trafficking, corruption, smuggling, and cybercrimes (Granados, 2001; Arciniegas, 2020).

Within this framework, Argentine legislation has developed a set of special procedural mechanisms, such as the undercover agent, the revealing agent, the informant, the controlled delivery, the repentant, and the extension of jurisdiction. These tools have been recognized in reforms such as Law 27,304 and allow for overcoming the obstacles imposed by the secrecy inherent to organized crime. They facilitate access to evidence, the internal structures of criminal organizations, and the location of their prominent leaders (González, 2007).

The digital undercover agent, in particular, represents an evolution of these tools by adapting to the virtual environments where many criminal networks operate today. Encrypted platforms, closed social networks, instant messaging services, and illegal markets on the deep web are used to commit crimes without leaving easily detectable traces. Therefore, the possibility of a public official infiltrating a website with judicial authorization represents an institutional response to these new criminal scenarios (Guariglia, 2007).

Law 9510, in line with international trends, incorporates this concept into the Mendoza criminal process and establishes rigorous requirements for its application. It requires a reasoned judicial authorization, a time limit, a prohibition on inciting the crime, and the obligation to preserve the integrity of the evidence (Del Pozo, 2006).

These types of tools, however, are not without their fair share of challenges. The use of false identities, the simulation of behavior, and the covert collection of information generate debates about the proportionality of the measure, its necessity in each specific case, and the risk of eroding fundamental rights. Legal doctrine has warned of the need for these measures to be used exceptionally, preventing the State from acting with an "enemy" approach that undermines the guarantee-based criminal justice model (Guerrero, 2013).

Therefore, its implementation must be accompanied by a system of institutional controls, accountability mechanisms, and a judicial culture that ensures its use is controlled and judicially supervised. Furthermore, it is essential to differentiate between the different types of agents: the disclosing agent acts without inducing a crime and only uncovers illicit activities; the informant transmits data without intervening;

the repentant collaborates after being arrested. This classification makes it possible to specify the scope of the undercover digital agent and prevent regulatory and operational confusion.

In short, the digital undercover agent is part of a modernization of investigative strategies against organized crime. However, its legitimacy will depend on its use of the principles of due process, respect for human rights, and the legitimate purpose of protecting society from complex and sophisticated threats.

Fundamental rights compromised: privacy and non-self-incrimination

Implementing the digital undercover agent poses serious constitutional challenges, particularly about the fundamental rights to privacy and freedom from self-incrimination. Both are essential pillars of due process and are recognized in both domestic law and international human rights treaties (Martínez, 1994; Madrid-Malo, 2004).

The right to privacy protects individuals' private spheres against arbitrary interference by the State. The role of the undercover digital agent, by infiltrating closed virtual spaces, even in environments that simulate personal or confidential relationships, can entail access to extremely sensitive information without the affected party's knowledge or opportunity to defend themselves. This intrusion can violate the principle of legality if it is not clearly defined and justified by reasons of strict necessity and proportionality (Martínez, 2001).

Article 19 of the National Constitution and 11 of the American Convention on Human Rights establish the right to privacy, honor, and reputation. Likewise, Article 17 of the International Covenant on Civil and Political Rights enshrines protection against arbitrary interference. The actions of undercover digital agents must be interpreted by these standards, which requires a case-by-case analysis to assess whether the means employed are appropriate, necessary, and proportionate to the legitimate purpose pursued (Guerrero, 2013).

On the other hand, the right against self-incrimination implies that no one is obligated to testify against themselves or contribute evidence that could lead to their conviction. The actions of the undercover officer can generate situations where the subject of investigation, believing they are interacting with a trusted third party, reveals incriminating information without having been informed of their rights or having legal advice. This is particularly problematic when the undercover officer induces or encourages behavior that would not otherwise have occurred, raising doubts about the validity of the evidence obtained and the possible configuration of a case of instigation or provocation to commit a crime (Jauchen, 2005).

National jurisprudence has addressed these issues with criteria ranging from strict respect for guarantees to a certain degree of flexibility regarding investigations into organized crime. The Supreme Court of Justice of the Nation held, in the “Fernández, Víctor H.” case, that the use of undercover agents does not, in itself, violate the right to defense in court, provided that they act within the framework of the rule of law and do not induce a crime. Legal doctrine has warned of the risk that the State could legitimize practices that border on illegality if clear limits and effective control mechanisms are not established (Ruiz, 2024; Guariglia, 2007).

Ultimately, the use of digital undercover agents will only be legitimate to the extent that its application is framed within a model of criminal procedure that guarantees justice, in which fundamental rights are respected as a condition for the validity of state action. Prior judicial oversight, transparency in the authorization procedure, and subsequent review of the proportionality of the measure are essential to avoid deviations that compromise the legitimacy of the criminal justice system (Gimeno et al., 2020).

Conclusions

The introduction of digital undercover agents into Mendoza’s criminal justice system under Law 9510 reflects a legislative effort to combat rising cybercrime, enabling the Public Prosecutor’s Office to more effectively prevent and prosecute complex offenses in digital spaces. While this measure enhances law enforcement’s ability to address organized crime in virtual environments, its implementation must carefully balance effectiveness with the principles of the rule of law, ensuring strict adherence to legality, proportionality, and necessity to prevent potential violations of fundamental rights. The Mendoza legislation includes safeguards—such as prior judicial authorization, time limits, and prohibitions on provocation—yet its success hinges on robust judicial oversight, specialized training for legal professionals, and strong institutional controls. Ultimately, the challenge is to strike a balance between leveraging digital undercover operations as a legitimate investigative tool and upholding the ethical and constitutional safeguards that define a democratic justice system.

References

- Anarte, E., & Ferré, J. C. (1999). Conjeturas sobre la criminalidad organizada. In *Delincuencia organizada: aspectos penales, procesales y criminológicos*. Universidad de Huelva. <https://dialnet.unirioja.es/servlet/articulo?codigo=589300>
- Arciniegas, G. A. (2020). *Policía judicial y sistema acusatorio*. Ediciones Nueva Jurídica. https://libreriatiemis.com/product/policia-judicial-y-sistema-acusatorio/?srsltid=AfmBOoptolnABV8qeZic4vB_esnKsMS2yU-TOqmjNsN9Rd0dnbnWd94Vm
- Barja, J., Granados, C., Martínez, A., Martínez-Arrieta, C., Villegas, M. Á., Barés, P., García-Comendador, L., Moreno, A., Sánchez, F. J., & Encinar, M. Á. (2019). *Tratado de Derecho procesal penal*. LIBRERÍAS MARCIAL PONS. <https://www.marcialpons.es/libros/tratado-de-derecho-procesal-penal/9788413094236/>
- Del Pozo, M. (2006). El agente encubierto como medio de investigación de la delincuencia organizada en la ley de enjuiciamiento criminal española. *Criterio Jurídico*, 6. <https://revistas.javerianacali.edu.co/index.php/criteriojuridico/article/view/1006>
- Gimeno, V., Calaza, M. S., & Díaz, M. (2020). *Derecho Procesal Penal*. LIBRERÍAS MARCIAL PONS. <https://www.marcialpons.es/libros/derecho-procesal-penal/9788413086293/>
- González, P. E. (2025). *La policía judicial en el sistema penal acusatorio* (2nd ed.). Doctrina y Ley. https://www.doctrinayley.com/tienda/libreria/derecho-penal/la-policia-judicial-en-el-sistema-penal-acusatorio/?srsltid=AfmBOorz0VYLisNEUJ_cUhdznKLfi0DdPT-GUAeO338SM8PF90IGIq-g
- Granados, C. (2001). Instrumentos procesales en la lucha contra el crimen organizado: agente encubierto, entrega vigilada, el arrepentido, protección de testigos, posición de la jurisprudencia. *Cuadernos de Derecho Judicial*, 2. Consejo General del Poder Judicial.
- Guariglia, F. (1994). El agente encubierto ¿un nuevo protagonista en el procedimiento penal? *Revista de Ciencias Penales*, (23), 16-33. <https://biblioteca.corteidh.or.cr/documento/52051>
- Guerrero, O. J. (2013). *Fundamentos teórico-constitucionales del nuevo proceso penal* (2nd ed.). Ediciones Nueva Jurídica. <https://nuevajuridica.com/Products/218-FUNDAMENTOS-TE%3%93RICO-CONSTITUCIONALES-DEL-NUEVO-PROCESO-PENAL>
- Hefendehl, R. (2004). ¿La criminalidad organizada como fundamento de un Derecho Penal de enemigo o de autor? *Derecho Penal y Criminología*, 25(75), 57–70. <https://revistas.uexternado.edu.co/index.php/derpen/article/view/1040>
- Jauchen, E. (2005). *Derechos del imputado*. R. Culzoni. <https://biblioteca.mpf.gov.ar/meran/opac-detail.pl?id1=719>
- Madrid-Malo, M. (2004). *Derechos fundamentales*. 3R Editores Ltda. <https://biblioteca.ucatolica.edu.co/cgi-bin/koha/opac-detail.pl?biblionumber=22780>
- Márquez, P. (2004). *El ojo ve, el poder mira: la arquitectura para la vigilancia y el fin de la privacidad*. Pontificia Universidad Javeriana.
- Martínez, J. (1994). La configuración constitucional del derecho a la intimidad. *Derechos y Libertades*. <https://e-archivo.uc3m.es/rest/api/core/bitstreams/95f37793-f655->

[4bc2-ab39-c52f81201f04/content](https://www.buscablibre.ec/libro-tecnologias-de-la-informacion-policial-y-constitucion/9788484423676/p/3307575?s-rltid=AfmBOoAIr4XV19rR0BBv-s7eBr48f9mAUgY8x4TgEaV9JRHA_dtnzSPq)

Martínez, R. (2001). *Tecnologías de la información, policía y constitución*. Tirant Lo Blanch. https://www.buscablibre.ec/libro-tecnologias-de-la-informacion-policial-y-constitucion/9788484423676/p/3307575?s-rltid=AfmBOoAIr4XV19rR0BBv-s7eBr48f9mAUgY8x4TgEaV9JRHA_dtnzSPq

Ruiz, W. (2024). *La investigación en el proceso penal acusatorio*. Ediciones Olejnik.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Author contributions

Patricia A. Cozzo and Jesús C. Salas: Conceptualization, data curation, formal analysis, investigation, methodology, supervision, validation, visualization, drafting the original manuscript and writing, review, and editing.

Data availability statement

Not applicable.

Statement on the use of AI

The authors acknowledge the use of generative AI and AI-assisted technologies to improve the readability and clarity of the article.

Disclaimer/Editor's note

The statements, opinions, and data contained in all publications are solely those of the individual authors and contributors and not of Journal of Law and Epistemic Studies.

Journal of Law and Epistemic Studies and/or the editors disclaim any responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products mentioned in the content.