


# Infiltrating virtual worlds. The regulation of undercover agents through fundamental rights

*Infiltração em mundos virtuais. A regulação de agentes encobertos diante dos direitos fundamentais*

**Salomé Lannier<sup>1</sup>**

University of Luxembourg, Luxembourg

salome.lannier@uni.lu

 <https://orcid.org/0009-0003-3650-7866>

---

**ABSTRACT:** As virtual worlds become increasingly integrated into daily life, law enforcement authorities face new challenges in adapting criminal procedure to these immersive digital environments. This paper explores how undercover operations might be conducted in virtual worlds, focusing on the legal frameworks governing traditional and cyber infiltration in France and Spain, in parallel with selected European Court of Human Rights' case law. Which opportunities these legal frameworks offer for investigations in virtual worlds, and how should they be balanced with the right to privacy and the right to a fair trial? In Spain, cyber infiltration is part of a unified framework, whereas France treats traditional and cyber infiltration as distinct. Both countries offer broader opportunities for virtual world investigations through cyber infiltration's flexible scope and authorization. However, traditional infiltration grants undercover agents wider powers that may better align with the unique dynamics of virtual worlds. Therefore, a mixed regime may be needed for effective investigations in these environments. The case law of the European Court of Human Rights underscores the importance of evaluating the proportionality of these measures, particularly with the right to privacy, regarding their regulation, and the right to a fair trial, regarding the risk of entrapment.

---

<sup>1</sup> Postdoctoral researcher at the University of Luxembourg. PhD in Private Law and Criminal Sciences.

**KEYWORDS:** virtual worlds; investigation; undercover agents; infiltration; cyber infiltration.

**RESUMO:** *Conforme os mundos virtuais se tornam cada vez mais integrados à vida cotidiana, as autoridades de persecução penal enfrentam novos desafios na adaptação do processo penal a esses ambientes digitais imersivos. Este artigo analisa como operações encobertas podem ser conduzidas em mundos virtuais, com foco nos marcos legais que regem a infiltração tradicional e cibernética na França e na Espanha, em paralelo com a jurisprudência do Tribunal Europeu de Direitos Humanos. Quais oportunidades esses marcos legais oferecem para investigações em mundos virtuais e como devem ser equilibradas com o direito à privacidade e o direito a um julgamento justo? Na Espanha, a infiltração cibernética faz parte de um regime unificado, enquanto a França trata a infiltração tradicional e cibernética como distintas. Ambos os países oferecem amplas oportunidades para investigações em mundos virtuais por meio da flexibilidade do escopo e autorização da infiltração cibernética. No entanto, a infiltração tradicional concede aos agentes infiltrados poderes mais amplos, que podem estar mais alinhados com as dinâmicas únicas dos mundos virtuais. Portanto, pode ser necessário um regime misto para investigações eficazes nesses ambientes. A jurisprudência do Tribunal Europeu de Direitos Humanos destaca a importância de avaliar a proporcionalidade dessas medidas, especialmente em relação ao direito à privacidade, quanto à sua regulamentação, e ao direito a um julgamento justo, quanto ao risco de indução ao crime.*

**PALAVRAS-CHAVE:** mundos virtuais; investigação; agentes encobertos; infiltração; infiltração digital.

---

## 1. INTRODUCTION: INVESTIGATING IN VIRTUAL WORLDS

As the use of virtual worlds, or metaverses, intensifies, virtual criminality and offenses facilitated by these technologies will increasingly present familiar challenges (e.g., jurisdiction, encryption) while also introducing new ones, particularly the adaption of criminal procedure to immersive environments. This paper aims to explore the implementation of investigative actions within virtual worlds. Law enforcement authorities (LEAs) may find it particularly necessary to enter virtual worlds

anonymously. Accordingly, this paper focuses on the deep dive of police officers in virtual environments, specifically through the application of undercover operations' legal frameworks to these settings.<sup>2</sup>

Traditionally, criminal procedure has regulated the activities of undercover agents through offline infiltration measures. However, the identification and repression of criminal behaviors online have underscored the need for a new investigative tool: cyber infiltration. In some jurisdictions, such as France, this distinction has resulted in two separate investigative measures, each governed by distinct regulatory frameworks. In others, such as Spain, legislation has integrated both offline and cyber infiltration into a single provision, treating cyber infiltration as a specific extension of traditional infiltration. These different legislative approaches offer varying opportunities for investigating offenses in metaverses, though both face similar challenges in maintaining proportionality, particularly concerning their interference with fundamental rights.

To set the context, the introduction will first provide an overview of the current state of research on the impact of virtual worlds on criminal law and criminal procedure (section 1.1), followed by a presentation of the research question and the structure of the analysis (section 1.2).

### **1.1. CRIMINAL LAW AND VIRTUAL WORLDS: STATE-OF-THE-ART**

The European Commission defines virtual worlds as “persistent, immersive environments, based on technologies including 3D and extended reality (XR), which make it possible to blend physical and digital worlds in real time, for a variety of purposes such as designing, making simulations, collaborating, learning, socializing, carrying out transactions or providing

---

<sup>2</sup> This concept has been depicted in science fiction, notably in the fourth episode of the first season of the Japanese series *Psycho-Pass*, titled “Nobody Knows Your Mask”, which aired on 2 November 2012. In this episode, detectives investigate the murder of a man whose popular virtual avatar continues to operate online after his death. To gather information about the murderer, one of the detectives infiltrates a virtual community, albeit using her personal avatar. She shares details of the investigation with another well-known avatar, trusting that the anonymity of the virtual world protects the identity of the user behind it. However, the informant is ultimately murdered by the same killer.

entertainment”.<sup>3</sup> This paper focuses on a specific example within the broader category of metaverses: a virtual environment where a person can connect, for instance, *via* a Virtual Reality (VR) headset, to embody a chosen character and interact within that space. Such environments might include VR games or virtual representations of cities (so-called “cityverses”), allowing users to, for example, access public services.

To date, the literature has primarily focused on predicting the evolution of crimes within metaverses.<sup>4</sup> It explores potential new forms of theft and counterfeiting that may emerge or be facilitated,<sup>5</sup> examines whether virtual sexual assault can be classified as such under current legal frameworks,<sup>6</sup> and considers how terrorists and money launderers might exploit virtual worlds to commit offenses.<sup>7</sup> Additionally, it questions whether cybercrimes 4.0, including hacking, will differ significantly

---

<sup>3</sup> EUROPEAN COMMISSION. COM(2023) 442/final: *Communication - An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition*. EU, 2023.

<sup>4</sup> ELSHENRAKI, Hossam Nabil. *Forecasting Cyber Crimes in the Age of the Metaverse*. IGI Global, 2023; HABER, Eldar. *The Criminal Metaverse*. *Indiana Law Journal*. v. 99, n. 3, p. 843–891. 2024.

<sup>5</sup> DREMLIUGA, Roman; PRISEKINA, Natalia; YAKOVENKO, Andrei. *New Properties of Crimes in Virtual Environments*. *Advances in Science, Technology and Engineering Systems Journal*. v. 5, n. 6, p. 1727–1733, 2020. <https://doi.org/10.25046/aj0506206>; HALLEVY, Gabriel. *Criminal liability for intellectual property offenses of artificially intelligent entities in virtual and augmented reality environments*. In: BARFIELD, Woodrow; BLITZ, Marc J. (eds.). *Research Handbook on the Law of Virtual and Augmented Reality*. Edward Elgar Publishing, 2018. p. 389–419.

<sup>6</sup> DANAHER, John. *The law and ethics of virtual sexual assault*. In: BARFIELD, Woodrow; BLITZ, Marc J. (eds.), *Research Handbook on the Law of Virtual and Augmented Reality*. Edward Elgar Publishing, 2018. p. 363–388; MALHOTRA, Vinayak. *That’s Assault! Extension of Criminal Law to the Metaverse*. *SSRN Scholarly Paper*. 2023. <https://doi.org/10.2139/ssrn.4595652>.

<sup>7</sup> YALCIN-ISPIR, Aybike. *The Metaverse and Terrorism*. In: ESEN, Fatih Sinan; TINMAZ, Hasan; SINGH, Madhusudan (eds.), *Metaverse: Technologies, Opportunities and Threats*. Singapore: Springer Nature, 2023. p. 275–284; KARAPATAKIS, Andreas. *Virtual worlds and money laundering under EU law: The inadequacy of the existing legal framework and the challenges of regulation*. *New Journal of European Criminal Law*. v. 10, n. 2, p. 128–150, 2019. <https://doi.org/10.1177/2032284419841711>. n. 2, p. 128.

or pose similar challenges to those faced today.<sup>8</sup> Alongside these substantive criminal law issues, online criminal behaviors have already been challenging LEAs for years. Difficulties arise in identifying crimes and perpetrators, assessing the competent jurisdiction,<sup>9</sup> investigating offenses, collecting evidence,<sup>10</sup> and proving liability.<sup>11</sup> Many of these challenges are not entirely new, as LEAs have been grappling with them since the rise of global efforts to combat offenses facilitated by information technologies such as the Web 3.0.<sup>12</sup>

In all areas of crime policing, LEAs will increasingly depend on private entities, particularly online service providers, to obtain data or access restricted online environments. In this context, the recent

- 
- <sup>8</sup> YADIN, Gilad. Beyond unauthorized access: laws of virtual reality hacking. In: BARFIELD, Woodrow; BLITZ, Marc J. (eds.). *Research Handbook on the Law of Virtual and Augmented Reality*. Edward Elgar Publishing, 2018. p. 340–362.
- <sup>9</sup> SCHAENGOLD, Zachary. Personal Jurisdiction over Offenses Committed in Virtual Worlds Comments and Casenotes. *University of Cincinnati Law Review*. v. 81, n. 1, p. 361–386, 2012; SINGH, Prachi; RAJPUT, Dev Karan. Metaverse: Surging Need for Competent Laws with Increasing Metaverse Crimes. *International Journal of Law Management & Humanities*. v. 5 Issue 5, p. 712-724, 2022. <https://doi.org/10.10000/IJLMH.113621>.
- <sup>10</sup> EL-KADY, Ramy Metwally. Investigating Forensic Evidence in Metaverse: A Comparative Analytical Study. In: ELSHENRAKI, Hossam Nabil. *Forecasting Cyber Crimes in the Age of the Metaverse*. IGI Global, 2024. p. 227–258; KIM, Donghyun; OH, Subin; SHON, Taeshik. Digital forensic approaches for metaverse ecosystems. *Forensic Science International: Digital Investigation*. v. 46, p. 301608, 2023. <https://doi.org/10.1016/j.fsidi.2023.301608>; SEO, Seunghee; SEOK, Byoungjin; LEE, Changhoon. Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing*. v. 79, n. 9, p. 9467–9485, 2023. <https://doi.org/10.1007/s11227-023-05045-1>.
- <sup>11</sup> LEVINE, Alec. Play Harms: Liability and the Play Conceit in Virtual Worlds Comment. *McGeorge Law Review*. v. 41, n. 4, p. 929–966, 2009; BOVENZI, Gian Marco. MetaCrimes: Criminal accountability for conducts in the Metaverse. In: *Companion Proceedings of the ACM Web Conference 2023*. New York, NY, USA: Association for Computing Machinery, 2023. p. 565–567. <https://doi.org/10.1145/3543873.3587535>.
- <sup>12</sup> MCKENZIE MARSHALL, Angus; TOMPSETT, Brian Charles. The metaverse—Not a new frontier for crime. *WIREs Forensic Science*. v. 6, n. 1, p. e1505, 2024. <https://doi.org/10.1002/wfs2.1505>; UNODC. *Comprehensive Study on Cyber-crime*. United Nations, 2013.

European Regulation on electronic evidence<sup>13</sup> represents a significant development by facilitating direct cooperation between States and foreign online service providers providing services within the European Union (EU). While many questions remain regarding its implementation and the role of online service providers in balancing law enforcement requests with the protection of human rights,<sup>14</sup> the regulation allows LEAs to directly request data critical to their investigations. For example, instead of conducting a physical search of a person's location who is interacting in virtual worlds, LEAs could directly request the relevant data from the appropriate online service providers.

However, the direct implementation of investigatory measures by LEAs, without reliance on the private sector, is likely to remain a crucial component of investigations in virtual worlds. Just as police patrols the internet, officers may patrol virtual worlds to monitor user behavior more generally or to observe specific spaces or data. This could lead to the initiation of investigations for flagrant offenses or the gathering of evidence for ongoing cases. In virtual worlds, LEAs could choose to appear in uniforms, as they do in the physical world, or they could operate covertly, "dressed" as civilians or in avatars not identifiable as law enforcement agents. As long as virtual worlds do not require avatars to conform to a person's real-life appearance, LEAs will not need to rely on private actors to create their undercover characters.

Despite the growing interest of legal scholars in virtual worlds, little attention has been given to the early stages of investigation, particularly, the implementation of investigative measures within the

---

<sup>13</sup> Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.

<sup>14</sup> TOSZA, Stanisław. Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review*. v. 43, p. 105614, 2021. <https://doi.org/10.1016/j.clsr.2021.105614>; TOSZA, Stanisław. Mutual Recognition By Private Actors In Criminal Justice? E-Evidence Regulation And Service Providers As The New Guardians Of Fundamental Rights. *Common Market Law Review*. v. 61, n. 1, 2024. <https://doi.org/10.54648/cola2024005>. p. 105614. 2021. DOI 10.1016/j.clsr.2021.105614.

metaverse. Over the years, national criminal procedure codes have introduced new digital investigation measures to combat cybercrime. These measures are broadly defined as any act of investigation aimed at obtaining data,<sup>15</sup> understood as any representation of information “regardless of the nature or content of the information and the technical format of presentation”.<sup>16</sup> Among the more invasive measures are legal hacking or remote searches, which allow LEAs to collect data while operating in the physical world, often with the help of advanced software. However, many of these measures are designed for investigations conducted in the physical world. As LEAs immerse their agents in virtual worlds, existing investigatory measures may require reinterpretation. For instance, body and domicile searches might be adapted to virtual environments, with LEAs directly accessing the virtual storage of an avatar as part of their investigative efforts.

To begin with, LEAs would be “wise to start building experience with establishing a presence online in virtual worlds”.<sup>17</sup> However, anonymous investigations present a significant challenge for criminal procedure. The concept of LEAs interacting anonymously—i.e., undercover agents engaging with individuals under false identities—was originally drafted for the physical world, where such interactions involve the agent’s physical presence and a fabricated identity, as in traditional infiltration. This approach has not been substantially reconsidered despite the evolution of criminal procedure and the introduction of a new investigative tool: cyber infiltration, or investigation under pseudonym. This measure allows agents to interact through online platforms, such as forums, where a virtual identity is required.

---

<sup>15</sup> ROUSSEL, Bruno. *Les investigations numériques en procédure pénale*. PhD thesis. Université de Bordeaux, 2020. Available at: <<https://theses.hal.science/tel-02947825>>. Access on: November 8, 2023.

<sup>16</sup> ART. 29 WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. EU, 2007.

<sup>17</sup> EUROPOL. *Policing in the metaverse: what law enforcement needs to know : an observatory report from the Europol innovation lab*. EU Publications Office, 2022. Available at: <<https://data.europa.eu/doi/10.2813/81062>>. Access on: September 18, 2023.

## 1.2. RESEARCH QUESTION AND STRUCTURE OF THE PAPER

This paper addresses the following research questions: Which opportunities bring legal frameworks for traditional and cyber infiltration to investigate in virtual worlds? How should these frameworks be balanced with the right to privacy and the right to a fair trial? It aims to evaluate the potential application of both frameworks in virtual worlds through a comparative analysis of Spanish and French national legislation. Under these frameworks, undercover agents could ensure the secrecy of investigations in virtual worlds by employing traditional infiltration techniques (known as *agente encubierto* in Spain or *infiltration* in France) or cyber infiltration (referred to as *agente encubierto informático* in Spain or *enquête sous pseudonyme* in France). As previously noted, despite their geographic proximity, Spain and France have taken different legislative approaches to regulating undercover operations. In France, traditional infiltration and cyber infiltration are treated as distinct investigative measures, whereas in Spain, both are governed by a unified framework, with cyber infiltration providing a specific regime for agents operating exclusively online. Given the hybrid nature of virtual worlds—combining elements of both the offline world and Web 3.0—these environments may expose both the opportunities and limitations of these differing legislative techniques. However, as a result of this focus, the scope of this paper is predominantly centered on Western European perspectives, potentially limiting its applicability to broader, global contexts and diverse legal frameworks.

Furthermore, these investigative measures must be examined in light of the case law of the European Court of Human Rights (ECtHR) to ensure an appropriate balance between the public interest in crime investigation and prosecution and the protection of fundamental rights. Surveillance measures, by their nature secretive, inherently interfere with several provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms, particularly Article 6, which guarantees the right to a fair trial, and Article 8, which protects the right to respect for private life. Despite differences in their regulation of undercover operations, both countries still fall short in fully aligning their procedural laws with the complex requirements set forth by the ECtHR, as explained below.



Section 2 provides a brief overview of the legal provisions examined in this paper and their potential application to investigations within virtual worlds. Section 3 outlines the legal framework for authorizing undercover investigations, both in physical and online contexts. On one hand, the suitability of these frameworks will be evaluated in the context of virtual world investigations. On the other hand, the legal basis of these measures will be analyzed in relation to the case law of the ECtHR on the right to privacy, assessing their proportionality and necessity in democratic societies. Section 4 will then delve into the implementation of powers granted to undercover agents in metaverses. Since traditional and cyber infiltrations do not confer the same powers to its agents, this section will highlight existing challenges and the additional concerns that may raise as they are applied in virtual worlds. Of particular interest is the potential serious interference with the right to a fair trial, especially given the heightened risk of entrapment in online environments. Finally, section 5 will conclude by summarizing the opportunities and limitations of the current legal provisions, offering insights into their applicability and areas for improvement in the context of virtual world investigations.

## **2. SPANISH AND FRENCH LEGAL PROVISIONS ON UNDERCOVER OPERATIONS**

This section briefly introduces the legal provisions examined in this paper for undercover operations in investigating criminal offenses: traditional infiltration (section 2.1) and its cyber counterpart (section 2.2).

### **2.1. INFILTRATION**

Infiltration is not a recent addition to most criminal procedure codes. Generally, this investigative measure allows a police officer to assume a false identity to monitor specific individuals, often by establishing contact with them or their associates.

In Spain, this measure was introduced by the Organic Law 5/1999, of 13 January, which amended the Criminal Procedure Law to improve investigative actions related to illegal drug trafficking and other serious offenses.

A similar technique was introduced earlier in France through Law No. 91-1264 of 19 December 1991, aimed at strengthening the fight against drug trafficking.<sup>18</sup> This law was later significantly modified and expanded by Law No. 2004-204 of 9 March 2004, which adapted the justice system to evolving crimes.

As the titles of these reforms suggest, undercover operations have been internationally recognized as particularly effective in investigating drug trafficking, notably through control deliveries,<sup>19</sup> corruption,<sup>20</sup> and organized crime.<sup>21</sup> Initially imported from the United States during the “War on Drugs”,<sup>22</sup> this method now enjoys dedicated legal frameworks across European countries, which could also be applicable for investigations within metaverses. Undercover agents in Spain are regulated by Article 282 bis of the Criminal Procedure Law (*Ley de Enjuiciamiento Criminal*, LEC), while in France, they are governed by Articles 706-81 to 706-87 of the Criminal Procedure Code (*Code de Procédure Pénale*, CPP).

These frameworks may prove relevant as investigative measures are extended to virtual environments. Infiltrated agents in metaverses would be assigned a false identity that includes not only a name or pseudonym but also an entirely different virtual alter ego. Given that the integration of agents into virtual worlds extends beyond merely adopting a pseudonym, it may be more appropriate to pursue traditional infiltration rather than cyber infiltration. This approach would better safeguard their real identities while collecting information in virtual worlds, ensuring the

---

<sup>18</sup> QUÉMÉNER, Myriam. Fasc. 1110 : Infiltrations numériques et enquêtes sous pseudonyme. *JurisClasseur Communication*. 2024.

<sup>19</sup> See Article 11 of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

<sup>20</sup> GONZÁLEZ-CASTELL, Adán Carrizo. La infiltración policial en España como medio de investigación en la lucha contra la corrupción. *Revista Brasileira de Direito Processual Penal*. v. 3, n. 2, p. 511–536. 2017. <https://doi.org/10.22197/rbdpp.v3i2.64>.

<sup>21</sup> See Article 20 of the 2000 United Nations Convention against Transnational Organized Crime; DEL POZO PÉREZ, Marta. El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de enjuiciamiento criminal española. *Criterio jurídico*. No. 6, p. 267–310, 2006.

<sup>22</sup> NADELMANN, Ethan. *Cops Across Borders - The Internationalization of U.S. Criminal Law Enforcement*. Pennsylvania: Penn State University Press, 1993.

secrecy of the investigation. The traditional infiltration measure appears more suitable for police undercover operations in virtual worlds, as these environments often necessitate the visible presence of a person or their avatar. However, this technique was not originally designed to allow LEAs to interact covertly in online settings. Consequently, a specific regulatory framework for cyber infiltration has been developed to address the unique challenges posed by virtual environments.

## 2.2. CYBER INFILTRATION

Cyber infiltration a relatively recent investigative measure, remains largely unregulated. Its introduction has been driven by the online evolution of criminal behaviors and the needs for LEAs to access specific cyberspaces under a false identity. For instance, cyber infiltrations have been deemed essential in combating crimes such as the production and dissemination of child sexual abuse materials<sup>23</sup> and terrorism.<sup>24</sup> Broadly speaking, cyber infiltration refers to online interactions by a police officer using a pseudonym.

---

<sup>23</sup> CAROU-GARCÍA, Sara. Cibercriminalidad e investigación policial. El agente encubierto informático. In: SANZ DELGADO, Enrique, FERNÁNDEZ BERMEJO, Daniel (eds.), *Tratado de delincuencia cibernética*. Thomson Reuters Aranzadi, 2021. p. 825–864; SÁNCHEZ GONZÁLEZ, Susana. Investigar y castigar la pornografía infantil gracias al agente encubierto informático. *La ley penal: revista de derecho penal, procesal y penitenciario*. n. 154, p. 3, 2022; SÁNCHEZ GONZÁLEZ, Susana. El agente encubierto informático en la lucha contra la pornografía infantil. In: GARRIDO CARRILLO, Francisco Javier; FAGGIANI, Valentina (eds.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital*. Thomson Reuters Aranzadi, 2022. p. 367–390; VALIÑO CES, Almudena. El agente encubierto informático y la ciberdelincuencia. El intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil. In: BUENO DE MATA, Federico (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*. Granada: Comares, 2016. p. 275–285; VILLAMARÍN LÓPEZ, María Luisa. La nueva figura del agente encubierto online en la lucha contra la pornografía infantil. Apuntes desde la experiencia en Derecho Comparado. In: CEDEÑO HERNÁN, Marina (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*. Cizur Menor (Navarra): Aranzadi, 2017.

<sup>24</sup> MAYAUD, Yves. Terrorisme – Poursuites et indemnisation. *Répertoire de droit pénal et de procédure pénale*. 2023.

In Spain, there is no dedicated article in the LEC that specifically regulates cyber infiltration. Instead, its introduction stems from the amendment of Article 282 bis on traditional infiltration by Organic Law 13/2015 of 5 October 2015, which aimed to strengthen procedural guarantees and regulate technological investigative measures. Consequently, cyber infiltration is classified under the broader category of undercover operations, albeit with specific conditions.

In France, the measure for cyber infiltration was initially introduced by Law no. 2007-297 of 5 March 2007, focusing on delinquency prevention and targeting offenses such as pimping and child pornography. The legal framework was later expanded to encompass other offenses, particularly terrorism, by Law no. 2014-1353 of 13 November 2014, which reinforced provisions relating to the fight against terrorism. The current iteration of the regulation was established through the creation of Article 230-46 of the CPP by Law no. 2019-222 of 23 March 2019, as part of the programming for the justice system for the period 2018-2022.

Considering that the legislature has adopted specific provisions, in France, or exceptions to the traditional infiltration framework, in Spain, for cyber infiltration, it may be appropriate to apply these new regulations to secret investigations in virtual worlds. In these settings, agents would not interact physically with other individuals, which could mitigate potential impacts on their personal lives. Since agents do not need to establish direct, face-to-face relationships or immerse themselves in potentially dangerous environments, the risk to their personal safety and the likelihood of their real identities being compromised are minimized. These provisions could thus be viewed as an initial framework for conducting covert deep dives into virtual worlds as an investigative measure. However, two criticisms emerge. First, the binary distinction between infiltration in the real world and cyber infiltration in the online realm is becoming increasingly blurred. Offenders are often aware that certain online spaces are subject to monitoring or infiltration by LEAs. Moreover, online interactions, especially on social media platforms or communication applications, now extend beyond mere text messages to include exchanges of videos, images, and audio messages. Consequently, agents may need to conceal

their true identities or physical appearances, particularly when posing as individuals who do not look resemble them, such as children. Second, the investigative measure of cyber infiltration is relatively new and lacks detailed regulation. Its adequacy for investigating in virtual worlds may therefore be called into question, as these technologies are designed to digitally represent physical interactions.

However, to evaluate the adequacy of both measures, the following sections will outline their respective regimes while considering the requirements of the ECtHR. Although there is a pressing need for LEAs to implement such measures in metaverses, it is essential that these measures are balanced with fundamental rights. Undercover agents pose a particular threat to the right to a fair trial, as protected under Article 6.1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.<sup>25</sup> However, this interference is not automatic; it depends on “the presence of clear, adequate and sufficient procedural safeguards [to] set permissible police conduct aside from entrapment”.<sup>26</sup> These procedural safeguards have been extensively developed concerning the right to data protection and privacy. Indeed, investigative measures interfere to Article 8 of the same convention, particularly when executed without the knowledge of the person under investigation.<sup>27</sup> Therefore, this analysis, grounded in the ECtHR’s criteria for ensuring the proportionality of such investigative measures, will facilitate a discussion on the appropriateness of employing one method over the other for investigations in virtual worlds.

---

<sup>25</sup> See, particularly, ECtHR. *Teixeira De Castro v. Portugal*. 1998. 22064/13, 20763/08, 57325/13, 54294/09, 65133/11, 22326/11, 35845/13, 26220/06, 33045/09, 16178/07, 59187/09, 65525/09, 36773/13, 32993/13, 74694/12, 26578/08, 24073/13, 35432/13, 499/08, 46311/09, 77813/12, 25834/10, 58193/10, 9134/10.

<sup>26</sup> ECtHR. *Ramanauskas v. Lithuania (no. 2)*. 2018. 55146/14.

<sup>27</sup> ECtHR. *Klass and others v. Germany*. 1978. 5029/71. ; *Leander v. Sweden*. 1987. 9248/81. ; *Kruslin v. France*. 1990. 11801/85. ; *Amann v. Switzerland*. 2011. 27798/95.

### 3. BALANCING UNDERCOVER OPERATIONS IN VIRTUAL WORLDS AND THE RIGHT TO PRIVACY

To ensure the proportionality of an investigative measure, the law must clearly define the regulations governing secret measures and adhere to an expanding list of criteria established by the ECtHR.<sup>28</sup> Specifically, the procedures and conditions required for deploying undercover agents, whether in physical settings or online, are critical to evaluating their appropriateness for investigating crimes in virtual worlds. This paper will therefore focus on the material scope of the measure (section 3.1), its temporal scope (section 3.2) and the procedures for authorization (section 3.3).

#### 3.1. UNDERCOVER OPERATIONS: FOR WHICH OFFENSES?

First, undercover agents represent an exceptional measure that interferes with the right to privacy by potentially gathering substantial amounts of data related to the lives of the investigated persons and others in their environment. Consequently, such operations should be authorized in a proportional manner, specifically for designated offenses or based on defined criteria, in order to delineate the material scope of the measure in a foreseeable manner.<sup>29</sup>

In Spain, infiltration operations can only be authorized for investigations pertaining to organized crime, which is defined as the “association of three or more persons to carry out, on a permanent or reiterated basis, conduct aimed at committing” an exhaustive list of offenses.<sup>30</sup> For example, this list includes various types of trafficking

<sup>28</sup> For a summary of these criteria, see, for instance, ECtHR. *Centrum För Rättvisa v. Sweden*. 2021. 35252/08.

<sup>29</sup> ECtHR. *Big Brother Watch and others v. the United Kingdom (2)*. 2021. 58170/13, 62322/14 and 24960/15.

<sup>30</sup> Article 282 bis.4 of the LEC. However, there is a lack of uniformized drafting of the concept throughout the LEC and the Criminal Code (*Código penal*). Indeed, interception of communications (Article 588 ter a of the LEC in relation with Article 579.1.2°) and audio and image recording (Article 588 quater b.2.a.2°) rely on the notion of “criminal group or organization”,

(e.g., humans, organs, endangered species, drugs, weapons), currency counterfeiting, and terrorism. Such offenses can be facilitated through communication channels or directly perpetrated in virtual worlds (e.g., virtual shops for illegal drugs). However, these represent only a small fraction of all potential offenses for which evidence could be located in metaverses.

Similarly, Article 706-81 of the French CPP refers to an exhaustive list of offenses set forth in Articles 706-73 and 706-73-1 of the same code. These encompass offenses typically committed by organized groups, similar to those enumerated in the Spanish framework, as well as other serious offenses committed by organized groups, such as murder or rape. In France, an “organized group” is defined as an aggravating circumstance as “any grouping formed or any agreement established with a view to the preparation, characterized by one or more material facts of one or more offenses”.<sup>31</sup> This definition, however, does not specify the number of individuals involved or the temporal basis of the organization. As courts utilize diverse criteria that are not harmonized by the French High Court (*Cour de cassation*),<sup>32</sup> this concept remains a subject of significant criticism.<sup>33</sup>

Beyond this theoretical concern, which could affect the foreseeability of the law, it is crucial to acknowledge that not all offenses committed or facilitated within virtual worlds will satisfy the legal criteria for organized crime. While multiple actors may be involved in these offenses, the division of tasks and expertise among individuals does not necessarily indicate the existence of an “agreement” or a coordinated effort

---

defined as a “group formed by more than two persons on a stable basis or for an indefinite period of time, who, in a concerted and coordinated manner, shares various tasks or functions for the purpose of committing offenses”, Article 570 bis of the Criminal Code.

<sup>31</sup> Article 132-71 of the Criminal Code (*Code pénal*).

<sup>32</sup> With the exception of Cour de Cassation. 2016. 16-81.834.

<sup>33</sup> VERGÈS, Etienne. La notion de criminalité organisée après la loi du 9 mai 2004. *Actualité juridique Pénal*. p. 181, 2004; GODEFROY, Thierry. The Control of Organised Crime in France: A Fuzzy Concept but a Handy Reference. In: FIJNAUT, Cyrille; PAOLI, Letizia (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*. Springer, 2006. p. 763.

that characterizes a criminal organization. For instance, one individual might engage in the concealment of illegal funds (money laundering) as a “professional” illegal activity, without awareness of the underlying offense. Consequently, the applicability of measures designed to combat organized crime will significantly depend on the specific criminological patterns observed within virtual worlds, particularly regarding whether such patterns exhibit the requisite level of coordination or cooperation to be classified as organized criminal activity.

In contrast, a cyber infiltration can be authorized to investigate a broader range of offenses, thereby providing greater flexibility for investigations within virtual worlds. In Spain, cyber infiltrations can be authorized for any offenses committed by a criminal group or organization, as well as for terrorism-related offenses,<sup>34</sup> meaning that the exhaustive list of offenses applicable to traditional infiltration does not pertain to this measure. Furthermore, cyber infiltration may be authorized for any intentional offenses that carries a penalty of at least three years of imprisonment, encompassing a substantial proportion of criminal offenses. Finally, the measure can be employed to investigate “offenses committed by means of computer tools or any other information or communication technology or communication service”,<sup>35</sup> which could potentially cover virtually any offenses occurring within virtual worlds.

Likewise, in France, a cyber infiltration may be authorized to investigate any offense “punishable by imprisonment committed via electronic communications”,<sup>36</sup> which encompasses the majority of criminal activities occurring in virtual environments.

Cyber infiltration thus presents greater opportunities for investigations within virtual worlds. However, certain critiques from the Spanish literature have highlighted the absence of a threshold for imprisonment regarding offenses committed online.<sup>37</sup> This lack of a

---

<sup>34</sup> Article 282 bis.6 of the LEC referring to Article 588 ter a, referring to Article 579.1 of the same law.

<sup>35</sup> Article 282 bis.6 of the LEC referring to Article 588 ter a of the same law.

<sup>36</sup> Article 230-46 of the CPP.

<sup>37</sup> BUENO DE MATA, Federico. *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*. Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2019; VELASCO NÚÑEZ,



specific threshold may not adequately justify the proportionality of the measure, particularly as it grants undercover agents extensive powers that can significantly infringe on individual privacy. Given the digitalization of human activities, the necessity of LEAs to operate in online environments is undeniable. Nevertheless, the intrusiveness and secrecy of their powers in online spaces, including metaverses, must remain proportional to the objectives of the investigation and the safeguarding of fundamental rights. A more detailed discussion of these powers will be provided in section 4.

### 3.2. UNDERCOVER OPERATIONS: FOR HOW LONG?

Second, undercover operations should be restricted to a specific duration. In France, traditional infiltration can be authorized for up to four months.<sup>38</sup> In Spain, the law imposes a six-month limit for both cyber and traditional infiltrations.<sup>39</sup> However, in Spain, this time frame refers specifically to the use of the false identity and is not directly tied to the overall duration of the operation. While both countries allow for the renewal of the authorization under the same conditions, neither legal framework establishes a maximal duration, despite this being a criterion emphasized by the ECtHR.<sup>40</sup> Of particular concern is that the French CPP does not impose a time limit for cyber infiltrations.

---

Eloy; SANCHÍS CRESPO, Carolina. *Delincuencia informática: tipos delictivos e investigación: con jurisprudencia tras la reforma procesal y penal de 2015*. Tirant lo Blanch, 2019; LÓPEZ-BARAJAS PEREA, Inmaculada. El derecho a la protección del entorno virtual y sus límites. El registro de los sistemas informáticos. In: BUENO DE LA MATA, Federico; DÍAZ MARTÍNEZ, Manuel; LÓPEZ-BARAJAS PEREA, Inmaculada (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*. Valencia: Tirant lo blanch, 2018. p. 135–168; BACHMAIER WINTER, Lorena. Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: algunas cuestiones sobre el principio de proporcionalidad. In: CEDEÑO HERNÁN, Marina (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*. Cizur Menor (Navarra): Aranzadi, , 2017. 2019. Thomson Reuters Aranzadi: Cizur Menor (Navarra

<sup>38</sup> Article 706-83 of the CPP.

<sup>39</sup> Article 282 bis.1 of the LEC.

<sup>40</sup> ECtHR. *Szabó and Vissy v. Hungary*. 2016. 37138/14.

Despite the ECtHR's criteria, establishing a time limit for both cyber and physical infiltrations can be challenging, as it largely depends on the outcome of the operation, both in the physical and virtual worlds. However, allowing unlimited undercover operations in virtual worlds risks enabling secret and continuous surveillance of specific places. While such a measure might be justified by the need to protect national security—thereby permitting more serious interferences with fundamental rights—it may not be proportionate to allow police officers to engage indefinitely and secretly with users in virtual world. The European Court of Justice (ECJ) has developed a hierarchy of public interest objectives, notably in its rulings on data retention and access,<sup>41</sup> which could offer useful guidance in regulating secret operations or other intrusive investigative powers conducted by various authorities (administrative, police, judicial, or intelligence) in metaverses.

### 3.3. UNDERCOVER OPERATIONS: INITIAL AUTHORIZATION

Third, although undercover agents are highly intrusive, they can be authorized by various judicial authority, including judges or public prosecutors. In both Spain and France, either an investigative judge or a prosecutor can authorize traditional infiltration. However, in Spain, a prosecutor must immediately inform the investigative judge upon authorizing the measure.<sup>42</sup> Interestingly, in Spain, only an investigative judge can approve cyber infiltration, despite its potentially lesser impact on fundamental rights due to the absence of physical investigation.<sup>43</sup> This safeguard is sensible, given that cyber infiltration can be authorized for a broader range of offenses. In France, however, there is no requirement for an initial authorization for cyber infiltration; police officers can implement the measure directly, provided they are specially empowered

---

<sup>41</sup> Originally in ECJ, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*. 2014. C-293/12, C-594/12. The criteria of the ECJ have been systematized in *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH*. 2022. C-793/19, C-794/19.

<sup>42</sup> Article 282 bis.1 of the LEC.

<sup>43</sup> Article 282 bis.6 of the LEC.

and when “the needs of the inquiry or investigation so justify”.<sup>44</sup> This absence of judicial authorization may constitute as a direct violation of the ECtHR’s case law.<sup>45</sup>

While allowing prosecutors or police officers to authorize or initiate the measure enhances its flexibility, particularly when time-sensitive, it raises concerns about compliance with the ECtHR’s requirements. The court has stipulated that intrusive investigations should be authorized by an independent body, even if non-judicial.<sup>46</sup> To date, the ECtHR has determined that French prosecutors lack independence,<sup>47</sup> and the independence of Spain’s prosecutors has been similarly criticized in Spanish legal scholarship.<sup>48</sup>

This initial authorization should also ensure that the legal conditions for implementing the measure are met and address any elements not explicitly by law, such as the precise duration of the operation.

In cases of emergency, the absence of initial authorization might be justified to protect the interests of the investigation, particularly when immediate entry of a police officer into a virtual world is required. According to ECtHR case law, postponing authorization is permissible in urgent situations, provided that the concept of “emergency” does not grant an “unlimited degree of discretion” to LEAs.<sup>49</sup> However, the complete lack of authorization for such a measure, or authorization granted solely by a prosecutor, raises significant concerns regarding its compliance with fundamental rights.

---

<sup>44</sup> Article 230-46 of the CPP.

<sup>45</sup> ECtHR. *Klass and others v. Germany*. 1978. 5029/71; ECtHR. *Roman Zakharov v. Russia*. 2015. 47143/06.

<sup>46</sup> ECtHR. *Weber and Saravia v. Germany*. 2006. 54934/00; *Szabó and Vissy v. Hungary*. 2016. 37138/14.

<sup>47</sup> ECtHR. *Moulin v. France*. 2010. 37104/06.

<sup>48</sup> BUENO DE MATA, Federico. *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*. Cizur Menor (Navarra): Thomson Reuters Aranzadi, 2019. However, another part of the literature considers that an authorization by a prosecutor is proportional as long as there is a judicial control, EXPÓSITO LÓPEZ, Lourdes. El agente encubierto. *Revista de derecho UNED*. n. 17, p. 251–286, 2015. <https://doi.org/10.5944/rduned.17.2015.16277>.

<sup>49</sup> ECtHR. *Roman Zakharov v. Russia*. 2015. 47143/06.

## 4. BALANCING THE POWERS OF UNDERCOVER AGENTS IN VIRTUAL WORLDS AND THE RIGHT TO A FAIR TRIAL

The powers granted to undercover agents are especially important when evaluating the suitability of these frameworks for virtual worlds (section 4.1). While these powers must be broad enough to facilitate the collection of information relevant to investigations within virtual environments, the ECtHR establishes a clear boundary: they must not lead to entrapment (section 4.2).<sup>50</sup>

### 4.1. INVESTIGATORY POWERS OF UNDERCOVER AGENTS

In Spain, undercover agents, for a traditional infiltration, are generally authorized “to act under a false identity and to acquire and transport the objects, effects, and instruments of the crime and to defer their seizure”.<sup>51</sup> However, a specific judicial authorization is required “when investigative actions may affect fundamental rights”.<sup>52</sup> This applies to actions that restrict constitutional rights, such as the inviolability of the home, secrecy of communications, seizure of publications, and the right to association.<sup>53</sup> For example, paragraph 7 of Article 282 bis specifies that recording images and conversations between the agent and the suspect requires such additional authorization.

In France, for a traditional infiltration, undercover agents may surveil suspects “by assuming the role of a co-perpetrator, accomplice, or fence”, using a false identity.<sup>54</sup> They are also authorized to “acquire,

---

<sup>50</sup> ECtHR. *Teixeira De Castro v. Portugal*. 1998. 22064/13, 20763/08, 57325/13, 54294/09, 65133/11, 22326/11, 35845/13, 26220/06, 33045/09, 16178/07, 59187/09, 65525/09, 36773/13, 32993/13, 74694/12, 26578/08, 24073/13, 35432/13, 499/08, 46311/09, 77813/12, 25834/10, 58193/10, 9134/10; ECtHR. *Ramanauskas v. Lithuania (no. 2)*. 2018. 55146/14.

<sup>51</sup> Article 282 bis.1 of the LEC.

<sup>52</sup> Article 282 bis.3 of the LEC.

<sup>53</sup> Articles 18.2 and 3, 20.5 and 22.4 of the Spanish Constitution, see EXPÓSITO LÓPEZ, Lourdes. El agente encubierto. *Revista de derecho UNED*. n. 17, p. 251–286, 2015. <https://doi.org/10.5944/rduned.17.2015.16277>.

<sup>54</sup> Article 706-81 of the CPP.

hold, transport, deliver, or issue substances, goods, products, documents, or information derived from or used in the commission of offenses”, and “use or provide to persons committing these offenses legal or financial means as well as means of transport, deposit, accommodation, storage, and telecommunications”.<sup>55</sup> This broader scope of powers, absent in the Spanish legislation, is particularly useful for enabling agents to use specific telecommunications methods, such as those utilized by offenders in virtual worlds, including dark worlds.

In Spain, cyber infiltration operates under the general framework of traditional infiltration, with Article 282 bis.6 granting additional powers to agents operating online. These agents are authorized to “exchange or send illegal files by reason of their content” or “analyze the results of the algorithms applied for the identification of such illegal files”, but only with specific judicial authorization. Given the potentially large amount of data collected from virtual worlds, automated processing becomes particularly important, necessitating a clear legal basis for its lawfulness.<sup>56</sup> This provision implicitly refers to, for example, the automatic identification of child sexual abuse material. However, algorithms might also be employed for other purposes, such as detecting suspicious transactions or behaviors: the law therefore does not encompass all technical possibilities.

In France, cyber infiltration offers two general investigative powers to agents. They can “participate in electronic exchanges, including with individuals suspected of committing offenses”, and “extract or preserve data on individuals suspected of committing offenses as well as any evidence”.<sup>57</sup> After securing approval from the prosecutor or an investigative judge, agents can exercise two additional powers. First, they may “acquire any content, product, substance, sample, or service,

---

<sup>55</sup> Article 706-82 of the CPP.

<sup>56</sup> Article 8 of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

<sup>57</sup> Article 230-46.1° and 2° of the CPP.

or transmit any content in response to a specific request”.<sup>58</sup> This gives French agents broader capabilities than their Spanish counterparts, who are limited to illegal files or objects related to the offense. Spanish legal scholars suggest that agents should be able “to operate in the socio-economic sphere by opening current accounts or engaging in electronic transactions”.<sup>59</sup> Expanding agents’ powers would allow them to better navigate virtual worlds, which replicate many aspects of real-life interactions. Second, in France, agents may provide suspected perpetrators with “legal or financial means as well as means of transport, deposit, accommodation, storage, and telecommunications”.<sup>60</sup> However, the framework is more restrictive compared to traditional infiltration, as agents directly cannot use these means themselves.

A critical question surrounding the investigative powers of undercover agents relates to the geographical scope of these powers. Investigative measures are typically national in scope and should be confined to a state’s territory due to the principle of state sovereignty. For example, in France, undercover agents are authorized to operate only within national borders, under the infiltration framework.<sup>61</sup> Similarly, the Spanish High Court (*Tribunal Supremo*) has emphasized that any infiltration conducted by foreign agents within Spain, outside of the framework of formal criminal cooperation, constitutes a breach of supranational rules and national regulations governing infiltration operations.<sup>62</sup> However, online spaces, including many virtual worlds,<sup>63</sup> lack clear geographical boundaries or direct ties to any specific state.

In Spain, cyber infiltration permits agents to operate only in “communications maintained in closed communication channels”, a term that remains undefined. Some legal scholars interpret this to mean that “Internet browsing in forums and open communications by the

---

<sup>58</sup> Article 230-46.3° of the CPP.

<sup>59</sup> LEÓN CAMINO, Arantza. Modo de actuación del agente encubierto virtual. *Claves Jurídicas*. n. 1, p. 28–48, 2024.

<sup>60</sup> Article 230-46.4° of the CPP.

<sup>61</sup> Article 706-82 of the CPP.

<sup>62</sup> Tribunal Supremo. 2009. 154/2009. However, in that case, the High Court still deemed the evidence constitutionally admissible.

<sup>63</sup> Excluding augmented reality which is directly related to a physical space.

Judicial Police does not imply interference in any fundamental right”,<sup>64</sup> thus requiring neither authorization nor identification. According to this interpretation, entering virtual worlds would likely involve some form of identification, thereby qualifying these spaces as closed communication channels. However, within virtual worlds, certain areas might be viewed as public, accessible to all users, while others could be considered “extra” closed, restricted to individuals with a specific identification procedure. Other scholars<sup>65</sup> draw upon the Spanish Constitutional Court’s rulings, which are informed by the ECtHR’s case law to define privacy. A communication channel is regarded as open if “there could not be a reasonable expectation of confidentiality arising from the use of the installed program”<sup>66</sup>. Thus, the degree of privacy would depend on the affordances (design features) of virtual worlds and the privacy settings chosen by users. For spaces deemed open, judicial authorization or oversight would not be necessary, provided that no other fundamental rights are infringed.

#### 4.2. LIMITATION OF UNDERCOVER AGENTS’ POWERS

While the frameworks governing undercover operations grant significant powers to agents these powers must be limited, particularly to prevent violations of the right to a fair trial.<sup>67</sup> Specifically, the ECtHR emphasizes that officers must “confine themselves to investigating criminal activity in an essentially passive manner”, and should not influence the target to incite commit an offense they would not otherwise have

---

<sup>64</sup> VILLAR FUENTES, Isabel. El agente encubierto informático: reto legislativo pendiente en un escenario digitalizado. *Revista de Estudios Jurídicos y Criminales*. n. 6, p. 197–228, 2022.

<sup>65</sup> SÁNCHEZ GONZÁLEZ, Susana. Investigar los delitos en la red a través del agente encubierto informático. In: MERINO CALLE, Irene; HERNÁNDEZ LÓPEZ, Alejandro; LARO GONZÁLEZ, María Elena (eds.), *Desafíos del derecho en la sociedad actual: reflexiones y propuestas*. Ediciones Universidad de Valladolid, 2022. p. 267–278.

<sup>66</sup> For instance, Tribunal Supremo. 2013. 241/2012.

<sup>67</sup> Article 6.1 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

committed.<sup>68</sup> The court refers to such violations as entrapment,<sup>69</sup> police incitement,<sup>70</sup> or *agent provocateur*<sup>71</sup>.

The ECtHR applies a substantive test to assess the conduct of undercover agents.<sup>72</sup> First, it requires a clear legal framework with sufficient safeguards, similar to those needed for the protection of the right to privacy, as outlined in section 3. The court particularly examines whether the law provides a “clear and foreseeable procedure for authorizing investigative measures”,<sup>73</sup> which, while not necessarily judicial, must exist.<sup>74</sup> This is problematic in France, where cyber infiltration lacks any formal authorization requirement. The court also assesses the supervision of these measures, which may be judicial<sup>75</sup> but could also be conducted by a prosecutor.<sup>76</sup> In France, the prosecutor oversees cyber infiltration,<sup>77</sup>

---

<sup>68</sup> ECtHR. *Ramanauskas v. Lithuania*. 2008. 74420/01.

<sup>69</sup> ECtHR. *Vanyan v. Russia*. 2005. 53203/99.

<sup>70</sup> ECtHR. *Teixeira De Castro v. Portugal*. 1998. 22064/13, 20763/08, 57325/13, 54294/09, 65133/11, 22326/11, 35845/13, 26220/06, 33045/09, 16178/07, 59187/09, 65525/09, 36773/13, 32993/13, 74694/12, 26578/08, 24073/13, 35432/13, 499/08, 46311/09, 77813/12, 25834/10, 58193/10, 9134/10.

<sup>71</sup> ECtHR. *Schenk v. Switzerland*. 1988. 57572/16.

<sup>72</sup> If this first test is not conclusive, the court checks if the applicant had the opportunity to challenge the admissibility of the evidence, an issue that falls outside of the scope of this paper, ECtHR. *Matanović v. Croatia*. 2017. 2742/12; *Bannikova v. Russia*. 2010. 18757/06.

<sup>73</sup> ECtHR. *Teixeira De Castro v. Portugal*. 1998. 22064/13, 20763/08, 57325/13, 54294/09, 65133/11, 22326/11, 35845/13, 26220/06, 33045/09, 16178/07, 59187/09, 65525/09, 36773/13, 32993/13, 74694/12, 26578/08, 24073/13, 35432/13, 499/08, 46311/09, 77813/12, 25834/10, 58193/10, 9134/10.

<sup>74</sup> However criticized by ORMEROD, David; ROBERTS, Andrew. The Trouble with Teixeira: Developing a Principled Approach to Entrapment. *International Journal of Evidence & Proof*. v. 6, n. 1, p. 37–61. 2002. <https://doi.org/10.1177/136571270200600103>.

<sup>75</sup> ECtHR. *Vanyan v. Russia*. 2005. 53203/99.

<sup>76</sup> ECtHR. *Miliniene v. Lithuania*. 2008. 74355/01.

<sup>77</sup> Article 230-46 of the CPP. However, the literature advocates for a judicial supervision of the measure, BRIGANT, Jean-Marie. Mesures d’investigation face au défi numérique en droit français. In: FRANSSSEN, Vanessa; FLORE, Daniel; STASIAK, Frédéric (eds.), *Société numérique et droit pénal : Belgique, France, Europe*. Bruylant, 2019.



whereas in Spain, an investigative judge performs this role.<sup>78</sup> In both countries, the supervising magistrate is either the judge or prosecutor who authorized a traditional infiltration.<sup>79</sup>

Second, the ECtHR scrutinizes the implementation of the operations to ensure agents do “not incite”<sup>80</sup> criminal behavior. This includes examining, on the one side, the behavior of the suspect to establish “objective suspicions” about their involvement in criminal activities.<sup>81</sup> LEAs must demonstrate “good reasons for mounting the covert operation”,<sup>82</sup> such as suspicion or evidence of the suspect’s involvement in the crime under investigation.<sup>83</sup> The mere existence of a criminal record is insufficient;<sup>84</sup> instead, there must be verifiable “pre-existing criminal intent”.<sup>85</sup> On the other side, agents must remain passive participants, merely observing and not provoking the criminal acts. A key factor in this evaluation is the nature of the first contact between the undercover agent and the individual or group under investigation.<sup>86</sup> In virtual worlds, undercover agents must carefully navigate their actions to avoid any conduct that could be classified as entrapment, which would violate the right to a fair trial.

In Spain, undercover agents are exempt from criminal liability for actions taken during their operations, as long as these actions remain proportional and do not amount to “provocation to crime”.<sup>87</sup> The risk of entrapment is particularly high when agents are involved in sharing

---

<sup>78</sup> Article 282 bis.6 of the LEC.

<sup>79</sup> Article 282 bis.1 of the LEC and Article 706-81 of the LEC.

<sup>80</sup> ECtHR. *Khudobin v. Russia*. 2006. 59696/00.

<sup>81</sup> ECtHR. *Bannikova v. Russia*. 2010. 18757/06.

<sup>82</sup> ECtHR. *Ramanauskas v. Lithuania*. 2008. 74420/01.

<sup>83</sup> ECtHR. *Teixeira De Castro v. Portugal*. 1998. 22064/13, 20763/08, 57325/13, 54294/09, 65133/11, 22326/11, 35845/13, 26220/06, 33045/09, 16178/07, 59187/09, 65525/09, 36773/13, 32993/13, 74694/12, 26578/08, 24073/13, 35432/13, 499/08, 46311/09, 77813/12, 25834/10, 58193/10, 9134/10.

<sup>84</sup> ECtHR. *Constantin and Stoian v. Romania*. 2009. 23782/06, 46629/06.

<sup>85</sup> ECtHR. *Vanyan v. Russia*. 2005. 53203/99.

<sup>86</sup> ECtHR. *Sequeira v. Portugal (dec.)*. 2003. 73557/01. ; *Sepil v. Turkey*. 2013. 17711/07.

<sup>87</sup> Article 282 bis.5 of the LEC.

illegal files,<sup>88</sup> but the required judicial authorization is viewed as an appropriate safeguard to assess and mitigate this risk.<sup>89</sup> The regulation of entrapment has largely been left to the courts,<sup>90</sup> with the Spanish High Court setting clear principles, summarized in a 2019 ruling.<sup>91</sup> The court specified that there is not entrapment if the criminal intent existed independently of the agent's involvement. In other words, the agent's role is strictly investigative, reacting to the actions of the suspect rather than inciting them. "The work of the undercover agent does not aim at the commission of the crime. The agent is limited to checking the actions of the subject, collecting evidence of crimes already committed or being committed [...], and even carrying out some activities of collaboration with the investigated person".<sup>92</sup> The court outlined three key elements of entrapment: (1) an objective element, where the agent's provocation leads the target to act in response, with the aim of arresting them; (2) a subjective element, where the agent creates the intent to commit a crime in the suspect; and (3) a material element, where the operation is fully controlled by the police, hence there is no risk or endangerment to the protected legal right.<sup>93</sup>

In France, both infiltration and cyber infiltration provisions prohibits agents from inciting criminal activity.<sup>94</sup> However, the provision

---

<sup>88</sup> VALIÑO CES, Almudena. El agente encubierto informático y la ciberdelincuencia. El intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil. In: BUENO DE MATA, Federico (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*. Granada: Comares, 2016. p. 275–285.

<sup>89</sup> RIZO GÓMEZ, Belén. La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. In: ASECIO MELLADO, José María; FERNÁNDEZ LÓPEZ, Mercedes (eds.), *Justicia penal y nuevas formas de delincuencia*. Tirant lo Blanch, 2017. p. 97–123.

<sup>90</sup> Some authors would prefer to have this topic regulated in the LEC, BELLIDO PENADÉS, Rafael. *La captación de comunicaciones orales directas y de imágenes y su uso en el proceso penal (propuestas de reforma)*. Tirant lo Blanch, 2020.

<sup>91</sup> Tribunal Supremo. 2019. 65/2019.

<sup>92</sup> Tribunal Supremo. 2019. 65/2019.

<sup>93</sup> Tribunal Supremo. 2019. 65/2019.

<sup>94</sup> Articles 706-81 and 230-46 of the CPP.

for cyber infiltration only applies to operations that require prior authorization,<sup>95</sup> which creates inconsistency as any action could potentially result in entrapment. French law operates under the principle of freedom of proof, and all evidence must be obtained fairly.<sup>96</sup> However, the French High Court's case law on entrapment has been inconsistent.<sup>97</sup> In one case involving a child pornography website created by the US LEAs, which identified<sup>98</sup> one offender in France, the court initially ruled the evidence inadmissible as well as all subsequent evidence.<sup>99</sup> In a subsequent ruling in the same case, the court confirmed that the evidence was unfair as there was no prior suspicion.<sup>100</sup> In another case involving a forum for bank card fraud created by US LEAs, which identified one user located in France, the court admitted the evidence, despite the absence of prior suspicion, due to the suspect's active participation.<sup>101</sup> This suggests that the court places greater emphasis on the suspect's demonstrated criminal intent. The mere connection to a child pornography website does not prove the criminal intent; based on the principle *in dubio pro reo*, a connection can be interpreted as a mistake.<sup>102</sup> In contrast, if the suspect actively

---

<sup>95</sup> Article 230-46.3° and 4° of the CPP.

<sup>96</sup> Article 427 of the CPP.

<sup>97</sup> QUÉMÉNER, Myriam. Les spécificités juridiques de la preuve numérique. *Actualité juridique Pénal*. p. 63, 2014; PERRIER, Jean-Baptiste. Le fair-play de la preuve pénale. *Actualité juridique Pénal*. p. 436, 2017; LEPAGE, Agathe. Provocation sur Internet - La distinction entre provocation à la preuve et provocation à la commission d'une infraction à l'épreuve d'Internet. *Communication Commerce électronique*. n. 9, 2014. For a list of case law admitting or excluding fair or unfair proofs, see VLAMYNCK, Hervé. La loyauté de la preuve au stade de l'enquête policière. *Actualité juridique Pénal*. p. 325, 2014.

<sup>98</sup> The loyalty of proof applies to all the evidence brought to the court, independently of whether it was obtained by French law enforcement authorities or abroad.

<sup>99</sup> Cour de cassation. 2007. 06-87.753.

<sup>100</sup> Cour de cassation. 2008. 08-81.045.

<sup>101</sup> Cour de Cassation 2014. 13-88.162.

<sup>102</sup> FRANCILLON, Jacques. Infractions relevant du droit de l'information et de la communication. *Revue de science criminelle et de droit pénal comparé*. v. 2014/3. n. 3. p. 577, 2014. <https://doi.org/10.3917/rsc.1403.0577>; BUISSON, Jacques. Contrôle de l'éventuelle provocation policière : création d'un site pédo-pornographique un policier, même étranger. *Revue de science criminelle et de droit pénal comparé*. p. 663, 2008.

writes messages after accepting an invitation to join a forum, it proves their criminal intent. The court utilizes evidence on the *actus reus* to demonstrate the *mens rea*. A further case involved blackmail over a sex tape, where a police officer posed as a friend of the victim to gather evidence. Initially, the High Court ruled the operation unfair due to the officer's use of a pseudonym and his initiation of some conversations,<sup>103</sup> but a later ruling reversed this, stating that the crime would have occurred regardless of the agent's actions.<sup>104</sup> This lack of consistency in French case law creates legal uncertainty for both infiltration and cyber infiltration operations. In France, the distinction between a lawful undercover operation and entrapment remains unclear.

European and national case law on entrapment will thus have a significant impact on how undercover agents operate in virtual worlds. Although they are granted considerable powers, it remains ambiguous which actions require additional authorization. Such authorizations are crucial for determining whether an agent's conduct could amount to entrapment.

## 5. CONCLUSIONS

The rapid evolution of virtual worlds as integral components of daily human activities necessitates a parallel development in the capabilities of LEAs to operate in these environments. As criminal behaviors extend into virtual realms, LEAs will increasingly seek to conduct undercover operations within these spaces, enabling them to gather evidence and assess risks without always relying on data requests to online service providers. Legal frameworks for traditional and cyber infiltration provide significant opportunities to investigate criminal activities in virtual worlds. On the one hand, traditional infiltration grants broader powers to undercover agents, which may align well with the complex dynamics of virtual worlds. On the other hand, cyber infiltration frameworks offer a more flexible scope, allowing investigations into a wider range of offenses,

---

<sup>103</sup> Cour de cassation. 2017. 17-80.313.

<sup>104</sup> Cour de cassation. 2019. 18-86.767.

particularly those committed online. Undercover agents will likely play a crucial role, either by adapting traditional infiltration techniques to the virtual sphere or through the use of the cyber infiltration, the latter being particularly well-suited to the nature of many virtual platforms. However, the immersive qualities of virtual environments—amplified by technological advancements that blur the lines between the physical and digital—may make the case for extending physical infiltration frameworks into these virtual settings. In virtual worlds, undercover agents may operate with a dual nature: acting physically-like by transporting virtual objects or virtually-like by exchanging data. This hybrid nature highlights the need for a fusion of legal frameworks that govern both traditional and cyber infiltration.

Such a merger is further justified by the shared challenges that these forms of infiltration face, particularly in avoiding entrapment and ensuring that the agents' conduct remains within legal boundaries. Indeed, these expanded opportunities raise concerns about the right to privacy and the right to a fair trial, especially when there is a lack of clear authorization procedures or limits on the duration of operations, as emphasized by the ECtHR. To ensure proportionality, the law must clearly define the scope, duration, and authorization of undercover operations, with particular attention to avoiding entrapment. Moving forward, a mixed regime that combines elements of both traditional and cyber infiltration may be necessary to navigate the unique affordances of virtual worlds while safeguarding fundamental rights. One area that requires urgent attention is the authorization and oversight processes, which currently do not adequately consider the public interest, or the severity of the potential rights violations involved. The regulation of undercover agents follows a binary division between their implementation offline or online and does not take into account the types and amount of data that can be gathered. This challenge is further compounded in virtual worlds, where the absence of geographical limitations allows LEAs unprecedented access to any digital space, complicating the application of traditional or cyber infiltration measures. Jurisdictional boundaries, which are well-defined in the physical world, become ambiguous in virtual spaces, raising proportionality concerns for national law enforcement efforts. Existing frameworks for both traditional and cyber infiltration

fail to address this complexity, necessitating a thorough reevaluation of how LEAs operate across virtual borders. Tackling these challenges is critical to ensure the admissibility of evidence in court.

This paper provides an introductory reflection on the need to adapt criminal procedure to accommodate investigations in virtual worlds, but much remains to be explored. Key unresolved issues include the admissibility of evidence collected in virtual environments and the potential conflicts with the right to privacy and the right to a fair trial, as studied here. The ECtHR has emphasized that the regulation of such matters is primarily the responsibility of national laws,<sup>105</sup> yet this remains a contentious issue in the context of cross-border criminal cooperation within the EU. The European Law Institute's Proposal for a Directive on the Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings marks a step forward, but further refinement is needed.<sup>106</sup>

Additional challenges arise when virtual operations translate into physical courtroom procedures, such as ensuring a fair trial, protecting the identity of undercover agents (whether through anonymous or open testimony), and managing the vast amount of data collected.<sup>107</sup> Future legal challenges may also emerge from novel forms of infiltration, such as law enforcement-controlled bots or invisible avatars operating within virtual spaces. Moreover, the visible presence of law enforcement in virtual worlds, where agents are identified as such, introduces new dilemmas—particularly concerning their interactions with private policing entities, which are becoming more prevalent in these environments.

In conclusion, as LEAs expand their operations into virtual worlds, the balance between effective policing and the protection of fundamental rights must be carefully managed. The proliferation of surveillance, whether conducted by public or private actors, underscores the urgent

---

<sup>105</sup> ECtHR. *Schenk v. Switzerland*. 1988. 57572/16.

<sup>106</sup> BACHMAIER WINTER, Lorena and SALIMI, Farsam. P-2020-21: *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings. Draft Legislative Proposal of the European Law Institute*. European Law Institute, 2023.

<sup>107</sup> ECtHR. *Van Wesenbeeck v. Belgium*. 2017. 67496/10, 52936/12. See Article 282 bis.2 of the LEC and Articles 706-86 and 706-87 of the CPP.

need for a comprehensive regulatory framework that addresses these novel challenges while safeguarding the fundamental rights of individuals.

## REFERENCES

ART. 29 WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. EU, 2007.

BACHMAIER WINTER, Lorena. Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: algunas cuestiones sobre el principio de proporcionalidad. In: CEDEÑO HERNÁN, Marina (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*. Cizur Menor (Navarra) : Aranzadi, 2017.

BACHMAIER WINTER, Lorena; SALIMI, Farsam. P-2020-21: *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings. Draft Legislative Proposal of the European Law Institute*. European Law Institute, 2023.

BELLIDO PENADÉS, Rafael. *La captación de comunicaciones orales directas y de imágenes y su uso en el proceso penal (propuestas de reforma)*. Tirant lo Blanch, 2020.

BOVENZI, Gian Marco. MetaCrimes: Criminal accountability for conducts in the Metaverse. In: *Companion Proceedings of the ACM Web Conference 2023*. New York, NY, USA: Association for Computing Machinery, 2023. p. 565–567. <https://doi.org/10.1145/3543873.3587535>

BRIGANT, Jean-Marie. Mesures d’investigation face au défi numérique en droit français. In: FRANSSEN, Vanessa; FLORE, Daniel; STASIAK, Frédéric (eds.), *Société numérique et droit pénal : Belgique, France, Europe*. Bruylant, 2019.

BUENO DE MATA, Federico. *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*. Cizur Menor (Navarra): Thomson Reuters Aranzadi, , 2019.

BUISSON, Jacques. Contrôle de l’éventuelle provocation policière : création d’un site pédo-pornographique un policier, même étranger. *Revue de science criminelle et de droit pénal comparé*. p. 663, 2008.

CAROU-GARCÍA, Sara. Cibercriminalidad e investigación policial. El agente encubierto informático. In: SANZ DELGADO, Enrique; FERNÁNDEZ BERMEJO, Daniel (eds.), *Tratado de delincuencia cibernética*. Thomson Reuters Aranzadi, 2021. p. 825–864.

Cour de cassation. 2007. 06-87.753; 2008. 08-81.045; 2014. 13-88.162; 2016. 16-81.834; 2017. 17-80.313; 2019. 18-86.767

DANAHER, John. The law and ethics of virtual sexual assault. In: BARFIELD, Woodrow; BLITZ, Marc J. (eds.). *Research Handbook on the Law of Virtual and Augmented Reality*. Edward Elgar Publishing, 2018. p. 363–388.

DEL POZO PÉREZ, Marta. El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de enjuiciamiento criminal española. *Criterio jurídico*. n. 6, p. 267–310, 2006.

DREMLIUGA, Roman; PRISEKINA, Natalia; YAKOVENKO, Andrei. New Properties of Crimes in Virtual Environments. *Advances in Science, Technology and Engineering Systems Journal*. v. 5, n. 6, p. 1727–1733, 2020. <https://doi.org/10.25046/aj0506206>

ECJ, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*. 2014. C-293/12, C-594/12; *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH*. 2022. C-793/19, C-794/19.

ECtHR. *Klass and others v. Germany*. 1978. 5029/71; *Leander v. Sweden*. 1987. 9248/81; *Schenk v. Switzerland*. 1988. 57572/16; *Kruslin v. France*. 1990. 11801/85; *Teixeira De Castro v. Portugal*. 1998. 22064/13, 20763/08, 57325/13, 54294/09, 65133/11, 22326/11, 35845/13, 26220/06, 33045/09, 16178/07, 59187/09, 65525/09, 36773/13, 32993/13, 74694/12, 26578/08, 24073/13, 35432/13, 499/08, 46311/09, 77813/12, 25834/10, 58193/10, 9134/10; *Sequeira v. Portugal (dec.)*. 2003. 73557/01; *Vanyan v. Russia*. 2005. 53203/993; *Weber and Saravia v. Germany*. 2006. 54934/00; *Khudobin v. Russia*. 2006. 59696/00; *Ramanauskas v. Lithuania*. 2008. 74420/01; *Miliniene v. Lithuania*. 2008. 74355/01; *Constantin and Stoian v. Romania*. 2009. 23782/06, 46629/06; *Bannikova v. Russia*. 2010. 18757/06; *Moulin v. France*. 2010. 37104/06; *Amann v. Switzerland*. 2011. 27798/95; *Sepil v. Turkey*. 2013. 17711/07; *Szabó and Vissy v. Hungary*. 2016. 37138/14; *Matanović v. Croatia*. 2017. 2742/12; *Van Wesenbeeck v. Belgium*. 2017. 67496/10, 52936/12; *Centrum För Rättvisa v. Sweden*. 2021. 35252/08; *Big Brother Watch and others v. the United Kingdom (2)*. 2021. 58170/13, 62322/14, 24960/15.

EL-KADY, Ramy Metwally. Investigating Forensic Evidence in Metaverse: A Comparative Analytical Study. In: ELSHENRAKI, Hossam Nabil. *Forecasting Cyber Crimes in the Age of the Metaverse*. IGI Global, 2024. p. 227–258.

ELSHENRAKI, Hossam Nabil. *Forecasting Cyber Crimes in the Age of the Metaverse*. IGI Global, 2023.



EUROPEAN COMMISSION. COM(2023) 442/final: *Communication - An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition*. EU, 2023.

FRANCILLON, Jacques. Infractions relevant du droit de l'information et de la communication. *Revue de science criminelle et de droit pénal comparé*. v. 2014/3. n. 3. p. 577, 2014. <https://doi.org/10.3917/rsc.1403.0577>.

HABER, Eldar. *The Criminal Metaverse*. *Indiana Law Journal*. v. 99, n. 3, p. 843–891. 2024.

EUROPOL. *Policing in the metaverse: what law enforcement needs to know : an observatory report from the Europol innovation lab*. Publications Office, 2022. Available at: <<https://data.europa.eu/doi/10.2813/81062>>. Access on: September 18, 2023.

EXPÓSITO LÓPEZ, Lourdes. El agente encubierto. *Revista de derecho UNED*. n. 17, p. 251–286, 2015. <https://doi.org/10.5944/rduned.17.2015.16277>.

GODEFROY, Thierry. The Control of Organised Crime in France: A Fuzzy Concept but a Handy Reference. In: FIJNAUT, Cyrille; PAOLI, Letizia (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*. Springer, 2006. p. 763.

GONZÁLEZ-CASTELL, Adán Carrizo. La infiltración policial en España como medio de investigación en la lucha contra la corrupción. *Revista Brasileira de Direito Processual Penal*. v. 3, n. 2, p. 511–536. 2017. <https://doi.org/10.22197/rbdpp.v3i2.64>.

HALLEVY, Gabriel. Criminal liability for intellectual property offenses of artificially intelligent entities in virtual and augmented reality environments. In: BARFIELD, Woodrow; BLITZ, Marc J. (eds.). *Research Handbook on the Law of Virtual and Augmented Reality*. Edward Elgar Publishing, 2018. p. 389–419.

KARAPATAKIS, Andreas. Virtual worlds and money laundering under EU law: The inadequacy of the existing legal framework and the challenges of regulation. *New Journal of European Criminal Law*. v. 10, n. 2, p. 128–150, 2019. <https://doi.org/10.1177/2032284419841711>.

KIM, Donghyun; OH, Subin; SHON, Taeshik. Digital forensic approaches for metaverse ecosystems. *Forensic Science International: Digital Investigation*. v. 46, p. 301608, 2023. <https://doi.org/10.1016/j.fsidi.2023.301608>.

LEPAGE, Agathe. Provocation sur Internet - La distinction entre provocation à la preuve et provocation à la commission d'une infraction à l'épreuve d'Internet. *Communication Commerce électronique*. n. 9, 2014.

LEÓN CAMINO, Arantza. Modo de actuación del agente encubierto virtual. *Claves Jurídicas*. n. 1, p. 28–48, 2024.

LEVINE, Alec. Play Harms: Liability and the Play Conceit in Virtual Worlds Comment. *McGeorge Law Review*. v. 41, n. 4, p. 929–966, 2009.

LÓPEZ-BARAJAS PEREA, Inmaculada. El derecho a la protección del entorno virtual y sus límites. El registro de los sistemas informáticos. In: BUENO DE LA MATA, Federico; DÍAZ MARTÍNEZ, Manuel; LÓPEZ-BARAJAS PEREA, Inmaculada (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*. Valencia: Tirant lo blanch, 2018. p. 135–168.

MALHOTRA, Vinayak. That's Assault! Extension of Criminal Law to the Metaverse. *SSRN Scholarly Paper*. 2023. <https://doi.org/10.2139/ssrn.4595652>.

MAYAUD, Yves. Terrorisme – Poursuites et indemnisation. *Répertoire de droit pénal et de procédure pénale*. 2023.

MCKENZIE MARSHALL, Angus; TOMPSETT, Brian Charles. The metaverse— Not a new frontier for crime. *WIREs Forensic Science*. v. 6, n. 1, p. e1505, 2024. <https://doi.org/10.1002/wfs2.1505>.

NADELMANN, Ethan. *Cops Across Borders - The Internationalization of U.S. Criminal Law Enforcement*. Pennsylvania: Penn State University Press, 1993.

ORMEROD, David; ROBERTS, Andrew. The Trouble with Teixeira: Developing a Principled Approach to Entrapment. *International Journal of Evidence & Proof*. v. 6, n. 1, p. 37–61, 2002. <https://doi.org/10.1177/136571270200600103>.

PERRIER, Jean-Baptiste. Le fair-play de la preuve pénale. *Actualité juridique Pénal*. p. 436, 2017.

QUÉMÉNER, Myriam. Fasc. 1110 : Infiltrations numériques et enquêtes sous pseudonyme. *JurisClasseur Communication*. 2024; Les spécificités juridiques de la preuve numérique. *Actualité juridique Pénal*. p. 63, 2014.

RIZO GÓMEZ, Belén. La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

In: ASECIO MELLADO, José María; FERNÁNDEZ LÓPEZ, Mercedes (eds.), *Justicia penal y nuevas formas de delincuencia*. Tirant lo Blanch, 2017. p. 97–123.

ROUSSEL, Bruno. *Les investigations numériques en procédure pénale*. PhD thesis. Université de Bordeaux, 2020. Available at: <<https://theses.hal.science/tel-02947825>>. Access on: November 8, 2023.

SÁNCHEZ GONZÁLEZ, Susana. Investigar los delitos en la red a través del agente encubierto informático. In: MERINO CALLE, Irene; HERNÁNDEZ LÓPEZ, Alejandro; LARO GONZÁLEZ, María Elena (eds.), *Desafíos del derecho en la sociedad actual: reflexiones y propuestas*. Ediciones Universidad de Valladolid, 2022. p. 267–278; Investigar y castigar la pornografía infantil gracias al agente encubierto informático. *La ley penal: revista de derecho penal, procesal y penitenciario*. n. 154, p. 3, 2022; El agente encubierto informático en la lucha contra la pornografía infantil. In: GARRIDO CARRILLO, Francisco Javier; FAGGIANI, Valentina (eds.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital*. Thomson Reuters Aranzadi, 2022. p. 367–390.

SCHAENGOLD, Zachary. Personal Jurisdiction over Offenses Committed in Virtual Worlds Comments and Casenotes. *University of Cincinnati Law Review*. v. 81, n. 1, p. 361–386, 2012.

SEO, Seunghye; SEOK, Byoungjin; LEE, Changhoon. Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing*. v. 79, n. 9, p. 9467–9485, 2023. <https://doi.org/10.1007/s11227-023-05045-1>.

SINGH, Prachi; RAJPUT, Dev Karan. Metaverse: Surging Need for Competent Laws with Increasing Metaverse Crimes. *International Journal of Law Management & Humanities*. v. 5 Issue 5, p. 712-724, 2022. <https://doi.org/10.1000/IJLMH.113621>.

TOSZA, Stanislaw. Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review*. v. 43, p. 105614, 2021. <https://doi.org/10.1016/j.clsr.2021.105614>; Mutual Recognition By Private Actors In Criminal Justice? E-Evidence Regulation And Service Providers As The New Guardians Of Fundamental Rights. *Common Market Law Review*. v. 61, n. 1, 2024. <https://doi.org/10.54648/cola2024005>.

Tribunal Supremo. 2009. 154/2009; 2013. 241/2012; 2019. 65/2019.

UNODC. *Comprehensive Study on Cybercrime*. United Nations, 2013.

VALIÑO CES, Almudena. El agente encubierto informático y la ciberdelincuencia. El intercambio de archivos ilícitos para la lucha contra los delitos de pornografía

infantil. In: BUENO DE MATA, Federico (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*. Granada: Comares, 2016. p. 275–285.

VELASCO NÚÑEZ, Eloy; SANCHÍS CRESPO, Carolina. *Delincuencia informática: tipos delictivos e investigación: con jurisprudencia tras la reforma procesal y penal de 2015*. Tirant lo Blanch, 2019.

VERGÈS, Etienne. La notion de criminalité organisée après la loi du 9 mai 2004. *Actualité juridique Pénal*. p. 181, 2004.

VILLAMARÍN LÓPEZ, María Luisa. La nueva figura del agente encubierto online en la lucha contra la pornografía infantil. Apuntes desde la experiencia en Derecho Comparado. In: CEDEÑO HERNÁN, Marina (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*. Cizur Menor (Navarra): Aranzadi, 2017.

VILLAR FUENTES, Isabel. El agente encubierto informático: reto legislativo pendiente en un escenario digitalizado. *Revista de Estudios Jurídicos y Criminológicos*. n. 6, p. 197–228, 2022.

VLAMYNCK, Hervé. La loyauté de la preuve au stade de l'enquête policière. *Actualité juridique Pénal*. p. 325, 2014.

YADIN, Gilad. Beyond unauthorized access: laws of virtual reality hacking. In: ARFIELD, Woodrow; BLITZ, Marc J. (eds.). *Research Handbook on the Law of Virtual and Augmented Reality*. Edward Elgar Publishing, 2018. p. 340–362.

YALCIN-ISPIR, Aybike. The Metaverse and Terrorism. In: ESEN, Fatih Sinan; TINMAZ, Hasan; SINGH, Madhusudan (eds.), *Metaverse: Technologies, Opportunities and Threats*. Singapore: Springer Nature, 2023. p. 275–284.

### **Authorship information**

Salomé Lannier. Postdoctoral researcher at the University of Luxemburg. PhD in Private Law and Criminal Sciences. [salome.lannier@uni.lu](mailto:salome.lannier@uni.lu)

### **Additional information and author's declarations (scientific integrity)**

*Conflict of interest declaration:* the author confirms that there are no conflicts of interest in conducting this research and writing this article.

*Declaration of authorship:* all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

*Declaration of originality:* the author assures that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; she also attests that there is no third party plagiarism or self-plagiarism.

### **Editorial process dates**

(<https://revista.ibraspp.com.br/RBDPP/about>)

- Submission: 19/07/2024
- Desk review and plagiarism check: 30/07/2024
- Review 1: 16/08/2024
- Review 2: 21/08/2024
- Preliminary editorial decision: 28/09/2024
- Correction round return: 02/10/2024
- Final editorial decision: 12/10/2024

### **Editorial team**

- Editor-in-chief: 1 (VGV)
- Reviewers: 2

**HOW TO CITE (ABNT BRAZIL):**

LANNIER, Salomé. Infiltrating virtual worlds. The regulation of undercover agents through fundamental rights. *Revista Brasileira de Direito Processual Penal*, vol. 10, n. 3, e1066, set./dez. 2024. <https://doi.org/10.22197/rbdpp.v10i3.1066>



*License Creative Commons Attribution 4.0 International.*