RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0248 • articolo sottoposto a peer review • pubblicato in anteprima il 5 dic. 2025

María Dolores García Sánchez

The virtual restraining order as a novel cyber precautionary measure to combat online crime

In light of the increasing digitalization of criminal conduct, the necessity of proportionate and effective precautionary measures has become a critical concern in contemporary criminal justice. Accordingly, this research explores the extent to which traditional precautionary frameworks can be adapted to address the unique challenges posed by cybercrime while ensuring compliance with fundamental rights. The examination of precautionary measures within the digital sphere, with particular emphasis on what we define as cyber-precautionary measures, constitutes a fundamental aspect of contemporary criminal justice. This study adopts a progressive analytical approach, commencing with a general overview of this emerging category of precautionary measures in criminal proceedings before advancing to an in-depth analysis of a novel proposal: the virtual restraining order. The research further investigates the technical and legal feasibility of this new cyber-precautionary measure, as well as the role of Internet Service Providers in implementing it. Subsequently, the discussion will focus on the specific legal and practical dimensions of this measure, with particular attention to its implications for fundamental rights, the principle of proportionality, and its practical implementation.

Cyber-precautionary measures – Cybercrime – Virtual restraining order – Fundamental rights – Proportionality

L'ordine di allontanamento virtuale come nuova misura cautelare cibernetica per combattere il crimine online

Alla luce della crescente digitalizzazione delle condotte criminali, la necessità di misure cautelari proporzionate ed efficaci è diventata una questione cruciale nella giustizia penale contemporanea. Di conseguenza, questa ricerca esplora quanto le misure cautelari tradizionali possano essere adattate per affrontare le sfide uniche poste dalla criminalità informatica, garantendo al contempo il rispetto dei diritti fondamentali. L'analisi delle misure cautelari nell'ambito digitale, con particolare enfasi su quelle che definiamo misure cibernetiche, costituisce un elemento fondamentale della giustizia penale contemporanea. Questo studio adotta un approccio analitico progressivo, partendo da una panoramica generale di questa categoria emergente di misure cautelari nei procedimenti penali, per poi approfondire una proposta innovativa: l'ordine di restrizione virtuale. La ricerca esamina inoltre la fattibilità tecnica e giuridica di questa nuova misura cibernetica cautelare, nonché il ruolo dei fornitori di servizi Internet nella sua attuazione. Successivamente, la discussione si concentrerà sugli aspetti giuridici e pratici specifici di questa misura, con particolare attenzione alle sue implicazioni per i diritti fondamentali, il principio di proporzionalità e la sua applicazione pratica.

Misure cautelari cibernetiche – Criminalità informatica – Ordine di allontanamento virtuale
Diritti fondamentali – Proporzionalità

The author is Postdoctoral Research Professor at the University of Seville, Spain

The present study has been conducted within the framework of the 2021 Predoctoral Grant (PAIDI 2020), funded by the Regional Ministry of Economic Transformation, Industry, Knowledge, and Universities of the Government of Andalusia (PREDOC_02268)

1. Introduction

The increasing digitalization of criminal conduct has exposed the limitations of precautionary frameworks traditionally designed for an analog and territorially bounded environment. Whereas classical precautionary measures target individual's personal freedom or economic assets, the dynamics of cyberspace – characterized by anonymity, deterritorialization, and ubiquity – demand novel responses capable of addressing new forms of victimization and safeguarding the integrity of digital evidence. This evolving landscape calls for the reconceptualization of precautionary action, moving beyond conventional instruments to a set of cyber-precautionary measures specifically tailored to the challenges of online crime.

The present study introduces the proposal of a virtual restraining order as a distinctive cyber-precautionary measure. The aim of this instrument is to restrict an investigated individual's access to certain digital spaces in order to prevent reoffending, reduce impunity, and reinforce the protection of victims' rights in the online sphere.

The relevance of this proposal lies not only in its pragmatic orientation but also in its theoretical contribution to the debate on the modernization of criminal procedure in the digital age. By examining its legal feasibility, proportionality requirements, and practical implementation this study seeks to evaluate the potential of the virtual restraining order to operate as a proportionate and rights-compliant response to cybercrime. In doing so, it aims to contribute to the broader discussion on how criminal justice systems can adapt to technological transformations without compromising fundamental rights.

Accordingly, this research seeks to answer the following question: to what extent can the introduction of a virtual restraining order be framed as an effective and legally viable cyber-precautionary measure that complies with the principle of proportionality in combating cybercrime? Addressing this question requires an interdisciplinary perspective that combines doctrinal analysis, jurisprudential developments, and technological considerations.

The paper is structured as follows. First, it sets out the methodological premises, describing the analytical approach and the sources of law and doctrine employed. Second, it offers preliminary considerations, delimiting the concept of cyber-precautionary measures as a new category distinct from traditional mechanisms. Third, it develops the central proposal of the virtual re-

straining order, examining (a) its definition and nature, (b) its implications for fundamental rights and the principle of proportionality, including the necessity of judicial authorization, and (c) the technical and practical aspects of its implementation, with specific reference to the role of Internet Service Providers. Finally, the article presents its conclusions, evaluating the feasibility, limitations, and potential contributions of the measure to the modernization of criminal procedural law in the digital environment.

2. Methodological premises

This study undertakes a comprehensive examination of precautionary measures within the realm of cybercrime, with a particular focus on the adoption and legal implications of cyber-specific precautionary mechanisms such as the virtual restraining order.

Methodologically, for this research we employ an analytical and deductive approach, progressing from a general overview of precautionary measures in criminal proceedings to an in-depth assessment of their applicability to cybercrime cases. Additionally, we adopt a critical and proactive stance, aiming not only to assess current regulatory and jurisprudential developments but also to propose concrete legal and technical solutions to enhance the effectiveness of this virtual restraining order as a cyber-precautionary measure. A central emphasis is placed on the principle of proportionality as the guiding criterion for evaluating the necessity, suitability, and proportionality in the strict sense of digital restrictions.

In terms of methodological techniques, our study relies primarily on jurisprudential analysis, ensuring a thorough examination of relevant judicial decisions at the national, European and international levels. This is complemented by an extensive review of legal texts, including the Spanish Constitution, organic and ordinary laws, European regulations, and pertinent international treaties. Furthermore, by integrating recent academic discourse on digital evidence, cybersecurity, and judicial cooperation this research aims to contribute to the ongoing legal and theoretical debate on the adaptation of precautionary measures to the evolving landscape of cybercrime.

3. Preliminary considerations: cyber-precautionary measures as a new category of precautionary measures

The distinctive characteristics of digital interactions – particularly anonymity, ubiquity, and deterritorialization – have facilitated the rapid expansion of new forms of criminal activity in cyberspace. As a dynamic and adaptive normative system, Law must provide effective responses to these evolving criminological challenges. Such adaptation must occur in parallel with technological advancements, addressing the inherent risks and threats they entail.

In a globalized world, the absence of physical boundaries in cyberspace enables the commission of crimes beyond geographical borders, underscoring the need for transnational prevention and prosecution strategies. These strategies must overcome jurisdictional fragmentation and reduce impunity. The complexity of investigating and prosecuting cybercrimes, coupled with their high impunity rates[1], highlights the importance of prevention and the adoption of precautionary measures suited to the digital landscape. Consequently, precautionary regulations must be tailored to the specific challenges of cyberspace and the demands of a technologically evolving society. The dynamic nature of cybercrime requires a flexible and effective precautionary framework aimed at preserving digital evidence, preventing recidivism, and protecting victims throughout the criminal process.

Within this context, an expanded and redefined concept of precautionary measures emerges, specifically adapted to the peculiarities of cybercrime. Traditional precautionary measures, designed for the physical world, are primarily aimed at restricting individuals, either through limitations on personal freedom or on economic assets. By contrast, in the online environment, the immediate object of criminal conduct lies in digital elements – such as data, content, communication channels, or online platforms – that require a different form of intervention. This mismatch highlights the need for a new category of instruments: cyber-precautionary measures.

Cyber-precautionary measures encompass those adopted in response to illicit conduct per-

1. The "unrecorded" crime rate.

petrated in cyberspace, facilitated by or involving the use of the Internet and ICTs. Given the altered spatiotemporal parameters of this digital realm, these measures are conceptually distinct from conventional precautionary mechanisms designed for the analogue world. Their defining feature rests upon their function: to block, restrict, or remove unlawful digital content, ensuring its preservation for judicial purposes, while simultaneously protecting victims from the ongoing harm and revictimization associated with its continued availability online.

At first glance, the conceptual distinction appears straightforward: while traditional precautionary measures are person-oriented, cyber-precautionary measures are object-oriented, focusing on illicit electronic content or virtual spaces rather than directly on the alleged offender. However, this distinction requires careful refinement. Although cyber-precautionary measures are formally directed at digital "objects" (e.g., unlawful data, websites, or platforms), the implementation of certain measures may indirectly entail restrictions on individuals, since human interaction is the medium through which such digital objects are accessed, disseminated, and operationalized.

This tension becomes particularly evident in the case of the novel virtual restraining order we propose in this study (which will be examined in greater detail below). It represents the clearest point of friction between the person-oriented logic of traditional precautionary measures and the object-oriented nature of cyber-precautionary interventions. As a precautionary order, it must be issued against a specific individual and therefore retains an unavoidable personal dimension. Yet, its operational content remains object-centered: what is restricted is not the individual's ambulatory freedom, but their capacity to access, generate, or interact with defined digital spaces and electronic content. In other words, the measure targets the virtual space (the "object"), while its personal consequences materialize only as a derivative effect (namely, the prohibition of accessing that environment). This dual structure is unique to virtual restraining orders and explains why they occupy a hybrid conceptual position within the broader category of cyber-precautionary measures.

By contrast, other cyber-precautionary instruments – such as content removal, blocking orders, or data preservation – can be adopted even in the absence of an identified suspect, since their aim is to neutralize the circulation, persistence, or evidentiary vulnerability of illicit digital content. Such measures thus confirm the autonomous object-orientation of cyber-precautionary action and clearly differentiate it from the traditional framework, where precautionary powers are primarily exercised upon the person in the analogue sphere.

On this basis, the apparent conceptual tension does not undermine the coherence of cyber-precautionary measures, provided that their objectivization is explicitly articulated. The key differentiating factor is not the total absence of personal impact, but the locus of the legal intervention: whereas traditional precautionary measures directly curtail personal liberty in the physical world, cyber-precautionary measures operate in the digital domain, acting upon electronic data, online infrastructures, and virtual environments, with personal restrictions arising only as a secondary and indirect consequence. This object-centered and digitally-grounded design aligns with the structural aims of contemporary criminal procedure in cyberspace, where the urgency lies in preventing the dissemination of illicit content, preserving digital evidence, and mitigating ongoing victimization.

From this perspective, cyber-precautionary measures align with an expanded conception of precautionary action characterized by a dual function: (1) an evidentiary-preservation function, aimed at preventing the destruction or alteration of digital evidence, and (2) a preventive and restorative protective function, designed to halt or mitigate criminal activity while safeguarding the rights and interests of victims.

Given their potential to affect freedom of expression, privacy, and Internet access, cyber-precautionary measures must operate under the principle of proportionality, which functions as both a limiting and legitimizing norm.

Specifically, the proportionality test entails three cumulative requirements[2]: (1) Suitability, whereby the measure must be capable of achieving its legitimate aim; (2) Necessity, ensuring that no less intrusive

2. See , SSTC 66/1995; 55/1996; 207/1996;152/1996.

alternative exists; and (3) Proportionality *stricto sensu*, demanding that the interference with rights not exceed what is strictly required to meet its objectives.

This principle establishes a stringent threshold of judicial justification for any restriction of digital liberties. Accordingly, precautionary measures must be narrowly defined, exceptional in scope, and subject to continuous judicial oversight. Their legitimacy depends on a demonstrable connection between the imposed limitation and the protection of compelling public interests, notably the preservation of digital evidence and the prevention of further victimization.

As Alexy[3] has emphasized, proportionality transforms judicial discretion into a structured reasoning process, enhancing transparency, rationality and normative coherence. Likewise, Jackson[4] points out that proportionality operates as a *bridge principle* between decision making in courts and decision making by the people, legislatures and public officials. This interpretative framework ensures that the exercise of coercive state powers in the digital domain remains anchored in constitutional guarantees, even amidst rapidly evolving technological contexts.

Thus, proportionality not only circumscribes the reach of cyber-precautionary powers but also legitimizes them when strictly necessary to preserve digital evidence, prevent reoffending, and protect victims from renewed harm. In this dual role – constraint and justification – the principle stands as the doctrinal keystone of a precautionary model suited to the complex normative demands of the digital age.

Ultimately, the fight against cybercrime demands an updated precautionary framework capable of effectively addressing the distinctive challenges of the digital environment. Without a prompt and reinforced precautionary system, the effectiveness of investigative techniques is severely compromised, resulting in heightened levels of impunity and diminished victim protection. The evolution of cybercrime necessitates moving beyond outdated regulatory frameworks and advancing toward a precautionary model suited to the complexities of the digital age.

Within the Spanish legal framework, cyber-precautionary measures include those established under Article 13.2 of the Criminal Procedure Act (LECrim), which provide for content removal, access blocking, and service suspension, as well as the data preservation order set forth in Article 588-*octies* LECrim. However, given the rapid advancement of technology and the corresponding evolution of cybercriminal tactics, additional precautionary measures of this nature are required. Specifically, we propose the introduction of a "virtual restraining order", designed to restrict an investigated individual's access to specific digital spaces or online platforms associated with the victim or the offence. The conceptualization and development of this measure will be the focus of the following sections.

4. The virtual restraining order as a novel cyber-precautionary measure

4.1. Definition

The virtual restraining order can be defined as a measure designed to restrict contact, access to existing online content, or the generation of illicit online material by limiting the use of the medium through which the alleged criminal act is committed (namely, the Internet). It operates as a preventive mechanism intended to protect victims and prevent reoffending in cases where online interaction constitutes the means or context of the offence. This measure is particularly relevant in cases of cyberstalking, cyberbullying, and other unlawful behaviors perpetrated through digital means.

In Spain, the Supreme Court (TS) has provided a jurisprudential interpretation of restrictions on contact in the online sphere. Specifically, ruling 547/2022, of June 2, extends the prohibition of "contacting by any means" with the victim to include restrictions on the defendant's access to "computer locations" frequented by the victim. A detailed analysis of this ruling and its implications will be addressed later.

However, the novel precautionary measure proposed here offers an additional level of protection for victims and contributes to the prevention of repeat offenses. Firstly, it would not rely solely on jurisprudential interpretation, thereby providing greater legal certainty through the establishment of clearly defined conditions, requirements, and

3. Alexy 2002.
4. Jackson 2015.

principles for its application within the legal framework. Moreover, this virtual restraining order would extend beyond direct communication between the accused and the victim to encompass virtual spaces frequented by the victim, even in the absence of explicit interaction. The mere simultaneous presence of both parties in the same digital environment could suffice to activate the order. In this context, the psychological and relational dimension of harm[5] experienced by victims emerges as a core justificatory axis of the measure. The persistence of illicit material online or unwanted digital proximity with the offender can generate a form of continuous victimization, extending the effects of the original offence well beyond its initial commission[6]. Even without direct contact, the awareness of the offender's online presence may inhibit the victim's willingness to participate freely in digital spaces, producing a chilling effect on their autonomy and communicative self-determination. Such dynamics reveal how virtual coexistence can perpetuate relational coercion despite the absence of physical contact, thereby justifying a tailored precautionary intervention. Against this backdrop, the virtual restraining order extends protection within the digital sphere, offering more robust and context-sensitive safeguards than the current jurisprudential interpretation of "contact by any means". By targeting the digital spaces in which psychological pressure or symbolic intrusion occurs, the measure operates as both a preventive mechanism – reducing the risk of reoffending – and a restorative instrument, aimed at re-establishing the victim's sense of safety, autonomy, and digital dignity.

As regards the rationale underpinning the new precautionary measure, its foundation is twofold. On the one hand, it acknowledges that unrestricted Internet access for an individual under criminal investigation may seriously hinder efforts to prevent reoffending and to safeguard the victim's legal interests. As a precautionary measure rather than a penalty, the virtual restraining order effectively serves these objectives while preserving the integrity of the legal process. The interactive, decentralized and instantaneous nature of digital communication, renders *ex ante* control over illicit content neither feasible nor desirable. Consequently, regulatory intervention in cyberspace must focus on controlling access to the specific digital contexts where harm is generated or perpetuated. Within this framework, the virtual restraining order would, therefore, target those digital environments identified by judicial authorities as relevant to the alleged conduct, ensuring both proportionality and technological feasibility. On the other, as a procedural safeguard, the virtual restraining order embodies the principle of *ultima ratio*, intervening only where less intrusive alternatives prove inadequate to guarantee effective victim protection or the preservation of digital evidence.

In practical terms, enforcement of this measure would require collaboration between judicial authorities, Internet Service Providers (ISPs), and technical experts. Its implementation could involve the installation or execution of monitoring or blocking software on the devices used by the investigated individual, configurated to:

- prevent any form of contact with the victim, in the broad sense outlined above;
- restrict access to online platforms or websites habitually visited by the victim;
- limit the use of social networks or applications associated with the alleged conduct;
- apply other technically feasible restrictions necessary to prevent recidivism and protect the victim's rights in the digital environment.

This measure seeks to prevent reoffending concerning the protected legal interest, whether personal (as in offenses against honor or privacy) or collective (such as terrorism-related crimes or the distribution of child pornography).

It is important to clarify that a "virtual restraining order" does nor replicate the legal nature of a traditional restraining order, which limits physical proximity or ambulatory freedom. Instead, it operates through a digital analogue: a calibrated limitation on the individual's interaction with specific online environments identified as vectors of potential harm[7]. As such, it affects a distinct sphere of liberty: the freedom of expression and

5. See, Bettiga 2020, Martellozzo–Jane 2017.
6. Agustina Sanllehí–Gámez-Guadix–Montiel Juan, 2020.
7. It is important to remember that the virtual restraining order primarily targets electronic content and data, namely, the digital spaces, platforms, and communication channels where illicit conduct may be reproduced,

the right to Internet access, as the latter serves as a prerequisite for exercising the former through digital platforms[8]. Given its potential impact on these fundamental freedoms, its adoption must always undergo a proportionality assessment, ensuring necessity, suitability and proportionality *stricto sensu*, as further discussed in the subsequent section.

Ultimately, the virtual restraining order reflects the evolution of precautionary logic in the digital era: it's a forward-looking and technologically adapted mechanism, reconciling preventive protection with procedural guarantees. By combining technological feasibility, judicial oversight, and a proportional rights-based approach, it seeks to balance the imperatives of victim protection with the foundational principles of the rule of law in cyberspace.

4.2. Fundamental rights, proportionality principle, and the need for judicial authorization

4.2.1. Fundamental rights

As stated above, the implementation of such a precautionary measure inevitably affects fundamental rights, particularly freedom of expression and the right to Internet access. More broadly, such restrictions impinge upon the right to access technology, which has become an essential component of personal development and social inclusion in the information society[9].

The increasing significance of Internet access and digital connectivity is closely associated with what scholars describe as the emerge of a fourth generation of human rights[10], shaped by technological progress and the rise of informational autonomy. However, the extent of its legal recognition remains fragmented. Some jurisdictions have enshrined Internet access constitutionally, while others recognized it through judicial interpretation, statutory provisions, or soft-law[11].

At the international level, the United Nations (UN) has explicitly affirmed the human right to Internet access as intrinsically linked to freedom of expression and information. The UN Human Rights Council Resolution of 5 July 2018 on the *Promotion, Protection, and Enjoyment of Human Rights on the Internet*[12] declares that "the same rights people have offline must also be protected online;", thereby recognizing the Internet as a structural condition for democratic participation. The UN General Assembly Resolution of

disseminated, or perpetuated. The resulting limitation on the investigated person's conduct emerges only as an indirect consequence of this object-oriented intervention.

8. Aslam–Kaaniru–Abiero 2025.

9. In particular, as Rodotà points out: "Il diritto di accesso a Internet, tuttavia, va inteso non solo come diritto a essere tecnicamente connessi alla rete, bensì come espressione di un diverso modo d'essere della persona nel mondo, e dunque come effetto di una nuova distribuzione del potere sociale. (…) Il diritto di accesso, infatti, si presenta ormai come sintesi tra una situazione e l'indicazione di una serie tendenzialmente aperta di poteri che la persona può esercitare in rete". See , Rodotà 2012. On the other hand, in Frosini's view, "Il diritto di accesso a Internet è da considerarsi un diritto sociale, o meglio una pretesa soggettiva a prestazioni pubbliche, al pari dell'istruzione, della sanità e della previdenza. Un servizio universale che le istituzioni nazionali devono garantire ai loro cittadini attraverso investimenti statali, politiche sociali ed educative, scelte di spesa pubblica. Infatti, sempre di più l'accesso alla rete Internet, e lo svolgimento su di essa di attività, costituisce il modo con il quale il soggetto si relaziona con i pubblici poteri, e quindi esercita i suoi diritti di cittadinanza". See, Frosini 2011. In the same vein, the Council of Europe, in its Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to Human Rights for Internet UsersRecommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to Human Rights for Internet Users (adopted on April 16, 2014), recognizes that access to the Internet is an important means of exercising rights and freedoms, as well as participating in democracy. For this reason, it must be "affordable and non-discriminatory".

10. Bustamante Donas 2001; Bustamante Donas, 2010; Acata Águila 2011; Riofrío Martínez Villalba 2014; Morales Aguilera 2018; León Camacho 2020; Cova Fernández 2022.

11. Álvarez Robles 2022.

12. United Nations (2018), The promotion, protection and enjoyment of human rights on the Internet,The promotion, protection and enjoyment of human rights on the Internet, (A/HRC/RES/38/7), July 5, 2018.

13 July 2021[13] further deepened this perspective, highlighting Internet access as indispensable for education, employment, healthcare, and civic engagement, and urging States to ensure open, reliable, and secure connectivity while combating disinformation and hate speech within a human rights – compliant framework.

The COVID-19 pandemic reinforced the essential nature of Internet access in contemporary society, prompting the UN to explore its potential incorporation into binding international legal frameworks[14].

In the European context, the European Court of Human Rights (ECHR) addressed this issue in *Ahmet Yildirim v. Turkey* (Judgement of 18 December 2012). The ruling acknowledged that the right to Internet access is inherent to the right to access information and communication, as protected by national constitutions. It further established that this right entails both individual participation in the information society and a state obligation to ensure Internet access for citizens[15]. This judgment underscores the constitutional protection of Internet access due to its direct link to freedom of expression and information.

However, the ECHR also clarified that Internet access is not an absolute right, as its exercise may be lawfully restricted to serve overriding interests, such as crime prevention and law enforcement. Accordingly, any limitations must be proportionate and strike a balance between competing legal interests[16].

The Court of Justice of the European Union (CJEU) has similarly addressed Internet access within the framework of data protection (Article 16.1 TFEU and Article 8.1 CFR)[17] and digital market regulation. In its judgment of September 15, 2020[18], the CJEU interpreted Regulation 2015/2120[19] for the first time, establishing the principle of net neutrality and recognizing that unduly restricting access to online content or services infringes both the freedom to conduct a business and user's right to information. This jurisprudence positions Internet access as an instrumental right indispensable to the enjoyment of other freedoms protected under EU law.

Consequently, Internet access has thus evolved into an instrumental right, essential for the effective exercise of other fundamental rights, including education, employment, healthcare, and access to information. In the context of the ongoing technological and digital transformation, unrestricted access to the Internet is fundamental to personal development and human dignity. In the 21st century, where most interactions take place online[20], digital exclusion due to lack of Internet access can lead to social marginalization, exacerbating existing inequalities and hindering full participation in modern society[21].

Comparative constitutional experiences further illustrate this normative trajectory.

13. United Nations (2021), The promotion, protection and enjoyment of human rights on the Internet,The promotion, protection and enjoyment of human rights on the Internet, (A/HRC/RES/47/16), July 13, 2021.
14. United Nations (2020), Covid-19 makes universal digital access and cooperation essential: UN tech agencyCovid-19 makes universal digital access and cooperation essential: UN tech agency, May 2, 2020.
15. ECtHR (Second Section), December 18, 2012. *Yildirim v. Turkey*, application no. 3111/10, paragraph 31.
16. ECtHR, (Fourth Section), December 2, 2008, *K.U. v. Finland*, application no. 2872/2002.
17. Of particular significance in our constitutional context at this point is the *Google Spain* ruling (CJEU, Grand Chamber, May 13, 2014, case C-131/12).
18. Judgment in the joined cases C-807/18 and C-39/19 *Telenor Magyarország Zrt./Nemzeti Média- és Hírközlési Hatóság Elnöke*.
19. Regulation (EU) 2015/2120 of the European Parliament and of the Council, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (November 25, 2015).
20. Nannipieri 2013; Frosini 2011; Pisa 2010.
21. "In a world more and more based on economic and social electronic networks, the right not to be excluded the right to access acquires an increasing importance. Concepts like 'inclusion' and 'access' have today replaced those (corresponding) of autonomy and possession, which characterized the notion of property in a traditional sense: in the new economy, the concept of property does not refer to a power of excluding others from

In Mexico, the 2013 amendment to Article 6 of its Constitution expressly guarantees citizens the right to access and use ICTs in everyday life, obliging authorities to promote universal connectivity[22].

In other jurisdictions, this right has been established through judicial precedent. In France, the Constitutional Council (Decision No. 2009-580 DC, June 10, 2009) recognized Internet access as a fundamental right, distinct from freedom of thought and opinion enshrined in Article 11 of the 1789 Declaration of the Rights of Man and of the Citizen. Drawing on this comparative legal foundation, the Constitutional Chamber of the Supreme Court of Justice of Costa Rica subsequently ruled in favor of Internet access as a fundamental right[23].

By contrast, some States have opted for a legislative approach. On July 1, 2010, Finland passed a law recognizing Internet access as a legal right[24]. Similarly, Italy, through the Legge Stanca of January 9, 2004[25], linked access to digital services with the principle of equality (Article 3 of the Italian Constitution), emphasizing accessibility for persons with disabilities[26].

In Spain, Internet access enjoys statutory recognition under Article 81 of Organic Law 3/2018 on Data Protection and Digital Rights, which mandates universal, affordable, high-quality, and non-discriminatory connectivity. The Digital Rights Charter[27], although not binding, reinforces the State's responsibility to guarantee effective, equitable access and prevent digital exclusion. The General Telecommunications Law[28] (Law 11/2022, June 28) further strengthens this right by defining its minimum essential content[29], which include access to email services; search engines; basic online training and education tools; online news or press; e-commerce platforms; job search portals and professional networking; Internet banking; e-government services; social networking and instant messaging; and telephone and video calls (standard quality).

Given the above, this law could serve as a foundation for the constitutional recognition of Internet access as a fundamental right[30], analogously to the right to be forgotten, which emerged from the constitutional protection of data (Article 18.4 CE). Under this approach, a constitutional embodiment of this right could be achieved by linking it to the right to data protection (Article 18.4 CE), freedom of expression and information (Article 20 CE) and the right to communicate and receive truthful information by any means of dissemination[31] (Article 20 CE) [32], thereby affirming the digital dimension of citizenship.

In short, through a systematic interpretation of these pre-existing fundamental rights, the fundamental character of Internet access could be established.

enjoying personal goods anymore, rather it qualifies as a right to not be excluded from the society's resources". See , Rifkin 2000.

22. Comisión Nacional de los Derechos Humanos. Instituto Nacional de Estudios Históricos de las revoluciones de México, Derecho de acceso y uso de las tecnologías de la información y la comunicación, Biblioteca Constitucional CNDH-INEHRM, November 2015.
23. Ruling 12790-2010.
24. Miranda Bonilla 2016.
25. Known by this name after its promoter, Lucio Stanca.
26. Pollicino–Romeo 2016.
27. *Carta de Derechos Digitales*, in "Web oficial del presidente del Gobierno y el Consejo de Ministros", 2021.
28. Ley 11/2022, de 28 de junio, General de Telecomunicaciones, 2022.
29. According to Art. 37 in connection with Annex III.
30. Álvarez Robles 2024.
31. Frosini expands on this idea, arguing that a constitutional right to Internet access is being created at the jurisprudential level. In the context of widespread Internet diffusion, the freedom of communication and expression necessarily presupposes the freedom to access such online communication services, and it is the obligation of states to eliminate obstacles that, in practice, prevent the exercise of such universal service for all citizens. See, Frosini 2011.
32. Spanish Constitutional Court, rulings 31/2010, 8/2012, 8/2016 y 20/2016.

In particular, a constitutional recognition of Internet access as a fundamental right should entail, at a minimum, the prohibition of prior and collateral censorship, a ban on indiscriminate and arbitrary filtering, monitoring, or control mechanisms and protection against interference with content[33], including generalized blocking or interruptions of Internet services[34].

Any restrictions should be imposed only retrospectively, subject to the legality of the content in question[35]. However, until this right attains fundamental status, it remains structurally fragile, lacking both direct enforceability against public authorities and a reinforced system of legal guarantees that would allow individuals to enforce its protection before the courts[36].

In conclusion, the consolidation of a constitutional right to Internet would serve as a normative cornerstone for future digital precautionary measures. It would ensure that any restriction – such as the virtual restraining order proposed herein – operates within a framework of legality, necessity, and proportionality, thereby harmonizing individual rights, technological progress, and the preventive aims of criminal justice in the digital age.

4.2.1.1. The concept of the "computer domicile" and its implications for virtual restraining measures

At this juncture, it is pertinent to examine the legal implications of safeguarding what some jurisdictions refer to as the "computer domicile" when imposing cyber precautionary measures, such as a virtual restraining order. This concept, which has no direct equivalent in Spanish law, has been particularly developed in German and Italian jurisprudence.

In Germany, the term "computer domicile" is used to designate the virtual space where individuals or entities conduct online activities. A landmark ruling by the German Constitutional Court in 2008 played a pivotal role in this regard[37]. Faced with the challenges posed by covert surveillance of information systems, the Court found it insufficient to rely solely on an evolutionary interpretation of constitutional guarantees concerning the confidentiality of telecommunications, the inviolability of the home, and the right to informational self-determination. As a result, the Court explicitly recognized – for the first time in Europe[38] – a new fundamental right of constitutional rank: the "right to the integrity and privacy of information systems". This right ensures that the so-called "digital citizen" can freely and securely use information and communication technologies[39]. Subsequent rulings by the German Constitutional Court upheld the admissibility of digital investigative measures allowing remote data acquisition, provided they adhered to the principle of proportionality, ensuring a balance between protecting this newly recognized right and other competing legal interests and judicial oversight requirements, to prevent excessive state interference[40].

33. Except for those causes strictly provided for by law (principle of legality). See, García Mexía 2018.
34. Álvarez Robles 2022.
35. Velasco Núñez 2012.
36. In particular, that it can be challenged through the "amparo" appeal before the Constitutional Court (Article 53 CE), with direct effectiveness and development through Organic Law.
37. Decision of the German Federal Constitutional Court (BVerfG) of February 27, 2008, in which it was called upon to assess the legitimacy of a provision in the North Rhine-Westphalia State Constitution Protection Law, which allowed a government intelligence agency to conduct surveillance and secret access to networked computer systems.
38. Venegoni–Giordano 2016.
39. The German Constitutional Court, therefore, declared the unconstitutionality of the regulation that provided for the surveillance of computer systems as an intelligence activity in relation to the new fundamental right. However, it did not completely exclude the possibility of allowing such monitoring as an investigative tool. See, Torre 2015.
40. BVerfG, April 20, 2016, where the Court reaffirmed the compatibility of covert surveillance measures by the police with the fundamental rights recognized by the Constitution, in order to protect society from the threats of international terrorism. However, some provisions of the contested federal law – regulating the activities of

In Italy, references to the "computer domicile" have also emerged in legal discourse. However, before analyzing this concept, it is essential to distinguish it from the "digital domicile" (*domicilio digitale*[41]), as the two terms hold distinct legal meanings.

The "digital domicile" refers to a certified email address[42] that holds legal validity for official electronic communications. It can be voluntarily chosen by individuals upon reaching legal adulthood, but it is mandatory for certain legal entities and professionals. Since July 6, 2023, any individual in Italy can access another person's electronic domicile without prior authorization[43] by entering their *codice fiscale* (tax identification number) into a designated public platform. By contrast, the "computer domicile" – which is relevant for criminal law protections – refers to the virtual space where fundamental freedoms such as privacy, freedom of communication, and freedom of expression are exercised. This concept is characterized by its dynamic, mobile, and evolving nature, as digital technologies enable continuous access to sensitive data from multiple locations.

In particular, the Italian Court of Cassation has defined the "computer domicile" as the digital space where personal data is stored, protected by security measures such as passwords or encryption keys. This space, the Court has ruled, merits legal protection against unauthorized intrusions in the same manner as an individual's private sphere[44].

This protection is codified in Article 615-*ter* c.p. (Italian Penal Code)[45], which criminalizes: "Anyone who unlawfully accesses a computer or telematic system protected by security measures or remains within it against the express or implied will of the rightful owner". The decision to classify this offense alongside violations of the physical home's inviolability (Article 614 c.p.) underscores the legislative intent to equate the legal protection afforded to both physical and digital domiciles[46].

Traditionally, in procedural criminal law, the notion of "place" has been linked to a defined physical space. This conceptualization is relatively straightforward when applied to a tangible computing device, which occupies a specific location and serves as a data storage medium. As a result, digital devices are often treated as "places" for the purposes of criminal investigations, much like physical premises where searches and seizures are conducted. However, determining whether a virtual space within a network can also be regarded as a "place" presents significant legal challenges. The materiality that traditionally defines a "place" in the physical world cannot be strictly transposed to cyberspace, given its inherently fluid, decen-

the federal police and cooperation in criminal matters between state and federal governments, as well as with third countries – were declared unconstitutional for violating the principle of proportionality in the balance between public powers and individual prerogatives. See, Venegoni–Giordano 2016.

41. This figure also exists in Argentina (Article 40 of the Civil and Commercial Procedural Code of the Province of Buenos Aires, amended by Law 14.140). Specifically, the Diccionario panhipánico del español jurídicoDiccionario panhispánico del español jurídico defines it as "A domicile that replaces or coexists with the physical domicile established in the judicial file, to which all notifications that should not be sent to the actual domicile must be directed".
42. Known as "Posta elettronica certificata" (PEC) in Italy.
43. "Indice Nazionale dei Domicili Digitali" (INAD).
44. Cass., Sez. VI, 14 dicembre 1999, n. 3067, in "Cassazione Penale", 2000.
45. Introduced by Law No. 547/1993.
46. In an initial ruling, the Tribunale di Torino, Sez. IV penale, 7 febbraio 1998, already affirmed that: "È assolutamente pacifico che la normativa di cui all'art. 615-*ter* c.p., presentandosi come un'estensione della protezione generalmente assicurata ad ogni forma di domicilio, ha inteso reprimere qualsiasi introduzione in un sistema informatico che avvenga contro la precisa volontà dell'avente diritto". A subsequent decision – G.I.P. Roma, 21 aprile 2000 – further clarified that: "Il legislatore, con l'introduzione della norma incriminatrice di cui all'art. 615-*ter* c.p., ha inteso tutelare non la privacy di qualsiasi domicilio informatico, ma soltanto quella dei sistemi protetti contro il pericolo di accesso da parte di persone non autorizzate. (…) Considerato che l'esistenza di mezzi efficaci di protezione costituisce elemento costitutivo della fattispecie incriminatrice di cui all'art. 615-*ter* c.p., deve dichiararsi il non luogo a procedere".

tralized, and expandable nature. Unlike physical locations, the digital network is not confined by tangible boundaries but exists as a dynamic and interconnected structure[47].

This conceptual distinction becomes particularly relevant when considering precautionary measures in the digital domain, such as virtual restraining orders, which impose restrictions on an individual's ability to access, communicate, or interact within specific online environments. In this context, the legal recognition of digital spaces as protected domains – analogous to physical domiciles – remains a crucial yet unresolved issue in many legal systems.

In light of these considerations, it becomes evident that the notion of a physical domicile cannot be straightforwardly transposed onto the digital sphere. Firstly, unlike a computer domicile, a physical domicile is not subject to the requirement of security measures. Under Article 614 c.p.[48], the right to the inviolability of one's home is not contingent upon the implementation of protective barriers, meaning that the victim is not responsible for equipping their home with security measures[49]. In contrast, the legal recognition of a computer domicile is intrinsically linked to the presence of security mechanisms, effectively placing a degree of responsibility on the user to safeguard their digital space. Unlike physical homes, the legal protection of the computer domicile is not generic; rather, it is conditioned upon the existence of security measures implemented by the system owner to protect the confidentiality of data, programs, or information. This requirement underscores the distinct nature of the computer domicile and confirms that it cannot be equated with its physical counterpart. However, once such protective measures are in place, the protection extends independently of the physical location where the data are stored (whether on a personal device, a corporate server, or a remote cloud infrastructure)[50]. The computer domicile should thus be understood as an autonomous legal asset, characterized by its intangible nature and the manifestation of the owner's will to exclude third parties through technological means, rather than by spatial or territorial boundaries.

In comparative perspective, the Spanish equivalent to Article 615-*ter* c.p. is Article 197-*bis* CP (Spanish Penal Code), which is located in Title X (Offenses Against Privacy, the Right to One's Own Image, and the Inviolability of the Home), Chapter I (Discovery and Disclosure of Secrets). This provision transposes Directive 2013/40/EU of August 12, concerning attacks against information systems and the interception of electronic data, provided that the intercepted data does not constitute personal communication[51].

Both the Spanish and Italian provisions addressing the unauthorized access to computer systems require the presence of a pre-existing "digital bar-

47. In this sense, an Italian criminal law sector considers that the limits and corporeality are merely incidental, not substantial, elements of the concept of place, so it aligns more with the idea of being a space potentially suitable for containing something (as would happen, for example, with air). With this conception in mind, it would be possible to consider the network as a "place". See, Signorato 2018.

48. Specifically, the criminal conduct of this offense consists of the intrusion of any person into another person's home, or another private residence, or its dependencies, against the express or tacit will of the person who has the right to exclude them, or having entered clandestinely or by means of deception.

49. At this point, the proposal put forward by Picotti, Flor and Salvatori regarding the placement of this type of offense (as well as others related to it) within a new, autonomous Section of the "Crimes Against Individual Liberty", under the title "On Crimes Against Privacy and Computer Security" (*Dei delitti contro la riservatezza e la sicurezza informatiche*), is particularly interesting. They also propose revising Article 615-*ter* of the Penal Code to remove, among other changes, the reference to the requirement that the computer system, or a part of it, must have security measures in place in order to be subject to criminal protection. See, Picotti–Flor–Salvatori 2021.

50. For example, an individual using their laptop in public still has the right to privacy regarding its content, protecting it from any public or private intrusion. See e, Trogu 2019.

51. In this regard, among the requirements of the Directive, it is called for a clear separation between cases of data disclosure that directly affect individuals' privacy and access to other data or information that may affect privacy but are not directly related to personal intimacy. In this way, accessing a personal contact list would not be the same as collecting data related to the software version used or the status of the entry ports to a system.

rier" (such as passwords or access credential) for virtual intrusion to be legally actionable[52]. This requirement stems from the assumption that the existence of protective measures against unauthorized access reflects the system owner's explicit intent to exclude third parties.

Within the Spanish framework, Article 197-*bis* CP specifies that the perpetrator must lack authorization to enter the system, thereby emphasizing the unlawfulness of intrusion beyond permitted access boundaries.

In the Italian context, the corresponding Article 615-*ter* c.p., criminalizes unauthorized access to computer or telematic systems. The jurisprudence of the Court of Cassation has progressively refined the interpretation of this provision, particularly regarding the scope of authorization and its functional limits. The prevailing view, firmly established by the *Sezioni Unite* in Judgment No. 41210 of 18 May 2017 (filed 8 September 2017), affirms that the offence may be committed not only by individuals who lack any formal authorization, but also by those who, while holding valid credentials, access or remain within a system for purposes alien to, or exceeding, the legitimate scope of their authorization, a phenomenon described as *sviamento di potere* ("abuse of authority" or "deviation of power").

The Court's reasoning is grounded in a functional and purpose-oriented interpretation of authorization. Access rights are valid only insofar as they serve the institutional or professional objectives for which they were granted. When an individual uses authorized credentials for private, competitive, or otherwise illegitimate purposes, the authorization loses its justificatory force, and the conduct constitutes "unauthorized access" within the meaning of Article 615-*ter*. The Court emphasized that the criminal provision protects not only the system owner's exclusive control but also the fiduciary integrity and internal trust that underpin the lawful use of digital credentials.

This interpretation extends criminal liability to situations where an employee or official, though possessing valid credentials, exploits them for purposes extraneous to their duties (for instance, accessing confidential corporate data to gain personal advantage or to cause harm).

This jurisprudential approach underscores that the mere possession of access credentials does not exclude criminal liability. The offence materializes whenever the authorized user accesses or remains within a system for reasons incompatible with the legitimate purposes of their authorization, thereby violating the protected interest in the confidentiality, security, and integrity of information systems.

However, unlike the Italian legal system, Spanish law does not recognize the autonomous concept of a "computer domicile". Furthermore, an equivalence between the physical and computer domicile – analogous to the Italian jurisprudential approach – would conflict with the case law of the Spanish Supreme Court regarding "virtual" intrusions into the domicile. A key reference in this regard is Supreme Court ruling 329/2016, dated April 20[53], which emphasizes that a domicile, as a constitutionally protected space, does not lose its legal status simply because curtains are left open or because the resident does not employ sufficient physical barriers to obstruct visibility from the outside. As Martín Ríos[54] argues, applying this reasoning to the computer domicile would mean that the mere absence of technical barriers preventing access to a device does not justify unauthorized access.

Such an approach reflects a broader understanding of information privacy in the digital age, grounded in the recognition that digital spaces, by their very nature, constitute extensions of the individual's private sphere. Even when accessed data does not immediately relate to personal privacy – such as traffic or location data – it may, when isolated or combined with other datasets, enable the reconstruction of an individual's private sphere, thereby infringing upon the same legal interests protected by traditional privacy provisions.

Accordingly, the absence of technological barriers should not diminish the protection afforded

52. This has even been acknowledged by the ruling of the Court of Cassation on October 27, 2004, which establishes that the crime of unauthorized access cannot be considered committed if the computer or telematics system to which the accused gains access is not objectively protected by security measures.

53. The well-know "sentencia de los prismáticos".

54. Martín Ríos 2017.

to digital environments. Just as the legal protection of the physical domicile does not depend on the presence of physical exclusionary measures (e.g., a locked door or closed curtains), digital spaces should enjoy equivalent safeguards given the quantity and sensitivity of information they contain. In other words, the absence of a password-protected login screen on a personal laptop should not justify unauthorized third-party access[55]. The legal protection of digital environments must therefore derive from their informational function rather than their technical configuration. The normative value of informational privacy – as a manifestation of personal autonomy and human dignity – demands equivalent protection in both physical and virtual domains. From a criminal policy perspective, this alignment is essential to ensure coherence between the material realities of cyberspace and the fundamental rights architecture of contemporary European criminal law.

Moreover, the evolving nature of digital spaces and the diverse functions that a single virtual environment can serve preclude rigid classifications of legal protections. For instance, a social media platform, such as Twitter, facilitates both public communication and private interactions. Within such an environment, users may not only have a general expectation of privacy but, in some cases, an enhanced expectation comparable to that associated with a physical home. This occurs when a user activates all available privacy settings, restricting access to their content to a select group. In such cases, unauthorized access to their digital space could constitute a significant violation of their legally protected privacy rights.

In this regard, both doctrine and jurisprudence of the Italian Court of Cassation[56] emphasize that a personal computer should not be regarded merely as a tool for processing and storing electronic documents. Instead, it represents an essential medium for cataloging, applying, and researching information (one through which individuals develop their professional, cultural, and intellectual capacities)[57]. Furthermore, the Court of Cassation has articulated a doctrinal interpretation concerning the expansion of the constitutional concept of domicile to encompass computer systems and virtual spaces. By adopting a teleological interpretation of the relevant legal provisions, the Court has asserted that the legislature intended to safeguard the "extension of the material domicile and the ideal space (including the physical location where digital data is stored) belonging to an individual, to which the right to privacy extends as a constitutionally protected right (Article 14 of the Constitution)". Consequently, the Court has recognized the concept of "computer domicile" as an additional manifestation of traditional domicile, grounded in the ius excludendi alios principle, regardless of

55. Specifically, according to Circular3/2017, of September 21Circular 3/2017, of September 21, it is not considered that the legal interest protected by Article 197-*bis* CP is the "computer domicile", nor that it directly attacks personal privacy. Instead, it is more about safeguarding "the security of information systems as a means of protecting the reserved privacy area from potential public knowledge". In this way, as highlighted in the Preamble of Organic Law 1/2015, the autonomous classification of this figure aims to establish a distinction between the cases referred to in Article 197 CP (related to the unauthorized access, seizure, or knowledge of data or information affecting personal privacy) and those in which, although there is illegal intrusion into third-party data or systems, personal data or privacy are not directly affected. However, even if there is no direct impact, as we mentioned earlier, computer data entered into a system, seemingly disconnected from a user's privacy, can, when examined as a whole, be highly revealing of the user's privacy, even leading to the creation of a fairly comprehensive profile of the individual. It is important to remember that this situation is referred to as the "mosaic theory".

56. Cuomo 2000; Aterno 2000. In case law, see Cass., Sez. VI, 4 ottobre 1999, n. 3067, and, more recently, Cass., Sez. Un., 27 ottobre 2011, n. 4694.

57. Signorato refers to the creation of a new sphere of protection for a new right, stemming from the development of new technologies. This would be a fundamentally dynamic right, not static, like the right to a computer domicile: the right to the inviolability of digital life (*diritto all'intangibilità della vita digitale*). However, this right differs from the right to self-determination over the use of personal data (*diritto all'autodeterminazione sull'uso di dati personali*), as the right to the inviolability of private life would not be limited to guaranteeing subjective protection restricted to personal data, but would extend to any data or activity inserted or developed within the realm of a computer system and the network. See, Signorato 2018.

the nature of the stored data, provided it pertains to an individual's intellectual or professional activities[58].

This expansion of the traditional notion of domicile to the "digital projection of the individual" aligns with the rationale underlying the "right to the integrity and privacy of information systems" recognized by the German Federal Constitutional Court. This right has emerged specifically to protect individuals from state access to their digital devices, particularly in cases involving government surveillance of entire information systems rather than merely individual communications or data storage activities[59].

Ultimately, the debate on "computer domicile" centers on whether materiality and physical boundaries are essential for recognizing a "place" subject to criminal law protection. This conceptualization is particularly relevant to the application of precautionary measures. In an online context, a restraining order – traditionally understood as a prohibition on approaching specific physical locations – could be adapted into a "virtual restraining order", restricting the accused from accessing designated digital spaces to prevent interaction with the victim. Notably, such an order would not be limited to direct communication but could also encompass shared virtual spaces where both individuals coexist within the same digital environment (despite thede absence of direct communication).

While restraining orders were initially designed to protect an individual's physical integrity by restricting access to certain locations, they are equally relevant in the digital realm, where psychological integrity can be compromised by an individual's virtual presence. This further justifies the legitimacy of implementing a virtual restraining order as a precautionary measure.

Although the Spanish legal framework does not explicitly recognize the concept of "computer domicile" as developed in Italian and German law, a related notion does exist: the "right to one's own virtual environment". This term was referenced in Supreme Court Judgment 342/2013, of April 17, and later reaffirmed in Judgment 786/2015, of December 4, although it has yet to receive formal legislative recognition. This "right to one's own virtual environment" could serve as a means of addressing the current fragmented regulatory landscape, in which protection against intrusions into electronic devices must be sought through separate legal provisions related to privacy rights (Article 18.1 CE), secrecy of communications (Article 18.3 CE), and data protection (Article 18.4 CE). Despite this fragmentation, the practical consequence remains the same: any measure involving interference with electronic devices or information systems requires prior judicial authorization[60].

This requirement would equally apply to a virtual restraining order. Indeed, enforcing such a restriction – limiting an individual's online interactions or access to specific digital spaces – may necessitate technological mechanisms to ensure compliance. Given the potential impact on fundamental rights and the need to uphold the principle of proportionality, judicial authorization would be indispensable. This requirement precludes law enforcement authorities or the Public Prosecutor's Office from imposing such measures without judicial oversight during the preliminary investigative phase. Moreover, in cases requiring access to an individual's digital devices or systems, the concept of "digital privacy" may serve as an enhanced dimension of general privacy protections. Since such access could involve highly sensitive information, express judicial authorization would always be required before proceeding with any measure affecting digital privacy rights[61].

Since the Spanish legal system does not explicitly recognize the concept of "computer domicile" as a legally protected interest, it has only recently begun to explores the possibility of extending the traditional concept of "place" from the physical

58. Domenicali 2018.

59. BVerG, February 27, 2008. Translation extracted from Venegoni–Giordano 2016.

60. Martín Ríos 2017.

61. As recognized in the aforementioned Constitutional Court ruling 173/2011 of November 7 and in Supreme Court ruling 786/2015 of December 4, the safeguarding of this right, like the inviolability of the home or the right to the secrecy of communications, is granted a higher level of protection than that afforded to privacy "in general".

to the virtual realm, particularly in response to the rise of cybercrime. Notably, Supreme Court ruling 547/2022, of June 2, considered the possibility of extending the concept of "place of the crime" to include social networks – and, by extension, the Internet – as a locus of criminal activity. According to the Court, within the scope of Article 48 of the Spanish Penal Code, the prohibition on accessing certain locations could be interpreted to encompass digital spaces of interaction and communication where offenses were committed. However, the dissenting opinion in this ruling warns that this analogical interpretation risks overstepping the boundaries set by the principle of legality in criminal law, particularly concerning the legitimacy of penalties.

This concern highlights the distinction between restricting access to physical and virtual spaces. While prohibiting entry into a physical location primarily limits an individual's freedom of movement (albeit in a limited manner), restricting access to a social network would directly impact freedom of expression, and, arguably, the right to Internet access. Consequently, repurposing an existing legal measure originally designed for physical spaces to restrict access to online spaces could constitute a "label fraud"[62] of legal concepts. This would distort the true nature of the measure, concealing under one label what is, in reality, a different type of restriction: a limitation on freedom of expression and Internet access.

Given these considerations, it is imperative to establish a distinct precautionary measure – separate from traditional restraining orders – specifically tailored to the digital sphere. This would prevent "label fraud" and ensure that such measures are properly framed within the principles of legality and proportionality.

From this perspective, we argue that the proposed virtual restraining order could be accommodated within the Spanish legal framework. This measure could take the form of a temporary prohibition limited to the digital space where the offense was committed, such as a specific social network, forum, or platform. In particularly severe cases (where, for instance, the offense was committed across multiple platforms or websites, and the harm inflicted upon the victims is significant) broader restrictions, such as a general prohibition on Internet access or a ban on contracting with Internet Service Providers, could be considered. The following sections will further explore these potential applications.

4.2.2. Prerequisites for the adoption of the virtual restraining order: special reference to the principle of proportionality

Due to the profound implications that cyber-precautionary measures – such as the proposed virtual restraining order – may have for fundamental rights (including freedom of expression, Internet access, informational privacy, and even the emerging right to one's "digital environment"), the principle of proportionality assumes a central and indispensable role in ensuring their constitutional legitimacy and practical effectiveness. It functions not merely as a balancing mechanism but as the normative threshold distinguishing legitimate precautionary intervention from disproportionate encroachment on digital freedoms.

Since Internet access plays a crucial role in individuals' personal and professional development, as well as their integration into the digital sphere, a preliminary balancing test tailored to the specific circumstances of each case is indispensable[63].

Therefore, the application of a virtual restraining order must be assessed in relation to the protection of legally recognized interests, provided that these aims withstand a proportionality test demonstrating the necessity of the measure. This principle serves as an essential analytical tool for evaluating the rational connection between the means employed and the objectives pursued – namely, preventing recidivism and further harm to victims – while seeking to resolve conflicts between competing rights or interests. Ultimately, the suitability, necessity, and proportionality in the strict sense of

62. The term "label fraud" (*Etikettenschwindel*), used almost a century ago by Kohlrausch, refers to the attempt to assign the legal regime of one institution to another simply by labeling it with the name of the former. In this regard, our Constitutional Court, in its ruling 239/1988, already argued that the *nomen iuris* of an institution cannot be a determining factor. See, Puente Rodríguez 2019.

63. Pollicino, 2023.

the measure must be assessed on a case-by-case basis[64], precluding any automatic application.

As established in Article 52(1) of the Charter of Fundamental Rights of the European Union (CFREU) [65], any limitation on the exercise of fundamental rights – such as privacy (Article 7), data protection (Article 8), and freedom of expression (Article 11) – must be provided for by law, respect the essence of those rights, and, subject to the principle of proportionality, be necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. This principle thus serves as the analytical framework for judicial scrutiny of cyber-precautionary measures.

The Court of Justice of the European Union (CJEU) has progressively delineated the contours of proportionality in a series of landmark decisions concerning data retention, surveillance, and investigatory powers. In *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238), the Court invalidated the Data Retention Directive for disproportionately interfering with the rights to privacy and data protection, stressing that general and indiscriminate retention of electronic communications data exceeds what is necessary in a democratic society. The CJEU reaffirmed and deepened this approach in *Tele2 Sverige AB and Watson* (Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970), holding that only targeted and temporally limited retention, based on objective criteria and subject to prior independent review, can satisfy the proportionality requirement.

Similarly, in *La Quadrature du Net* (Joined Cases C-511/18, C-512/18, and C-520/18, 6 October 2020, ECLI:EU:C:2020:791), the CJEU reiterated the centrality of the principle of proportionality in the context of data retention measures affecting fundamental rights. The Court emphasized that any derogation from the protection of personal data must be strictly necessary and proportionate to the legitimate objectives pursued. It held that national legislation permitting the general and indiscriminate retention of traffic and location data for the purposes of combating crime and safeguarding public security exceeds the limits of what is strictly necessary and cannot be justified within a democratic society. The CJEU further clarified that only measures aimed at combating serious crime, preventing serious threats to public security, and safeguarding national security are capable of justifying such serious interference. Furthermore, the Court emphasized that retention must be limited in scope and duration, both in terms of the categories of data affected and the period of storage, and must be governed by clear, precise, and foreseeable rules providing effective safeguards against abuse. This reasoning encapsulates the CJEU's broader digital proportionality doctrine: the more intrusive the measure, the more stringent the justification required. The judgment thus consolidates a structured proportionality standard which national authorities must satisfy when implementing precautionary or investigative powers that restrict digital freedoms.

The European Court of Human Rights (ECtHR) has adopted a complementary stance. In *Ahmet Yildirim v. Turkey* (2012) and *Cengiz and Others v. Turkey* (2015), it condemned broad Internet blocking orders as disproportionate under Article 10 ECHR, emphasizing that such measures must pursue a legitimate aim, rest on clear legal grounds, and preserve the essence of freedom of expression and information. The same reasoning applies to precautionary restrictions imposed in the digital environment: they must be targeted, necessary, and reversible. Likewise, in *Roman Zakharov v. Russia* (App. No. 47143/06, Judgment of 4 December 2015) and *Big Brother Watch and Others v. the United Kingdom* (App. Nos. 58170/13, 62322/14, and 24960/15, Judgment of 25 May 2021), the ECtHR emphasized that surveillance and data

64. This is known as the "German test". The position of Spanish Constitutional Court regarding the applicability of the principle of proportionality can be observed in ruling 11/1981, FJ 7.

65. This principle of proportionality is also reflected in Article 8 of the European Convention on Human Rights, which, under the heading "Right to respect for private and family life", states that there shall be no interference with this right by public authorities unless "such interference is in accordance with the law and constitutes a measure that, in a democratic society, is necessary for national security, public safety, the economic well-being of the country, the defense of order and the prevention of criminal offenses, the protection of health or morals, or the protection of the rights and freedoms of others".

interception measures must be "necessary in a democratic society," subject to rigorous *ex ante* judicial authorization, foreseeability, and end-to-end proportionality assessment.

The convergence between the CJEU and ECtHR jurisprudence illustrates that proportionality functions as a structural and cross-systematic principle ensuring that the expansion of digital precautionary powers remain compatible with fundamental rights. In the context of cyber-precautionary measures such as the virtual restraining order, this convergence provides the normative compass: restrictions must be individualized, temporary, and judicially supervised, ensuring that the protection of victims does not erode the foundational liberties inherent to the digital public sphere.

This jurisprudential alignment finds strong resonance in European legal scholarship. Herlin-Karnell[66] argues that proportionality in EU criminal law operates not merely as a balancing tool, but as a constitutional compass preventing the creeping normalization of intrusive technologies under the guise of efficiency. Ashworth and Zedner[67] in *Preventive Justice* conceptualize proportionality as the key criterion distinguishing legitimate precautionary intervention from preventive overreach. In Italy, as noted by Torre[68], digital investigations embody in their most acute form the traditional tension between the protection of individual rights and the demands of social defense. In this context, the solution must rest on a rigorous and structured application of the principle of proportionality, ensuring a careful balancing of the competing legal interests at stake. The proportionality principle serves not only as a limit to the State's coercive powers but also as a structural guarantee of their legitimacy. By requiring a reasoned evaluation of suitability, necessity, and proportionality *stricto sensu*, it transforms judicial discretion into a transparent process of normative justification.

The Spanish Constitutional Court has similarly recognized proportionality as an essential condition of legitimacy for any measure restricting rights. In STC 292/2000 and STC 49/1999, the Court held that restrictions must be (a) suitable to achieve their purpose, (b) necessary in the absence of less restrictive alternatives, and (c) proportionate *stricto sensu*, ensuring that the sacrifice of individual rights does not exceed the benefits for the public interest. These standards apply fully to cyber-precautionary measures, which by their very nature intersect with rights to communication and information.

On the basis of the foregoing, a virtual restraining order should not, as a general rule, entail a blanket prohibition on Internet access. Rather, any restriction must be narrowly tailored to the specific circumstances of the case, such as the severity of the offense, the risk of reoffending, the potential harm to victims or other legal interests, and the technological proficiency of the investigated individual. Accordingly, in certain situations, a targeted restriction – such as blocking access to the specific website, platform, or application through which the unlawful conduct occurred – may suffice. In more severe cases (e.g., online child exploitation, gender-based violence, or systematic cyberstalking), technically enhanced measures, including the installation or execution of judicially approved software, may be required to prevent the investigated individual from re-entering the victim's digital environment. Only in cases of exceptional gravity could a temporary, general prohibition on Internet access, or a ban on entering into contracts with Internet Service Providers, meet the proportionality threshold.

It is axiomatic that any limitation of fundamental rights must have a clear legal basis. Legislation must precisely define the conditions, scope, and duration of such measures. Judicial authorization and oversight are indispensable, both *ex ante* – to approve and delimit the measure – and *ex post* – to monitor its implementation and termination. Such measures cannot be authorized by an administrative body, let alone by ISPs or digital platforms. To ensure compliance with the principle of proportionality, any judicial order authorizing a virtual restraining measure must specify:

- the devices, systems, or digital environments affected or parts thereof;
- the extent and technical modalities of the restriction;

66. Herlin-Karnell 2012.

67. Ashworth–Zedner 2014.

68. Torre 2019.

– the software or monitoring tools authorized;
– the duration, strictly limited to what is necessary.

Additionally, if there is evidence that the investigated individual has access to other devices that could undermine the effectiveness of the order, law enforcement authorities must notify the judge, who may authorize an extension of the measure's scope to ensure its effectiveness.

Regarding duration, and in alignment with the requirements established for other existing cyber-precautionary measures, the order must be strictly limited to the minimum time necessary to fulfill its protective function[69]. Naturally, the measure must be lifted as soon as the circumstances that initially justified its adoption cease to exist, preserving the proportional equilibrium between public protection and individual freedom.

Within this framework, the virtual restraining order exemplifies a measure that – while restrictive of certain digital freedoms – can remain constitutionally legitimate when applied under stringent judicial oversight, subject to temporal limits, and demonstrably necessary to prevent reoffending and protect victims from renewed harm in online environments.

The cooperation of Internet Service Providers and digital intermediaries is crucial to enforce such measures effectively. These entities must be legally bound by a duty of cooperation as well as an obligation of confidentiality concerning such activities, ensuring that the execution of judicial orders in the digital sphere is both effective and rights-compliant. In the event of non-compliance, they could be subject to criminal liability for disobedience of a judicial order[70]. However, as Starr[71] aptly observes, the delegation of enforcement functions to private digital actors – when performed negligently or without adequate legal safeguards –, risks turns them into *de facto* agents of state authority, thereby blurring the constitutional boundaries between public accountability and private discretion. Such a shift would undermine the principle of legality and erode the transparency that judicial control is designed to guarantee. Consequently, any cooperative framework must be narrowly defined, normatively grounded, and subject to continuous judicial oversight to avoid the privatization of coercive functions within cyberspace.

This participatory model aligns with the EU's Digital Services Act (Regulation 2022/2065), which emphasizes judicial oversight, due process, and accountability in the moderation of online content. By analogy, cooperation in enforcing this online restriction order must likewise be governed by transparent, rights-based standards.

In this regard, proposals such as Bajovic's concept of a "cyber-deportation," whereby a cyberspace police force could impose temporary Internet bans, raise profound constitutional concerns. According to Bajovic, since such a measure would not constitute a criminal sanction, the debate surrounding the right to a fair trial would not be applicable. She argues that the presumption of innocence remains intact, given the preventive, temporary, and non-punitive nature of the restriction. Under this framework, judicial safeguards would be available at a later stage before the national court, drawing an analogy with pretrial detention in traditional criminal proceedings, which can serve the same purpose of preventing recidivism[72].

While this theoretical approach is undoubtedly thought-provoking, even acknowledging the deterrent effect she defends, it presents significant shortcomings. First, it fails to specify how such an Internet access ban would be technically enforced or what its practical implications would be. Second, it grants discretionary authority to a cyberspace police force, despite the fact that, as previously noted, any measure temporarily restricting access to the Internet or specific online content inherently affects fundamental rights. As such, these restrictions cannot be left to extrajudicial powers, as their imposition must strictly adhere to the principle of proportionality on a case-by-case basis and must always require judicial intervention.

69. In this case, it is concretized in preventing recidivism and the attack on new legal assets of the victim.
70. Application, *mutatis mutandis*, of the provisions of Article 588-*ter* e) LECrim concerning the obligation of ISPs to cooperate.
71. Starr 2025.
72. Bajovic 2017.

In contrast, the virtual restraining order proposed here preserves judicial centrality. By requiring court approval, defining the technological implementation, and ensuring procedural safeguards, it reconciles efficiency and legality while maintaining coherence with EU and ECHR proportionality standards.

In sum, the principle of proportionality serves as the constitutional compass for cyber-precautionary measures, ensuring that preventive protection does not devolve into digital repression. Only through this equilibrium can the criminal justice system uphold its dual mission in the digital era: to protect victims and society while safeguarding individual rights against excessive or arbitrary interference.

4.3. Implementation of the virtual restraining order

Preventing an individual from accessing the Internet entirely is an almost impossible task, given the multitude of devices available for such access. Similarly, it is equally unfeasible to prevent someone from committing any criminal act unless they are held in a maximum-security prison under constant surveillance. As we know, suspending an individual's driver's license does not physically prevent them from operating a vehicle (whether by using one belonging to a family member or even a stolen one). The same applies to firearm prohibitions, as weapons can still be acquired on the black market. These examples illustrate the inherent difficulty of ensuring that a legal measure or sanction alone completely prevents an individual from engaging in a specific conduct. Therefore, Internet restrictions do not guarantee total compliance. Instead, the objective is to increase the difficulty of engaging in illicit activity by depriving individuals of the means to do so, while ensuring that any breach of the restriction carries a specific legal sanction, which serves as the true deterrent.

Accordingly, the virtual restraining order we propose does not aim to completely prevent Internet access or specific online content but rather to impose targeted restrictions in cases where such a precautionary measure is justified[73].

At this juncture, the possibility of implementing tailored blacklists (*ad hoc*) could be considered. These would consist of a list of websites that a specific individual is prohibited from accessing. Such personalized blacklists would be transmitted to the individual's ISP, which would disable access through technical means. To ensure compliance with the principle of proportionality, victims could be consulted regarding which social networks or online platforms they use, allowing for a precise and dynamic application of the restraining order. These lists would be periodically updated, with online sites being added or removed based on the evolution of the case and advancements in technology.

From an operational standpoint, two main scenarios could be considered for implementing this precautionary virtual restraining order:

1) Identifying the individual accessing the Internet, thereby allowing a specific online connection to be attributed to a particular person. This would require the establishment of a digital identity system.
2) Restricting Internet access on a particular electronic device associated with the investigated individual, without the capability to confirm whether that individual is indeed the one using the device at the time of the connection.

Both approaches require further legal and technical development to ensure their feasibility and compliance with fundamental rights.

4.3.1. Digital identity system

In the context of digital security and online accountability, the implementation of digital identity systems could be considered as a mean to directly associate a specific individual to a given IP address. Such a system would enable a direct association between an individual and their online activity, thereby allowing for targeted restrictions on Internet access during the enforcement period of a precautionary measure. Through this mechanism, a specific individual could be prevented from accessing the virtual environment for the duration of the imposed sanction.

Regarding digital identification on the Internet, a noteworthy initiative is "Proof of Humanity" (PoH), a system designed to enhance security in a decentralized digital ecosystem. PoH is a social

73. In the terms outlined in the previous section.

identity verification system built on Ethereum[74], aimed at enabling individuals to access various applications that require resistance to Sybil attacks[75] for large-scale implementation. The system integrates webs of trust, reverse Turing tests, and dispute resolution mechanisms to create a Sybil-resistant registry of verified human users. Registration requires multiple verification steps, including the creation of a video with a spoken statement, the linkage of an Ethereum address to a clearly identifiable profile, and endorsement by an already verified user. Each individual can only register one account.

PoH-verified accounts could serve multiple purposes, including functioning as universal login methods and integrating with other identity systems to strengthen Sybil resistance in user profiles[76]. However, this system raises concerns regarding online anonymity, a fundamental characteristic of the Internet. Currently, PoH-stored identities are not anonymous, prompting efforts to develop privacy-preserving, Sybil-resistant digital identities. Proposed solutions include Traceable Ring Signatures and zero-knowledge proof mechanisms[77], which would allow individuals to verify their humanity without disclosing their identity[78].

Similarly, Tools for Humanity Corporation (TFH), as part of the Worldcoin project, has developed World ID[79], a digital identity system designed to safeguard user's privacy. World ID verifies an individual's humanity through an iris scan, generating a unique numerical code intended to preserve user anonymity. This digital identity functions as a "digital passport" or "identity wallet" stored on the user's phone, which can be used anonymously to verify that the individual is real and unique. The system operates via The Orb, a biometric device that scans iris patterns within seconds, creating a unique digital record of human identity[80].

Despite their innovative approach, both Proof of Humanity and World ID raise critical concerns regarding personal data protection. Fundamental questions remain unanswered: How are these biometric data processed? Who has access to them? What are the risks of data breaches, theft, or unauthorized access? If these concerns are not adequately addressed with robust safeguards, these systems could lead to significant violations of privacy rights and potential abuses of personal data.

From a doctrinal standpoint, Bajovic has explored the feasibility of biometric authentication replacing traditional username-password methods. She argues that biometric markers, such as fingerprints, could serve as digital passports for Internet access, drawing a parallel to state-controlled border security mechanisms. In her view, regulating movement in cyberspace through biometric authentication could be a necessary response to rising cybercrime rates. This proposal suggests the

74. According to its official page, EthereumEthereum is a network of computers worldwide that follow a set of rules known as the Ethereum protocol and it serves as the foundation for communities, applications, organizations, and digital assets that anyone can build and use.

75. A Sybil attack is a security threat to a P2P network that involves the control of multiple fake identities through a single device, known as a node. The scheme is similar to creating multiple accounts on a social network by the same user. In this way, a single attacker can run more than one node (IP addresses or user accounts) simultaneously on the Internet. During a Sybil attack, each fake identity appears to be real, as if they were legitimate nodes operated by different users.

76. Likewise, the creation of PoH could ensure, if necessary, that the creator of a digital property is human, rather than an AI, serving as an important complement to blockchain and positively influencing its transparency and fairness by introducing bot blocking in the chain to provide a decentralized solution for decentralized networks.

77. Also known as Zero Knowledge Protocol (ZKP).

78. For example, it could be used in the context of KYC (Know Your Client), allowing privacy to be preserved by providing a zero-knowledge proof that demonstrates one is a citizen of a specific country or over a certain age without revealing their identity.

79. Company behind ChatGPT.

80. The procedure involves downloading the Worldcoin app, then registering with a phone number, followed by receiving a QR code. Next, at one of the locations where the orbs are placed – a silver device in the shape of a sphere – an ocular scan is performed and the verification is generated.

mandatory implementation of biometric security systems to control online access.

Although this idea presents intriguing possibilities – such as linking a biometric marker[81] to a judicially imposed virtual restraining order to restrict an individual's access to certain online spaces – there are substantial legal and ethical obstacles to the large-scale implementation of biometric identification systems. These challenges extend beyond technological feasibility and raise fundamental concerns about freedom of expression, privacy, and online anonymity[82].

Particularly, the compatibility of biometric access control systems with the Regulation on Artificial Intelligence (AI Act), recently adopted by the European Union, has been the subject of evolving discussions. The initial draft of the AI Act distinguished between real-time and non-real-time biometric identification systems. Real-time systems process biometric data instantaneously or with minimal delay, whereas non-real-time systems collect and analyze biometric data after a significant delay.

Given its operational model, biometric authentication for Internet access would likely fall under real-time biometric identification, where fingerprints or iris scans are instantly analyzed to grant access. Under the AI Act's original provisions, such systems were classified as high-risk due to their potential to infringe upon users' privacy, limit their personal freedoms online, and create a sense of constant surveillance, ultimately discouraging free expression and online activity[83].

However, in its first reading on March 13, 2024[84], the European Parliament introduced amendments excluding certain biometric verification systems from the category of real-time biometric identification. Specifically, the final version of the AI Act, adopted on May 21, 2024, and published on July 12, 2024[85], explicitly exempts AI-driven biometric verification systems used solely for authentication purposes, such as verifying an individual's identity for accessing Internet services, unlocking devices, or securing facilities. Additionally, Annex III of the AI Act maintains the classification of remote biometric identification systems as high-risk but excludes verification systems used exclusively to

81. Whether it is a fingerprint or the iris.

82. Faced with the idea of feeling identified and monitored, users may begin to self-censor. This is what we could call "digital panopticism" (in an analogous reference to Bentham's panopticon). Indeed, if an individual feels surveilled (even when they are not), they will act as if they were.

83. From another perspective, we could also argue that, while it is true that there must be freedom to navigate the Internet, this must occur within the limits of what is socially and legally acceptable and permissible. Users should be able to feel free to act in the online world as they wish and express themselves in the way they deem appropriate, as long as they do not infringe upon the freedom of others. However, at the same time, they should have the fear of being discovered if they engage in online activities that violate internationally protected legal rights (since, as we have already pointed out, speaking in virtual terms simply based on state boundaries is an abstraction, just as it is in the physical world). However, we currently lack mechanisms that allow us to strike a balance between a sense of online freedom for users that does not restrict their online actions, and the necessary mechanisms to identify an internet user when investigating serious crimes. Therefore, given the palpable risk of infringing upon users' fundamental rights, we believe it is more prudent, for now, to adopt a position that favors the protection of online personal freedom, privacy, and other fundamental rights on the Internet.

84. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative acts- Outcome of the European Parliament's first readingProposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative acts - Outcome of the European Parliament's first reading (Strasbourg, 11 to 14 March 2024).

85. Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, establishing harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, establishing harmonized rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1, published in the Official Journal of the European Union (OJEU) No. 1689, on July 12, 2024.

confirm an individual's identity (a carve-out based on the presumption that such systems pose a lesser threat to fundamental rights compared to mass biometric surveillance).

This regulatory clarification could accommodate Bajovic's biometric passport proposal, as it allows biometric markers to function as digital identity credentials.

However, from our point of view, biometric data collection and processing inherently involve handling highly sensitive personal information. These data are inextricably linked to the potential infringement of fundamental rights, particularly those related to privacy and personal integrity. The European Parliament, in its first reading position, has explicitly recognized that biometric information constitutes a special category of sensitive personal data and has acknowledged the intrusive nature of biometric identification systems for the individuals subjected to them. Consequently, even when biometric data are collected exclusively for legitimate purposes, their processing must be subject to robust and sufficient safeguards to prevent abuses stemming from improper management or storage.

The legal compatibility of biometric data collection with existing regulatory frameworks remains a complex and contentious issue. The final version of the AI Act could potentially conflict with key regulatory instruments, including Article 9.1 of the General Data Protection Regulation (GDPR), Article 10.1 of Regulation 2018/1725, and Article 10 of Directive 2016/680. These legal frameworks impose a general prohibition on the processing of biometric data aimed at uniquely identifying a natural person, allowing exceptions only under specific conditions. Among these, the sole applicable exception in this context would be the explicit and informed consent of the data subject. However, a fundamental question arises: to what extent can users fully comprehend the implications of their consent, particularly in relation to the surveillance risks it entails? It is imperative to establish mechanisms that ensure not only the effective collection of consent but also the provision of comprehensive information regarding the impact of biometric data processing on fundamental rights.

Beyond these legal considerations, if biometric authentication systems were to become a mandatory prerequisite for Internet access, the notion of freely given consent would be rendered highly questionable. In the current digital landscape, Internet access can no longer be considered an optional resource but rather an essential element of social and economic interaction. Indeed, as has been previously established in legal and academic discourse, Internet access has been recognized as a fundamental right in light of the pervasive and continuous nature of digital connectivity. Under these conditions, framing the provision of biometric data as a voluntary act would be a legal fiction, as the alternative – exclusion from digital life – is neither feasible nor proportionate.

Finally, any regulatory framework governing biometric data processing must aligned with fundamental procedural safeguards, including those enshrined in the Universal Declaration of Human Rights, the European Convention on Human Rights, and other relevant international and domestic legal instruments. To prevent emerging technologies from undermining rights originally designed for the physical world, classical procedural mechanisms – such as precautionary measures – must be adapted and reinterpreted within the digital domain. This recalibration is not merely advisable but an urgent necessity in the contemporary legal landscape.

4.3.2. *Restriction of network access for devices belonging to the investigated individual*

The establishment of a digital identity as a prerequisite for accessing the Internet – particularly when biometric identification methods are employed – poses significant challenges in terms of compliance with existing regulations on personal data protection, individual freedom, and the right to privacy. The primary concern arises from the erosion of online anonymity, a fundamental element of digital privacy. Given these legal and ethical constraints, the most immediate and practical approach to implementing a virtual restraining order as a precautionary measure would be to target the electronic devices linked to the investigated individual through which Internet access is sought[86].

86. However, it is clear that this can be more easily manipulated to bypass the prohibition or restriction on access, unlike biometric data, which cannot be tampered with.

In this context, it would be worth considering the requirement for the investigated individual to compile an inventory of electronic devices, a process in which ISPs with whom the individual has contracted network access services could play an active role. This inventory would serve as the basis for enforcing the virtual restraining order, allowing for the implementation of necessary technical modifications or software installations to restrict online access.

The proposed measure aims to temporarily restrict the ability of the investigated individual to access specific digital environments or online platforms through their personal devices. Its purpose is twofold: to prevent the continuation or repetition of unlawful online behavior and to ensure the effectiveness of ongoing investigations by limiting the suspect's capacity to interfere with digital evidence or victims.

In its technical implementation, the measure should rely on a hybrid enforcement model combining two complementary mechanisms: a cooperation framework with ISPs and, where legally and technically feasible, the use of access-control software installed on the individual's devices under judicial authorization. This dual structure ensures both proportionality and technical reliability.

Under the first component, collaboration with ISPs would allow the execution of network-level restrictions. ISPs could be required to block the investigated individual's access to specific domains, IP addresses, or platforms identified by judicial order. This approach guarantees that the restriction is implemented externally, at the level of network routing or domain resolution, without requiring intrusive monitoring of user data or communications content.

Such blocking may also extend to MAC (Media Access Control) addresses assigned to the investigated individual's devices, preventing connection to particular servers or online resources[87]. Nevertheless, these technical mechanisms present inherent limitations: both IP and MAC addresses can be easily obfuscated or spoofed with minimal expertise. For instance, an individual can employ a Virtual Private Network (VPN) to mask their real IP address by routing traffic through a remote server, or use MAC address spoofing to alter their device's network identity temporarily. These techniques, while legitimate for privacy purposes, are also routinely exploited by offenders to evade detection and bypass network-level access restrictions.

The second component – local access-control software – would apply in situations where ISP collaboration may prove insufficient. This occurs particularly when the investigated individual employs anonymization tools or alternative connection channels that operate beyond the effective reach of Internet Service Providers. For instance, if the individual connects to the Internet through public Wi-Fi networks, mobile hotspots, or virtual private networks that encrypt traffic and reroute it through foreign servers, ISP-based blocking orders issued within national jurisdiction may become ineffective. In such cases, a court-authorized software application could be installed on the individual's device(s) to enforce restrictions at the system level. The software would not intercept communications but would prevent connection attempts to specific sites, services, or applications, even when the device connects through networks not controlled by the designated ISP, thereby ensuring compliance with judicially mandated prohibitions. This solution should be subject to independent oversight to guarantee transparency, data minimization, and respect for fundamental rights.

Regardless of the enforcement mechanism adopted, the principle of proportionality must guide judicial decision-making. The measure should remain temporary, targeted, and necessary, limited to preventing access to online environments directly related to the alleged criminal activity (for example, platforms hosting illicit material or enabling further victimization). The choice between network-level blocking and device-level restriction – or a combined approach – should depend on technical feasibility, the nature of the investigated offence, and the degree of judicial control required.

87. It is not always easy to link a specific IP address, VPN, or MAC address to a particular person. Consequently, a direct connection between the owner of the IP address and the individual who committed the offense cannot be made. For instance, access credentials may have been stolen. Therefore, the fact that a person owns a line with a specific IP address does not constitute necessary and sufficient evidence to hold them accountable, unless there is other evidence pointing in that direction (Spanish Supreme Court, ruling 987/2012, December 3).

To reinforce compliance, these measures could also include a temporary prohibition on entering into new contracts with ISPs or purchasing additional Internet-enabled devices, except under judicially authorized circumstances. In such cases, appropriate safeguards must be established to ensure that any newly acquired device conforms to the existing access restrictions.

By adopting a calibrated hybrid model the combines ISP cooperation with judicially supervised technical safeguards, the proposed restriction of network access achieves coherence with the broader concept of cyber-precautionary measures. It is not designed to suppress a person's general access to the Internet, but to restrict digital interaction within specific illicit contexts, thereby aligning with the overarching objectives of criminal procedure in the digital era: preserving evidence integrity, preventing reoffending, and protecting victims from ongoing harm.

5. Conclusions

The evolution of criminal activity in cyberspace has challenged the foundations of traditional criminal procedure, revealing the inadequacy of precautionary mechanisms designed for an analogue world. The dematerialization of criminal conduct, the volatility of digital evidence, and the deterritorialized nature of online interactions demand a redefinition of precautionary action. Within this new paradigm, cyber-precautionary measures emerge as an indispensable legal instrument to ensure both the preservation of digital evidence and the protection of victims from ongoing harm in the digital environment.

The analysis developed throughout this study demonstrates that these measures possess a dual legal and functional nature. On the one hand, they serve an evidentiary function, aimed at preventing the alteration or destruction of digital content relevant to the proceedings. On the other, they fulfil a preventive and protective function, designed to interrupt the circulation of unlawful material and to safeguard victims from revictimization or renewed exposure. This duality reflects a necessary evolution of precautionary law toward a model that addresses not only the risks of procedural inefficiency but also the human and social consequences of cybercrime.

Nevertheless, the effectiveness of cyber-precautionary measures depends on the existence of a robust legal and technical infrastructure. National legal systems must articulate clear procedural guarantees, ensuring judicial control, transparency, and the protection of privacy and due process. At the same time, international cooperation remains essential, given the transnational nature of cybercrime and the global architecture of the Internet. Without coordinated mechanisms for enforcement and information exchange, the reach of national precautionary measures risks remaining merely symbolic.

The fight against cybercrime requires a precautionary paradigm attuned to the digital age: one that is technologically informed, normatively coherent, and procedurally fair. Cyber-precautionary measures, properly conceived and regulated, can bridge the gap between the law's traditional tools and the realities of cyberspace. They do not seek to expand punitive power but to ensure the effectiveness, proportionality, and humanity of criminal justice in a context where harm can spread at the speed of data.

The proposed "virtual restraining order" illustrates how precautionary law can evolve to meet the demands of a society increasingly shaped by technology, while maintaining fidelity to the fundamental principles of legality, proportionality and rights protection. However, the implementation of virtual restraining orders as a precautionary tool in cybercrime investigations presents both technical and legal challenges that must be carefully balanced to ensure effectiveness without disproportionately infringing upon fundamental rights. The proposed strategies offer viable solutions for limiting an investigated individual's online activity. However, their practical enforcement is constrained by the ease with which technologically adept individuals can circumvent them, particularly through techniques such as VPN usage or MAC address spoofing.

From a legal perspective, any measure restricting digital access must comply with overarching principles of proportionality, necessity, and legality. The erosion of online anonymity, inherent in some of these measures, raises critical concerns regarding personal data protection, individual freedom, and the right to privacy. Thus, a case-by-case judicial assessment is imperative, considering the

severity of the alleged cybercrime, the technological expertise of the investigated individual, and the potential impact of the restriction on their rights.

Additionally, the role of ISPs as key facilitators in the enforcement of these measures cannot be overlooked. Their cooperation in identifying, monitoring, and restricting access to specific devices is essential, yet it must be framed within a clear legal mandate to avoid excessive delegation of law enforcement powers to private entities.

Bearing in mind these complexities, a hybrid approach – combining technical restrictions with judicial oversight and regular re-evaluation of the necessity of the imposed measures – emerges as the most balanced solution. Furthermore, any regulatory framework governing such restrictions must remain adaptable to evolving technological advancements, ensuring that legal safeguards remain robust against emerging circumvention techniques.

Ultimately, while the virtual restraining order represents a promising avenue for addressing cybercriminal activities, their implementation must be meticulously calibrated to safeguard fundamental rights while upholding the legitimate interests of criminal investigations. Only through a nuanced, legally sound, and technologically informed approach can such measures achieve their intended purpose without compromising the broader principles of justice and due process.

Bibliographic references

I.J. Acata Águila (2011), *Internet, un derecho humano de cuarta generaciónInternet, un derecho humano de cuarta generación*, in "Misión Jurídica", vol. 4, 2011, n. 4

J.R Agustina Sanllehí, I. Montiel Juan, M. Gámez-Guadix (2020), *Cibercriminología y victimización online*, Síntesis, Madrid, 2020

R. Alexy (2002), *A Theory of Constitutional Rights*, Oxford University Press, 2002

T. Álvarez Robles (2024), *El Derecho de acceso a Internet. Especial referencial al constitucionalismo español*, Editorial Tirant Lo Blanch, 2024

T. Álvarez Robles (2022), *Las garantías de los derechos fundamentales en y desde la red: el contexto español*, in "Revista Chilena de Derecho y Tecnología", vol. 11, 2022, n. 1

A. Ashworth, L. Zedner (2014), *Preventive Justice*, Oxford University Press, 2014

Z. Aslam, J. Kaaniru, D. Abiero (2025), *Recognising Access to the Internet as a Fundamental Right: Political, Socio-economic, and Legal Perspectives,* Strathmore University, 2025

S. Aterno (2000), *Sull'accesso abusivo a un sistema informatico o telematico*, in "Cassazione Penale", 2000

V. Bajovic (2017), *Criminal Proceedings in Cyberspace: The Challenge of Digital Era*, in E. Viano (ed.) "Cybercrimen, Origanized Crimen, and Societal Responses", Springer, Cham, 2017

A. Bettiga (2020), *La tutela delle vittime di reati informatici*, in "Rivista italiana di diritto e procedura penale", 2020

J. Bustamante Donas (2010), *La cuarta generación de derechos humanos en las redes digitales*, in "Revista TELOS (Revista de Pensamiento, Sociedad y Tecnología)", 2010

J. Bustamante Donas (2001), *Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica*, in "Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación", 2001

E.J. Cova Fernández (2022), *Derechos Humanos y Derechos Digitales en la Sociedad de la Información*, in "Revista Derechos Humanos y Educación", 2022, n. 6

L. Cuomo (2000), *La tutela penale del domicilio informatico*, in "Cassazione penale", 2000

C. Domenicali (2018), *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in "federalismi.it", 28 marzo 2018

T.E. Frosini (2011), *Il diritto costituzionale di acceso ad Internet*, in "Rivista AIC", 2011, n. 1

P. García Mexía (2018), *El derecho de acceso a Internet*, in T. De la Cuadra Salcedo, J.L. Piñar Mañas, (dirs.), "Sociedad digital y Derecho", Agencia Estatal Boletín Oficial del Estado, Madrid, 2018

E. Herlin-Karnell (2012), *The constitutional dimension of European Criminal Law*, Hart Publishing, 2012

V.C. Jackson (2015), *Constitucional Law in an Age of Proportionality*, in "The Yale Law Journal", vol. 124, 2015, n. 8

J. León Camacho (2020), *Evolución y desarrollo de los derechos humanos. Hacia una cuarta generación*, in R. Miranda Gonçalves, G. Martín Rodríguez, F. da Silva Veiga et al. (eds.) "El Derecho Público y Privado Ante las Nuevas Tecnologías", Editorial Dykinson, 2020

P. Martín Ríos (2017), *La indemnidad del domicilio informático como posible límite a la digital forensics*, in L. Mezzetti, E. Ferioli (a cura di), "Giustizia e Costituzione agli albori del XXI Secolo", Bonomo Editore, 2017

E. Martellozzo, E.A. Jane (2017), *Cybercrime and its Victims,* Routledge Studies in Crime and Society, 2017

H. Miranda Bonilla (2016), *El acceso a Internet como derecho fundamental*, in "Revista Jurídica IUS Doctrina", 2016, n. 15

P. Morales Aguilera (2018), *Entre el prisma discursivo y el ciberhumanismo: algunas reflexiones sobre Derechos Humanos de cuarta generación*, in "Franciscanum", vol. LX, 2018, n. 169

L. Nannipieri (2013), *Profili costituzionali dell'accesso ad Internet*, doctoral thesis supervised by R. Romboli, Università di Pisa, 2013

L. Picotti, R. Flor, I. Salvatori (2021), *Gruppo VII, Reati contro l'inviolabilità del domicilio, la tutela della vita privata e dei segreti, la libertà e la personalità informatica. Sottogruppo: Reati contro la riservatezza e la sicurezza informatiche, nonché l'identità digitale*, Università di Veronain "www.aipdp.it", 2021

R. Pisa (2010), *L'accesso ad Internet: un nuovo diritto fondamentale?,* in "Treccani Magazine", 12 gennaio 2010

O. Pollicino (2023), *The Right to Internet Access. A comparative Constitutional Legal Framework*, in "The Cambridge Handbook of Information Technology, Life Sciences and Human Rights", Cambridge University Press, 2023

O. Pollicino, G. Romeo (2016), *The Internet and Constitutional Law. The protection of fundamental rights and constitutional adjudication in Europe*, Routledge, 2016

L. Puente Rodríguez (2019), *Consecuencias del carácter procesal del "fraude de etiquetas": especial referencia a la libertad vigilada*, in "Revista General de Derecho Procesal", 2019, n. 47

J. Rifkin (2000), *The Age of Access: The New Culture of Hypercapitalism, Where All of Life is Paid-For Experience*, New York, 2000

J.C. Riofrío Martínez Villalba (2014), *La Cuarta Ola de Derechos Humanos: Los Derechos Digitales*, in "Revista Latinoamericana de Derechos Humanos", vol. 25, 2014, n. 1

S. Rodotà (2012), *Il diritto di avere diritti,* Laterza, 2012

K. Starr (2025), *Negligent delegation of digital enforcement by sovereign governments™: A framework for global constitutional accountability in privatized enforcement systems.* KStarr Enterprises, LLC, 2025

S. Signorato (2018), *Le indagini digitali. Profili struttural di una metamorfosi investigativa*, Giappichelli, 2018

M. Torre (2019), *Indagini informatiche e principio di proporzionalità*, in "Processo penale e giustizia", 2019, n. 6

M. Torre (2015), *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in "Rivista Diritto penale e processo", vol. 21, 2015

M. Trogu (2019), *Intrusioni segrete nel domicilio informatico*, in A. Scalfati (a cura di), "Le indagini atipiche", Giappichelli, 2019

E. Velasco Núñez (2012), *Medidas restrictivas en Internet: cómo retirar contenidos ilícitos*, in M. Bauzá Reilly, F. Bueno de Mata (coord.), "El derecho en la sociedad telemática. Estudio en homenaje al profesor Valentín Carrascosa López", Andavira, 2012

A. Venegoni, I. Giordano, (2016), *La Corte costituzionale tedesca sulle misure di sorviglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in "Diritto Penale Contemporaneo", 8 maggio 2016