Revista de la Facultad de Derecho de México
Tomo LXXIII, Número 287, Septiembre-Diciembre 2023
DOI: http://doi.org/10.22201/fder.24488933e.2023.287.86913

Searches and Seizures in the Digital Age—The Need For a Prior Independent Oversight Among International and European Standards

La Incautación en la Era Digital: La Necesidad de una Supervisión Independiente Previa según los Estándares Internacionales y Europeos

Lorenzo Bernardini*

Abstract: The relentless march of technological progress has significantly streamlined the collection, transmission, and electronic storage of personal information, reshaping the landscape of searches and seizures of electronic devices. This digital evolution allows prosecuting authorities unprecedented access to vast volumes of information stored on computers, raising concerns about the potential misalignment between seized documents and suspected criminal activities. Emphasizing the importance of procedural guarantees for individuals impacted by digital searches and seizures measures, scholars have traditionally advocated for prior authorization from an independent authority. Still, the mere presence of prior authorization does not guarantee non-arbitrary implementation of those measures. Amidst this framework, international standards prefer prior judicial oversight, with "freedom from arbitrariness" test guiding competent authorities in scrutinizing relevant case facts. Conversely, the European legal framework,

* Postdoctoral Researcher in Criminal Law at the University of Luxembourg. PhD in Global Studies and Master of Laws at the University of Urbino "Carlo Bo". Contact: <lorenzo.bernardini@uni.lu>. Fecha de recepción: 12/10/2023. Fecha de aprobación: 19/10/2023.

DOI: http://doi.org/10.22201/fder.24488933e.2023.287.86913

especially Article 8 ECHR, lacks clarity, risking the fundamental nature of the right to privacy by allowing intrusive measures without prior control.

Keyword: Searches and Seizures; Article 17 ICCPR; Article 8 ECHR; Legality; Arbitrariness; Prior Independent Oversight.

Abstract: El incansable avance del progreso tecnológico ha simplificado significativamente la recopilación, transmisión y almacenamiento electrónico de información personal, transformando el panorama de incautaciones de dispositivos electrónicos. Esta evolución digital proporciona a las autoridades judiciales un acceso sin precedentes a vastos volúmenes de información almacenada en computadoras, generando preocupaciones sobre el posible desajuste entre los documentos incautados y las actividades delictivas sospechosas. Destacando la importancia de garantías procesales para individuos afectados por medidas de incautación digital, los académicos han abogado tradicionalmente por la autorización previa de una autoridad independiente. Sin embargo, la mera presencia de autorización previa no garantiza una implementación no arbitraria de esas medidas. En este marco, las normas internacionales prefieren la supervisión judicial previa, con la prueba de "libertad de arbitrariedad" guiando a las autoridades competentes en el examen de los hechos relevantes del caso. Por otro lado, el marco legal europeo, especialmente el Artículo 8 del CEDH, carece de claridad, poniendo en riesgo la naturaleza fundamental del derecho a la privacidad al permitir medidas intrusivas sin control previo.

Palabras claves: Incautación; Artículo 17 PIDCP; Artículo 8 CEDH; Legalidad; Arbitrariedad; Supervisión Independiente Previa.

I. Some introductory remarks

The fight against criminal phenomena is essential for ensuring security in modern societies, and nowadays its effectiveness may largely depend on the use of modern and digital investigative techniques.[1] The utilization of electronic devices, such as laptops, tablets, smartphones, smartwatches, and smart TVs, has become extremely pervasive in contemporary society, and criminal offenders are no exception. Very often, these IT tools are employed to commit criminal offenses – not only cybercrimes strictly speaking (e.g., cybersex trafficking or phishing) but also a wide range of other non-inherently-digital criminal offenses (e.g., an encrypted message sent among accomplices to organize a bank robbery or a murder). In turn, this implies that IT tools may become valuable sources of evidence in the context of criminal proceedings.

Indeed, electronic records, including computer network logs, emails, word processing files, and image files, are progressively serving as significant –oftentimes indispensable– evidence in criminal cases. The substantial surge in digital-related crime thus necessitates that prosecutors, judges and law enforcement officials acquire the expertise to procure the digital items stored in IT devices.

Among the legal tools that prosecuting authorities typically employ during the investigations, search and seizure measures (SSMs) play a pivotal role for the purpose of preserving electronic evidence.[2] This is so for several reasons. Firstly, these tools allow to

[1] In this regard, for a comprehensive analysis, see Bachmaier Winter, L., "Criminal Investigation, Technological Development, and Digital Tools: Where Are We Heading?", in Bachmaier Winter, L. and Ruggeri, S. (eds.), *Investigating and Preventing Crimein the Digital Era*, Cham, Springer, 2019, pp. 3-17.

[2] See, for instance, the legislative reform of the Spanish Code of Criminal Procedure which broadened the scope for the employment of SSMs of IT

DOI: http://doi.org/10.22201/fder.24488933e.2023.287.86913

temporarily seizing electronic devices, preventing the owner from altering, transferring, converting, or deleting any data contained therein. Secondly, such orders are indispensable instruments for securing digital evidence and ensuring its integrity throughout preliminary investigations and, eventually, the trial. Thirdly, almost every criminal investigation faces the necessity to access electronic data for the purpose of reconstructing the facts of the case – even if national authorities are equipped with a robust toolkit of other measures for the same purpose (e.g., wiretappings), SSMs are the most significant ones because they are the sole means by which investigating authorities can gain physical possession of the relevant IT tool and, more importantly, all the huge amount of information contained therein.

In this regard, I pointed out elsewhere that "the *fil rouge* between 'searches' and 'seizures' has become uncertain in the digital realm. In non-digital investigations, the authority usually issues a search warrant and, if evidence is found, a seizure can be implemented. However, in the digital field, the opposite is often true. As a general rule, investigating authorities make first a forensic copy of the IT device (a 'seizure') and, afterwards, search for the relevant data – this *modus operandi* is followed in order to preserve data integrity".[3]

---

tools. For a comprehensive analysis, see López-Barajas Pereja, I., "Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos", in *IDP. Revista De Internet, Derecho Y Política*, 2017, n. 24, pp. 64-76 and Rayón Ballesteros, M.C., "Medidas de investigación tecnológica en el proceso penal la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", in *Anuario jurídico y económico escurialense*, 2019, n. 52, pp. 179-204.

[3] Bernardini L. and Sanvitale, F., "Searches and Seizures of Electronic Devices in European Criminal Proceedings: A New Pattern for Independent review?", in *Revista Ítalo-española De Derecho Procesal*, 2023, n. 1, pp. 79-80.

The latter is a focal point of the analysis. Technological developments have brought unexpected changes to modern societies (and, as a consequence, to criminal proceedings, particularly concerning the role of digital evidence).[4] The exponential growth in the use of electronic tools has led to an unprecedented amount of personal data being generated, stored, and transmitted daily, raising various privacy and security concerns.[5] It is noteworthy that the data stored in an IT device could paint a *comprehensive picture of the person under investigation*. It extends beyond photos or videos, encompassing the content of emails, SMS messages, traffic, and location data, all of which can be examined and retained by the investigating authorities.[6]

This is especially relevant in criminal proceedings when the contents of electronic devices are the focus of investigation. It becomes thus crucial to ensure that the implementation of digital SSMs (i.e. SSMs of IT devices) is balanced with the protection of the individuals' right to privacy. In other words, the use of such measures shall not result in an arbitrary infringement of the prerogatives of the individuals.

The central issue in the clash between the necessity to preserve digital evidence in criminal proceedings and the rights of the individuals subjected to digital SSMs lies in the rhetorical question posed by Judge Pavli of the European Court of Human Rights

---

[4] Rodrigo, F.M., "La Evidencia Digital en el Proceso Penal Y la Preservación de los Derechos Fundamentales", in *Revista Acadêmica Escola Superior Do Ministério Público Do Ceará*, 2021, n. 13(1), pp. 135–161.

[5] While, on the contrary, "the existing rules of evidence collection, especially the search and seizure regime, is largely designed for physical evidence and eyewitness accounts" (Leacock, C., "Search and Seizure of Digital Evidence in Criminal Proceedings", in *Digital Evidence and Electronic Signature Law Review*, 2008, n. 5, p. 225).

[6] In contrast, other traditional surveillance measures, such as wiretappings, reveal only partial yet pertinent pieces of information, specifically the suspect's conversations *at the time they occur*.

(ECtHR) – "how many of us can claim to keep an impenetrable wall between the personal and professional data held within our smartphones?".[7]

For the purpose of this analysis, I would provocatively rephrase this question as follows – how can investigating authorities assure citizens that they will establish an impenetrable wall between the data pertinent to investigations and all other data? That is to say, more broadly, how can they ensure that they will search and seize *only those IT tools (and those pieces of information) that are relevant for the investigations*, setting aside all others? Those issues are strictly linked, on the one hand, to the vast amount of data contained within IT tools and, on the other hand, to the potential infringement of individual prerogatives on the part of the investigating authorities.

As noted by Moore, a potential concern in this context may revolve around *whether the judge issuing the search warrant fully comprehends the scope of the search*.[8] Whereas it is crucial that law enforcement officers requesting a warrant make certain that the judge has a clear understanding of what the officer intends to search for and the types of information that may be uncovered, this is not always possible due to "new advances and new terminology being used in the field of computer technologies everyday".[9]

Against this background, it should not be forgotten that breaches of the right to private life may result in substantial consequences, such as severe damage to reputation, the exposure of highly sensitive information regarding medical treatments or sexual orientation, the disclosure of bank account credentials, and a breach of confidentiality that should cover specific conversations, including those between lawyers and their clients. Therefore, the

---

[7] *Särgava v. Estonia*, App. no. 698/19 (ECtHR, 16 November 2021), Concurring Opinion of Judge Pavli, para. 5.

[8] Moore, R., *Search and Seizure of Digital Evidence*, New York, LFB Scholarly Publishing LLC, 2005, p. 80.

[9] *Ibidem*, pp. 80-81.

implementation of digital SSMs present noteworthy challenges due to the extensive volume of personal data contained therein which may also *relate to individuals other than the device's owner*.[10] A primary concern is the matter of procedural safeguards that must be guaranteed for the individuals involved, whether they are the suspect/accused person or a third party. This becomes especially critical due to the broad powers often wielded by prosecuting authorities in the process of searching and seizing electronic devices.

In this context, and following the example of various criminal justice systems,[11] it may intuitively be contemplated that, in order to forestall arbitrary conduct by investigating authorities, a prior independent scrutiny mechanism should be established. To put it differently, in order to avert law enforcement officers or public prosecutors from conducting searches and seizures of IT tools in an arbitrary fashion, the necessity for a *ex ante* independent evaluation of the legality of SSMs should be acknowledged. As a result, the implementation of a prior independent oversight may – and, in my understanding, should – emerge as a fundamental aspect of the procedure in which investigating authorities deliberate on digital SSMs.

The need for an *ex ante* evaluation could encompass an analysis of the necessity and proportionality of digital SSMs and may be

[10] Historically, personal information about a suspect might have been obtained, among other methods, through witnesses, phone tapping, and material evidence (e.g., tax documents). Yet, the landscape has crucially changed. As a concrete example, smartphones and personal computers now serve as repositories in which individuals gather personal information, not only belonging to themselves but also to third parties.

[11] In Germany, Article 98 of the German Code of Criminal Procedure (StPO, *Strafprozeßordnung*) provides that "seizures may only be ordered by the court, and in cases of imminent danger, also by the public prosecutor's office and its investigative personnel". Therefore, as a general practice, SSMs are sanctioned only following an independent evaluation by the judicial authority. Notably, this holds true even when the subject of seizure is not a digital device.

conducted by a panel of public officers, judges or experts, rather than a sole individual, thereby guaranteeing a more comprehensive and equitable assessment of the specific circumstances and decreasing the potential for biases in the decision-making process. Whereas I do not dispute that the introduction of a prior assessment requirement alone would not render the entire procedure less arbitrary,[12] I would nonetheless maintain that the lack of any *ex ante* independent oversight on SSMs of IT tools poses a risk of significantly expanding the powers of investigating bodies to a degree that may be incompatible with individuals' right to private life. This situation also may increase – and, regrettably, might foster – the potential for haphazard implementation of digital SSMs.[13]

---

[12] I thus espouse the view according to which "judicial involvement in oversight should not be viewed as a panacea" (see the report *The Right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, 30 June 2014, para. 38). For a critical perspective, see Kerr, O.S., "Searches and Seizures in a Digital World", in *Harvard Law Review*, 2005, n. 119(2), pp. 571-576. Kerr claimed that "a requirement that courts approve search strategies ex ante (…) serves little purpose" due to several factors – among others, he mentioned the fact that "warrant applications are *ex parte*" and this implies that "a judge must try to determine whether the search protocol is appropriate based only on the government's presentation of the empirical picture" as "it is generally impossible to know ahead of time what techniques officers need, and judges in ex parte proceedings are particularly unlikely to grasp the difficulties" (*ibidem*, pp. 575-576).

[13] In the absence of prior independent authorization, public prosecutors or law enforcement officers might be permitted, for example, to conduct a search and seize all the IT tools belonging to an alleged dangerous suspect, subsequently affording the individual an opportunity to contest the legality of such a measure. Even if a violation of the right to privacy is established afterward (e.g., due to unnecessary or disproportionate implementation of digital SSMs in their regard), the indisputable fact remains that the investigating authorities have gained awareness of the content within the IT tools at stake. This

Still, may such an assessment be *indispensable* according to international law standards? To answer this question, my analysis revolves around what I call a *qualitative* argument. Digital SSMs possess a degree of severity against the individual concerned that is qualitative comparable to that held by other intrusive measures, such as wiretappings[14] or home searches.[15] In interpreting the scope and the extent of the right to privacy as safeguarded at the international level, the UN Human Right Committee (HRC) has not established a uniform stance regarding the procedural safeguards

---

issue represents a breach of the right to privacy that no *ex post facto* procedural guarantee can rectify.

[14] Wiretappings and digital SSMs share a qualitative similarity in terms of intrusiveness, albeit with quantitative differences. While phone tapping allows investigating authorities to eavesdrop on and record *phone conversations* of a suspect at the time they occur, SSMs enable authorities to gain access to an electronic device and gain comprehensive insight into its entire contents (photos, videos, messages, contacts, metadata, traffic and location data *etc.*). From this perspective, SSMs appear to be more invasive than wiretappings because they heavily affect the most intimate aspects of a person's life. Conversely, in situations where, for instance, the individual subject to wiretapping refrains from using the phone or avoids discussing the crime over the phone, wiretappings prove to be entirely ineffective. In other words, there is a *higher likelihood* that the suspect's mobile phone contains *pertinent information* concerning both themselves and third parties; contrarywise, before ordering a phone tapping, there might be uncertainty regarding, for instance, whether the suspect will discuss the crime over the phone.

[15] House searches may be equated to digital searches in that the latter "like the traditional searches (…) are usually followed by the seizure of information stored in hardware, servers, clouds, mailboxes (…) the reach of search and seizure of digital evidence in cyberspace is enormous" (Di Nuzzo, V., "Search and Seizure of Digital Evidence: Human Rights Concerns and New Safeguards", in Bachmaier Winter, L. and Ruggeri, S. (eds.), *op. cit.*, p. 121). Also, in this regard, see Kerr, O.S., "Search warrants in an era of digital evidence", in *Mississippi Law Journal*, 2015, n. 75(1), pp. 90-95.

that should be extended to individuals impacted by digital Ssms. However, it has offered valuable insights with respect to surveillance measures and home searches. Consequently, addressing the earlier question would involve carving out the standards developed for these aforementioned instruments and examining their relevance when applied to the context of digital Ssms. Differently, in the European legal framework, several decisions of the European Court of Human Rights (Ecthr) dealt directly with the procedural guarantees to be ensured to individuals affected by digital Ssms. In this last regard, accordingly, the qualitative approach may provide an added value to the analysis, but it does not constitute its kernel.

In this paper I will explore the international and European standards regarding the need for a prior independent assessment in the context of the implementation of digital Ssms. The focus will thus not be on the necessity to combine such antecedent authorization with a subsequent assessment (which, in my understanding, would represent the optimal scenario).[16]

This article consists of three parts. Part II and III pertain, respectively, to the international and European standards concerning the necessity of establishing prior independent oversight as a prerequisite for the legality of digital Ssms. Part IV will offer concise comparative and concluding remarks on the key issues highlighted in the preceding analysis.

II. Brushstrokes of Privacy—Illuminating the Role of "Lawfulness" and "Freedom from Arbitrariness" Criteria in Painting *ex Ante* Independent Review Mechanisms in the Context of Digital Searches and Seizures

[16] I have already dealt with this issue in Bernardini L. and Sanvitale F., *op. cit.*, pp. 95-106.

As anticipated, digital SSMs are extremely invasive legal tools, and their implementation plainly encroaches upon the individuals' right to privacy. But which are the substantive and procedural international standards under which these measures may be deemed lawful? And, specifically, does international law imply a requisite for a prior, independent oversight in the authorization of digital SSMs measures?

At the international level, both Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) protects the right to privacy.[17] Specifically, Article 17(1) ICCPR stipulates the entitlement of an individual to safeguard against "arbitrary or unlawful" encroachments upon their privacy, family, home, or correspondence, and further shields them from "unlawful attacks" on their honor and reputation. Besides, Article 17(2) of the ICCPR ensures that every individual is afforded "protection of the law against such interference". Importantly, it is immaterial whether such interference originates from private individuals or governmental authorities, as the safeguards of Article 17 ICCPR are applicable in any case.[18] Whereas the wording of this latter provision is concise, it has been dubbed "versatile" by legal scholars, as it would be "capable of answering a broad diversity of unlawful and arbitrary incursions into privacy (…) including many instances which could not have been specifically foreseen by the drafters".[19]

---

17 UN General Assembly, *Resolution adopted by the General Assembly on 18 December 2013*, *The right to privacy in the digital age*, A/RES/68/167, 21 January 2014, para. 1.

18 UN Human Rights Committee, *General Comment No. 16*, *Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)*, Adopted at the Thirty-second Session of the Human Rights Committee on 8 April 1988, para. 1.

19 Taylor, P.M., *A Commentary on the International Covenant on Civil and Political Rights. The UN Human Rights Committee's Monitoring of ICCPR Rights*, Cambridge, Cambridge University Press, 2020, p. 458.

Arguably, SSMs of digital devices may be considered one of those instances, involving the collection of extremely sensitive personal data. I thus share the view of those who contend that the concept of "home" under Article 17 ICCPR should encompass not only physical residences but also online, virtual, and digital private spaces (e.g., a smartphone's memory). Similarly, the term "correspondence" should be construed to include all forms of communication, irrespective of whether they are analog or digital in nature.[20]

In the context of the present analysis, by "privacy", I refer to a domain of personal autonomous development, interaction, and liberty that is free from State intervention and "free from excessive unsolicited intervention by other uninvited individuals".[21] Under Article 17(1) ICCPR, both *unlawful* and *arbitrary* interference of the right to privacy are forbidden. Each facet of this dichotomy bears autonomous meaning, as any infringement of such provision must not only conform to the requirements of legality but must also refrain from being arbitrary.

A) The Two Legs of "Lawfulness"— Does Article 17 ICCPR Mandates to Establish a Prior Independent Oversight?

That of "lawfulness" (or "legality") constitutes the primary element subjected to scrutiny when assessing an alleged infringement of the right to privacy. In fact, Article 17 ICCPR does not furnish an exhaustive enumeration of circumstances wherein such interference might be permissible. Instead, it merely defers to domestic legislations, entrusting them with the responsibility to provide

[20] See ACLU, *Privacy Rights in the Digital Age. A Proposal For a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights*, New York, 2014, pp. 16-18.

[21] See the *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/13/37, 28 December 2009, para. 11.

"the protection of the right set forth in [Article 17 ICCPR]" at the national level.[22] In the seminal *Van Hulst* decision – concerning the wiretapping and recording of the applicant's telephone calls (a lawyer) with his client –, the Human Rights Committee (HRC) ruled out the presence of an interference with Article 17 ICCPR on the basis that the latter "complies with the relevant domestic law, as interpreted by the national courts".[23] At a first glance, the HRC's approach proves to be very formalistic.

Yet, under the umbrella of the notion of "lawfulness" is also the need to ensure the "protection of the law" against the infringement of the right to privacy, a *dictum* which is laid down in Article 17(2) ICCPR.[24] This seems to be a ground which refers to the *quality* of the law, in spite of its formal existence within a legal framework. It implies that domestic legislation must comprehensively outline the "precise circumstances" under which infringements upon the right to privacy could be authorized.[25]

In this vein, the HRC has ruled out in *Pinkney* that a law drafted in excessively general terms could be deemed in keeping with Article 17(2) ICCPR.[26] This aligns with the obligation imposed on State Parties to ensure that pertinent legislation is specific in detailing the grounds under which an infringement of the right to privacy may be permissible. The public accessibility of those laws and, more importantly, the need to specify therein "the procedures for authorization" of the measures at stake are also factors to be taken in due consideration.[27]

---

22 UN Human Rights Committee, *op. cit.*, para. 2.

23 *Van Hulst v. the Netherlands*, CCPR/C/82/D/903/1999 (HRC, 1 November 2004), para. 7.5 *in fine*.

24 Taylor, P.M., *op. cit.*, pp. 461-462.

25 UN Human Rights Committee, *op. cit.*, para. 8.

26 *Pinkney v. Canada*, CCPR/C/OP/1 (HRC, 29 October 1981), para. 34.

27 These are the grounds referred to by the HRC in its *Concluding observations on the fourth periodic report of the United States of America*, CCPR/C/USA/CO/4, 23 April 2014, para. 22(b)(iii) and in its *Concluding observations on*

In a nutshell, the respect of the principle of lawfulness demands a dual evaluation of the legal instrument under scrutiny: (i) the formal presence of a legal provision permitting the implementation of such a measure (i.e., legality *stricto sensu*); (ii) the requirement that such a law be precise, comprehensive, and furnish specific details regarding the circumstances under which the right to privacy might be encroached and, interestingly, the procedural steps to be taken for *authorizing* those measures (i.e., the quality of law requirement).

The latter point is of a certain interest for the purpose of the present analysis. I will now scrutinize the principal findings of the HRC within the framework of the two legal instruments that, in accordance with the *qualitative* approach I endorse, may serve as benchmarks, namely, surveillance measures and house searches.

In the field of surveillance measures (typically, wiretappings and data retention procedures), the HRC has pointed out the imperative for domestic legislation to delineate the procedure governing the *authorization* of any intrusion into the right to privacy. As for the extent of such a prior assessment, different viewpoints have been endorsed by the Committee. In 2014, it urged the United States of America to foster the "judicial involvement in the authorization or monitoring of surveillance measures", stopping short, however, of explicitly demanding prior *judicial* oversight on intrusive measures.[28] Yet, in 2015, it demanded *expressis verbis* that the United Kingdom institute measures for "providing for judicial involvement in the authorization of [surveillance] measures *in all cases*".[29]

---

the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 17 August 2015, para. 24(b)(iii).

[28] See the *Concluding observations on the fourth periodic report of the United States of America*, *op. cit.*, para. 24(c).

[29] See the *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland*, *op. cit.*, para. 24(c), emphasis added.

While these differing perspectives may be influenced by the particulars of individual domestic frameworks, it remains a consistent principle that, in any scenario, prior authorization is essential in the context of surveillance measures. Notably, the Committee's findings appear to be grounded in the substantive content of Article 17 ICCPR, which implies – as per the "quality of law" requirement – the necessity for legal provisions shaping authorization procedures. Consequently, this would indirectly confirm the imperative existence of such procedures.

As for the competent authority, the 2015 UK Concluding Observations, addressing the "current legal regime governing the interception of communications and communications data",[30] advocate for substantial court involvement "in all cases", as anticipated. This stance aligns with the HRC's commitment to enhance the effectiveness of authorization procedures, entrusting them to typically independent and impartial authorities such as courts.[31] This is evident from the position articulated in *Van Hulst*, where the Committee acknowledged that Dutch law fulfilled the requirements of Article 17 because the interception of communications had to be "based on a written authorization by the investigating judge".[32]

In this vein, the Committee has ruled out that determinations regarding the legality of surveillance measures can rest solely within the purview of a Prosecutor General, without any sort of judicial review. Consequently, it has recommended that "the competence to decide upon *requests for* and the legality of such [sur-

[30] *Ibidem*, para. 24. Interestingly, the HRC did not explicitly focus on counter-terrorism or national security interception of communications. Consequently, the observations regarding the significance of judicial involvement in *ex ante* oversight over surveillance measures are of a particular interest, as broadly applicable to general wiretappings' legal regimes.

[31] See, for further references, Taylor, P.M., *op. cit.*, pp. 476-478.

[32] *Van Hulst v. The Netherlands*, *op. cit.*, para. 7.7 *in fine*. See, for further references, ACLU, *op. cit.*, pp. 27-28.

veillance] activities be *transferred to the courts*".[33] In support to this standpoint, it is noteworthy that the HRC expressed concern about the "lack of adequate *judicial* oversight" in the Polish counter-terrorism wiretapping framework. This concern prompted the Committee to urge the State Party to reassess its legislation "in order to *bring it into line with its obligations under the Covenant*",[34] thus upholding that the absence of judicial involvement may render *per se* such interference with the right to privacy incompatible with Article 17 of the ICCPR. This inclination towards a prior *judicial* assessment was explicitly articulated in a 1997 report, wherein the Committee underscored the significance of "appropriate mechanisms for judicial oversight" as a means to align the domestic framework with the provisions of Article 17 of the ICCPR.[35] More straightforwardly, the Committee express concerns that, in the then-Polish criminal procedure framework, "the Prosecutor (*without judicial consent*) may permit telephone tapping".[36]

Whereas in the realm of surveillance measures the HRC emphasized the necessity for a prior oversight ideally conducted by a judicial authority, in the context of house searches, the Committee emphasized the importance of these measures being executed with a *warrant*. These two aspects are fundamentally interlinked – a warrant is typically granted following a prior assessment of requests made by prosecutors or law enforcement officials to employ certain intrusive measures against individuals. In other

---

[33] See the *Concluding Observations of the Human Rights Committee (Belarus)*, CCPR/C/79/Add.86, 19 November 1997, para. 15, emphasis added. More recently, cfr. *Andrei Sannikov v. Belarus*, CCPR/C/122/D/2212/2012 (HRC, 14 May 2018), para. 6.9.

[34] See the *Concluding observations on the seventh periodic report of Poland*, CCPR/C/POL/CO/7, 23 November 2016, paras. 39-40, emphasis added.

[35] See the *Concluding Observations of the Human Rights Committee (Jamaica)*, CCPR/C/79/Add.83, 19 November 1997, para. 20.

[36] See the *Concluding Observations of the Human Rights Committee (Poland)*, CCPR/C/79/Add.110, 29 July 1999, para. 22, emphasis added.

words, the warrant represents the *outcome of a prior oversight process*. Once this process is completed and the relevant request is approved, the competent authority issues a warrant, which serves as the legal basis for executing the subsequent interference with the individual concerned.[37] This clearly aligns with the need to ensure that "searches at a person's home should be restricted to a search for necessary evidence and should not be allowed to amount to harassment".[38]

The Committee has been clear that house searches without a previous warrant are incompatible with Article 17 ICCPR. In *Coronel et al.*, home raids carried out by soldiers against victims' houses were dubbed illegal "*since* the soldiers did not have search or arrest warrants".[39] There is thus a link between the lack of search warrants and the unlawfulness of subsequent house searches, as reiterated in *Boudjema*.[40] Looking at a Malawian legal provision that broadened the authorization of searches without warrants,

---

[37] Typically, the request is submitted by the public prosecutor to the judge who, following an assessment of the circumstances of the case, may issue the warrant. However, it is plausible that a warrant might be authorized by a public prosecutor following a request from law enforcement authorities. Nevertheless, in the latter scenario, some concerns may arise regarding the impartiality of the oversight conducted by the prosecutor, particularly when the latter is subject to hierarchical dependence on the government. Therefore, I would lean towards the idea that a warrant should consist in an official order issued by an impartial authority, such as the court, in response to a request from the public prosecutor or law enforcement agencies. This is notwithstanding the fact that, in instances where public prosecutors operate independently from the government and the parties to the proceedings (e.g., in the Italian criminal justice system), the aforementioned apprehensions may be significantly mitigated.

[38] UN Human Rights Committee, *op. cit.*, para. 8.

[39] *José Antonio Coronel et al. v. Colombia*, CCPR/C/76/D/778/1997 (HRC, 29 November 2002), para. 9.7, emphasis added.

[40] *Abdelkader Boudjema v. Algeria*, CCPR/C/121/D/2283/2013 (HRC, 1 December 2017), para. 8.11.

the Committee called upon the State Party to undertake all requisite measures (i.e., repealing the provision at stake) to prevent arbitrary searches and infringements on liberty and privacy.[41] What is more, in expressing concerns over abuses by authorities in implementing house searches, the HRC urged Belarus to shift the authority to make decisions regarding requests for (and the legality of) house searches from the Prosecutor General to the judiciary.[42]

As a result of this composite framework, it appears that the HRC is dedicated to averting unlawful encroachments upon the right to privacy by imposing various obligations on State Parties. Among them is the requirement for State Parties to establish accessible and predictable provisions within their domestic legal frameworks, with a particular emphasis on precision and specificity. This is aimed at preventing abuses of authority by national bodies. Besides, the preference for a prior *judicial* –and not merely *independent*– oversight on alleged interferences against the right to privacy seems to emerge from both the jurisprudence and the Observations of the HRC.

Against this backdrop, much like surveillance measures and house searches, the implementation of digital SSMs should be regarded as a profoundly intrusive legal tool. It has the potential to infringe upon individuals' right to privacy in a manner comparable to, and often more invasive than, wiretappings or house searches. In my understanding, even SSMs should necessitate a prior *judicial* authorization to be ordered and executed, meaning that a warrant should be issued by a court before their implementation. This approach aligns with the "quality of law" requirement deri-

---

41 See the *Concluding observations on the initial periodic report of Malawi*, CCPR/C/MWI/CO/1/Add.1, 19 August 2014, para. 20. The same exhortation was indeed contained in the *Concluding Observations of the Human Rights Committee (Malawi)*, CCPR/C/MWI/CO/1, para. 14.

42 See the *Concluding Observations of the Human Rights Committee (Belarus)*, cit., para. 15.

ved from Article 17 of the ICCPR, which mandates that the relevant legal provisions must be precise, comprehensive, and provide specific details regarding the circumstances under which the right to privacy may be infringed, along with the procedural steps for *authorizing* such measures.

B) The Blurred Portrait of the Non-Arbitrariness Test—How Should a Prior Judicial Oversight Mechanism Be Conceived?

While the implementation of a prior judicial oversight appears to be the most appropriate mechanism for State Parties to deploy digital SSMs without violating Article 17 ICCPR, it should be noted that the mere existence of such authorization is not sufficient *per se*. In other words, while advocating for a prior judicial oversight for digital SSMs is commendable, such oversight could become bureaucratic, formalistic, and, to some extent, arbitrary if, for instance, the burden of proof required to authorize the measure is set at a very low threshold.[43] Similarly, such an evaluation could become pointless if the measure at stake is allowed to be conducted for an indefinite duration. By analogy, the efficacy of judicial control might be rendered ineffective when it relies on legal presumptions (e.g., in the case of serious criminal offenses, where, in some State Parties, the necessity of the measures might be presumed by law).

Accordingly, the fact that the principle of lawfulness is complied with does not imply, in turn, that State Parties are accorded an unrestricted *carte blanche* in this domain. Indeed, certain interferences with the right to privacy – though formally complying with the two facets of the principle of legality, that is, even when

[43] This aspect was expressly stressed in the *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40, 17 April 2013, paras. 54-57.

authorized by a judicial authority – may still run afoul "the provisions, aims, and objectives of the Covenant".[44]

In order to avert such scenarios, the criterion of arbitrariness assumes paramount significance. This essentially entails that the existence of a provision of a certain "quality" in domestic law allowing for an infringement of the right to privacy is a *necessary* ground, yet not *sufficient*, to acknowledge the compliance of a certain measure with Article 17 ICCPR.

Whereas the ground of legality is mildly straightforward to ascertain, that of arbitrariness is more blurred. In accordance with the succinct language of General Comment No. 16, the concept of "arbitrary interference" includes interferences that are "provided for under the law". Also, it is stressed that the introduction of the term "arbitrariness" serves the purpose of ensuring that compliance with the principle of legality does not exempt State Parties from their obligations to ensure that every interference with the right to privacy aligns with the "provisions, aims, and objectives of the Covenant".[45] Finally, the HRC highlighted that "in any event", the measure at stake shall be "reasonable in the particular circumstances".

To precisely define the criteria by which compliance with the non-arbitrariness criterion may be determined, it is essential to draw upon the jurisprudence of the HRC which specifically focused on the concept of "reasonableness".[46] In *Toonen*, the Committee famously stressed that the latter notion encompasses the need for the measure at stake to be "proportional to the end sought" and to be "necessary in the circumstances of any given case".[47] Hence, for a measure to be deemed reasonable, it must be *both* necessary and proportionate in the specific case. This implies that

---

44 UN Human Rights Committee, *op. cit.*, para. 4.

45 *Idem*.

46 See, among others, *Ilyasov v. Kazakhstan*, CCPR/C/111/D/2009/2010 (HRC, 23 July 2014), para. 7.2.

47 See *Toonen v. Australia*, *op. cit.*, para. 8.3 *in fine*.

a personalized assessment is required for the impact of any proposed measure, and in consideration of this, its proportionality, in relation of a *legitimate aim* to be pursued.[48] In this context, the purpose for which the measure is undertaken becomes crucial in the analysis, further considering that "it is not enough that [a certain restriction] serves one of the legitimate aims, [but] it must be necessary for reaching the legitimate aim".[49] As acknowledged in *Van Hulst*, the necessity to implement effective measures for the prevention and prosecution of criminal offenses can be considered a "legitimate aim" within the framework of the non-arbitrariness assessment.[50] After all, it is universally understood that once an individual becomes subject to a formal criminal investigation, infringements to their right to privacy may occur for law enforcement purposes.[51]

Interestingly, whereas the Committee has typically emphasized the proportionality between the measure and the objectives pursued, it also considered the *impact of the interference on the applicant* ("its effects on him") in *Canepa*.[52] This finding is particularly interesting because digital interferences on the right to privacy can have a far-reaching impact on the personal lives of individuals. Such impact-factor may thus reveal an inherent importance in the arbitrariness assessment when intrusive digital

---

48 Taylor, P.M., *op. cit.*, p. 464.

49 See the *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *op. cit.*, para. 29.

50 *Van Hulst v. The Netherlands*, *op. cit.*, para. 7.6 *in fine*. In this light, wiretappings, house searches, and digital SSMs adopted in this context may appropriately be characterized as necessary measures, determined on a case-by-case basis, for the purpose of combating crime.

51 See, in this regard, the *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, op. cit., para. 30.

52 *Canepa v. Australia*, CCPR/C/59/D/558/1993 (3 April 1997), para. 11.4.

or surveillance legal tools are implemented. To further clarify the framework, the Committee has further supplemented the concept of "reasonableness" with other criteria – a measure may be deemed arbitrary where it displays elements of "inappropriateness, injustice, lack of predictability and due process of law".[53] In a nutshell, infringements of the right to privacy must conform with the spirit of article 17 ICCPR, including (but not limited to) the principles of legality, proportionality and necessity.[54] The latter two concepts form part of the broader non-arbitrariness assessment undertaken by the HRC, as consistently reiterated in the aforementioned Committee's jurisprudence. Besides, other features of the measure at stake (e.g., its inappropriateness) shall be considered.

Turning back to the prior judicial oversight issues, the concept of arbitrariness, as conceived by the HRC, can be highly valuable in shaping the *extent* and *authority* that courts should hold when deciding whether to authorize an intrusive measure that affects the right to privacy. In other words, while the principle of legality appears to require State Parties to establish certain judicial *ex ante* authorization mechanisms when implementing digital SSMs which affect the rights enshrined in Article 17 of the ICCPR, the notion of arbitrariness helps to precisely *delineate the functions of these authorities*. As they should be courts – not public prosecutors – their powers should be structured within domestic frameworks to endow them with substantive authority to assess the arbitrariness of the measure in question.

---

[53] See, among others, *A.B. v. Canada*, CCPR/C/117/D/2387/2014 (16 March 2017), para. 8.7; *Deepan Budlakoti v. Canada*, CCPR/C/122/D/2264/2013 (HRC, 29 August 2018), para. 9.6 and *B.D.K. v. Canada*, CCPR/C/125/D/3041/2017 (HRC, 6 June 2019), para. 7.8.

[54] See, for instance, the *Concluding observations on the sixth periodic report of Italy*, CCPR/C/ITA/CO/6, 1 May 2017, para. 37; the *Concluding observations on the fourth periodic report of the United States of America*, *op. cit.*, para. 24(a), and the *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland*, *op. cit.*, para. 24(a).

Against this background, certain considerations can be explored concerning the *ex ante* judicial authorization mechanisms in the context of digital SSMs. The application of the non-arbitrariness test in this context may reveal interesting insights.

For instance, the *burden of proof* required for the issuance of digital SSMs should not be excessively low – this is in accordance with the principle of necessity. For a measure to be deemed necessary for the purpose of crime prosecution, it implies that its use should be the sole means by which such objective can be attained. In practical terms, this would entail that digital SSMs should not be authorized solely based on a "mere suspicion" that an individual is allegedly involved in criminal activities using a digital tool. Rather, additional circumstances (e.g., other pieces of evidence) should exist for this purpose. Otherwise, the measure risks being not only unnecessary but also disproportionate, given the huge amount of data contained in the electronic device at stake.

Besides, digital SSMs can be considered free from arbitrariness when their *duration* is not indefinite but is tailored within certain limits. In this context, there is uncertainty regarding whether specific formulas (e.g., "the measure is authorized as long as it is necessary") can align with the non-arbitrariness requirement outlined in Article 17 ICCPR.[55] While it may be true that establishing an exact *ex ante* time limit could be challenging, it would be a good practice for courts to periodically review their authorizations to extend or, if necessary, terminate the measures in question. Besides, it should be acknowledged in domestic frameworks that once an IT tool has been searched and seized, it should be immediately returned to the owner, even by order of the court on its own motion.

[55] See, for instance, Article 262(1) of the Italian Code of Criminal Procedure ("*When it is not necessary to maintain the seizure for evidentiary purposes*, the seized items are returned to the rightful owner, even before the judgment", emphasis added). Accordingly, this leaves the decision to lift the seizure entirely in the hands of the public prosecutor.

Lastly, as for *the material competence of courts*, it is evident that they should hold the capability to scrutinize all materials related to the case. Domestic legislations that hinder the court from conducting a comprehensive, case-by-case examination of the circumstances ought to be deemed incompatible with Article 17 ICCPR. In essence, the prior assessment should be fair and thorough and not merely formalistic – in a word, it shall not constitute "an exercise in rubber-stamping".[56] The issue of bureaucratization of judicial prior authorization mechanisms should not be underestimated. As has been observed, "there is evidence that in some jurisdictions the degree and effectiveness of such scrutiny has been circumscribed by judicial deference to the executive".[57] Yet, for any *effective* arbitrariness assessment, judicial authorities must be empowered to adjudicate on *all pertinent matters of fact and law* to ascertain whether the request for an infringement of the right to privacy is justified *in casu*. This necessitates an in-depth examination of the specific factual circumstances of each individual case. Moreover, in my personal understanding, the authority must have the ability to consider, even *ex officio*, any other relevant element for its decision if *it deems it necessary*. Therefore, the powers of the judicial authority should not, under any circumstances, be restricted solely to the matters presented by the requesting administrative/criminal authority. To hold otherwise would be tantamount to undermining the substantive nature of the prior judicial assessment that is required as per Article 17 ICCPR.

---

[56] This is the expression adopted in the *The Right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights*, *op. cit.*, para. 38.

[57] See the *Report on the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/69/397, 23 September 2014, para. 46.

III. Shades and Lights—Delving into the European Legal Framework

At the regional level, both the EU and the ECHR legal frameworks has dealt with the digital SSMs. However, deep divergencies among the two legal systems can be noted.

A) The Shades—The Lack of a Comprehensive EU Discipline

Despite the importance of the matter, no piece of EU legislation explicitly addresses the *grounds and modalities* for ordering and executing searches and seizures of digital tools. Notably, the former measure is not even mentioned in EU law, while seizures (encompassed in the broader category of "freezing orders") have been regulated, but only to a limited extent.[58] To put it simpler, only freezing orders *with the purpose of confiscation* are regulated within the EU legal framework – frozen property (e.g., an electronic device) is deemed relevant not because of its content or its informative role as evidence, but rather because of *its economic value*. Conversely, the regulation of freezing orders for the purpose of preserving evidence (dubbed as "evidentiary" or "probatory" seizures), has been left within the procedural autonomy of Member States.

Freezing orders, when intended for subsequent confiscation, has been deemed the most effective answer to the exploitation of the free movement of goods, services, and individuals that criminal organizations carry out across the EU, which facilitates their illicit activities and poses a significant threat to regional security and stability.[59] In a nutshell, the application of freezing orders,

[58] I have already dealt with this issue in Bernardini L. and Sanvitale, F., *op. cit.*, pp. 74-78.

[59] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Com-

along with subsequent confiscation measures, is considered a viable approach to disrupt the activities of criminal organizations by impeding their access to and use of assets. Moreover, it serves as a deterrent to potential criminal actors, as the prospect of losing assets acts as a disincentive for engaging in illicit activities.

In the context of addressing criminal activities within the EU, there has been an increasing focus on establishing a regulatory framework for freezing orders with the intent of subsequent confiscation. Over the past decade, the EU has devoted attention to this aspect, particularly in the realm of targeting illegal assets. The legislative emphasis has been evident in Directive 2014/42/EU, which set out minimum rules governing confiscation and freezing orders in criminal matters.[60] The primary objective of this Directive was to address the necessity of targeting the assets of criminal organizations. This entails the seizure or freezing of items, including electronic ones, considered as "instrumentalities" or "proceeds" of specific criminal offenses. The Directive reflects an economic-oriented approach, aligning with the goal of identifying, confiscating, and repurposing criminal assets. Consequently, the EU legal framework provides comprehensive regulation specifically for freezing orders designed for confiscation purposes.

From a substantive perspective, there is no distinction between the implementation of "evidentiary" or confiscation-related seizures, both involving a temporary prohibition on certain actions related to the property in question. Electronic devices may be subject to both measures, with the differentiating factor being the intended purpose: either securing evidence or preventing the dissipation of property. Specific rules within the EU framework address only the latter scenario. Accordingly, "Directive 2014/42

mittee of the Regions *on the EU Strategy to tackle Organised Crime 2021-2025* (COM(2021) 170 final), 14 April 2021.

[60] See the Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 *on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union* [OJ L 127, 29.4.2014, p. 39-50].

proves to be useless for the purpose of understanding how, and to what extent, EU law might regulate seizures/freezing orders affecting electronic devices and based on evidence-related needs".[61]

B) The Lights—Deconstructing the Florid ECtHR's Case-law on SSMs

Within the ECHR's legal framework, Article 8 of the Convention serves as the normative cornerstone that safeguards the right to privacy. Distinct from Article 17 ICCPR, the former provision acknowledged the right to privacy but proceeds to outline specific grounds in which this right may be restricted. These circumstances involve instances where the alleged interference is "is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

According to the established ECtHR's case-law, a four-fold test is applied to evaluate the compatibility of a measure with Article 8 ECHR. Firstly, as a preliminary step, the ECtHR assesses whether the measure in question constitutes an "interference" within the meaning of Article 8 ECHR. Once this assessment positively carried out, the ECtHR proceeds to examine: (i) whether there is a legal basis in domestic law for the implementation of the measure; (ii) whether the interference serves a legitimate aim (e.g., crime prevention); (iii) whether the interference is "necessary in a democratic society".[62]

---

[61] Bernardini L. and Sanvitale, F., *op. cit.*, p. 77.

[62] See the landmark *Vavřička and Others v. the Czech Republic* [Grand Chamber], App. nos. 47621/13, 3867/14, 73094/14, 19298/15, 19306/15 and 43883/15 (ECtHR, 14 January 2021), paras. 261-312 and further case-law cited therein. For a recent application of this test, see also *Vig v. Hungary*, App. no. 59648/13 (ECtHR, 14 January 2021), paras. 51-63

It is noteworthy that, in contrast to the HRC, the ECtHR has a florid body of case law on digital SSMs. The Court's decisions are grounded in its broader findings in the realm of surveillance measures employed in criminal proceedings. Before delving into the specific ECtHR case law related to SSMs, some general points should be emphasized.

Firstly, the ECtHR explicitly recognized that the existence of prior authorization is a crucial safeguard against abuse.[63]

Secondly, it established that "in principle" *judicial* authorities should be responsible for this task as they offer the highest guarantees of independence and impartiality. Still, the court did not go so far as to assert that judicial oversight is universally required, leaving room for the possibility of *independent non-judicial oversight* being compatible with Article 8 ECHR.[64]

Thirdly, with regard to wiretappings, the Court identified a violation of the right to private life in *Dumitru Popescu* due to the absence of any prior independent review of the phone tapping order issued by a public prosecutor.[65] In contrast, the Court did not find such a violation in *Roman Zakharov* and *Dragojević*, where phone tapping measures were implemented after obtaining independent authorization.[66]

Fourthly, with regard to home searches, the Court has taken a more flexible approach. While recognizing the significance of prior judicial authorization for the issuance of home search

---

[63] *Lindstrand Partners Advokatbyrå AB v. Sweden*, App. no. 18700/09 (ECtHR, 20 December 2016), para. 97.

[64] *Big Brother Watch and Others v. the United Kingdom* [Grand Chamber], App nos. 58170/13 *et al.* (ECtHR, 25 May 2021), paras. 197 and 351.

[65] *Dumitru Popescu v. Romania (No. 2)*, App. no. 71525/01 (ECtHR, 26 April 2007), paras. 72-73.

[66] See, respectively, *Roman Zakharov v. Russia* [Grand Chamber], App. no. 47143/06 (ECtHR, 4 December 2015), para. 232, and *Dragojević v. Croatia*, App. no. 68955/11 (ECtHR, 15 January 2015), para. 92.

warrants,[67] the ECtHR has found that the absence of such an authorization does not automatically constitute a violation of the Convention. In specific cases, the presence of *ex post facto* oversight on home search warrants may compensate for the lack of preventive review.[68] Yet, it has expressly stated that the failure to assess the lawfulness of the measure, both before and after its implementation, may automatically lead to a breach of Article 8 ECHR.[69]

To sum up, the ECtHR has established that independent prior authorization is a crucial factor when evaluating the lawfulness of measures infringing upon the right to private life as enshrined in Article 8 ECHR. However, it is noteworthy that such authorization: (i) may be conducted by *non-judicial* authorities as long as they meet independence standards; (ii) might not be a mandatory requirement in domestic frameworks, within the meaning of Article 8 ECHR, if an *ex post facto* assessment of the measure can be conducted, that is, after the execution of the latter.

Against this background, the ECtHR's case-law on digital SSMs aligns with the framework previously discussed. Cases such as *Wieser and Bicos*, *Robathin*, and *Posevini* can be considered consistent with the two points already articulated – in the implementation of digital SSMs, a prior independent oversight may be preferable, but its absence can be compensated for by an effective *ex post facto* assessment of the measure at hand.[70]

---

[67] *Funke v. France*, App. no. 10828/84 (ECtHR, 23 February 1993), para. 57.

[68] See, among others, *Smirnov v. Russia*, App. no. 71362/01 (ECtHR, 7 June 2007), para. 45 *in fine*.

[69] *DELTA PEKÁRNY a.s. v. the Czech Republic*, App. no. 97/11 (ECtHR, 2 October 2014), paras. 88-94.

[70] See, respectively, *Wieser and Bicos Beteiligungen GmbH v. Austria*, App. No. 74336/01 (ECtHR, 16 October 2007), *Robathin v. Austria*, App. No. 30457/06 (ECtHR, 3 July 2012), and *Posevini v. Bulgaria*, App. No. 63638/14 (ECtHR, 19 January 2017).

In this highly fragmented framework, I would emphasize some findings of *Trabajo Rueda*, a judgment from which valuable insights can be gleaned.[71] Indeed, I would consider this judgement – albeit isolated within the ECtHR's case-law – as a shareable departure from the current (fuzzy) established approach taken by the Strasbourg Court *in parte qua*.

The case concerned the circumstances in which the applicant, Mr. Trabajo Rueda, brought his computer to a technician for repair, disclosing that it was not password-protected. Upon discovering child pornography on the device, the technician informed the police, who then searched and seized the computer *without obtaining a prior judicial warrant*, citing urgency reasons. The applicant was subsequently arrested.[72] Despite the absence of a prior judicial authorization, which was allowed by domestic law in urgent cases, the applicant challenged the existence of such urgency.

The ECtHR, in finding a breach of Article 8 ECHR, established that the urgency justifying the omission of such control must exist concretely and cannot be presumed by the police. In the material case, according to the Court, the Spanish authorities failed to adequately justify the need to act without prior authorization, which could have been obtained relatively quickly. This rendered the search and seizure of the applicant's computer disproportionate *per se* and, consequently, unnecessary in a democratic society within the meaning of Article 8(2) ECHR.[73]

In developing its line of reasoning, the ECtHR emphasized the pivotal role of prior oversight, stating *en passant* that "the rule of prior judicial authorization [is] a condition required *in any event* by Article 8 of the Convention (*which mandates the issuance of a warrant by an independent body*) when an intrusion into an individual's privacy is at stake".[74] This consideration, framed as

71 *Trabajo Rueda v. Spain*, App. no. 32600/12 (ECtHR, 30 May 2017).

72 *Ibidem*, paras. 5-7.

73 *Ibidem*, paras. 45-47

74 *Ibidem*, para. 35, emphasis added.

a universal ground of Article 8 ECHR, may suggest a departure from the fragmented case-by-case approach previously employed. Here, the Court seems to advocate for a consistent application of prior independent authorization for *all intrusive measures involving electronic devices*, rejecting the traditional blurred approach in its previous case-law. Though, it stops short from acknowledging the need for a prior *judicial* authorization mechanism.

But, after all, *Trabajo Rueda* is to be applauded for two significant reasons. Firstly, it establishes a definitive standard for interpreting Article 8 ECHR and the associated procedural safeguards, providing much-needed clarity in this regard. Secondly, it enhances the protection of the right to private life, thereby reducing the potential for arbitrary violations of this fundamental prerogative.

Regrettably, subsequent rulings did not take this specific aspect of *Trabajo Rueda* into consideration. This may foster the ECtHR's ambiguous approach in this realm. In this regard, criticism is thus warranted for the equivocal path the Strasbourg Court has taken in downplaying the importance of compulsory prior independent oversight in all instances involving digital intrusive measures (e.g., SSMs) in the context of criminal proceedings.

IV. Not a Panacea, Neither a Triviality—Some Concluding Remarks

It is indisputable that technological progress has facilitated the collection, transmission, and electronic storage of personal information, allowing for easier access and analysis compared to the era when privacy laws were originally formulated.[75] In the field of searches and seizures of electronic devices, this has essentially meant allow the prosecuting authorities to access to the extraordinary volume of information that may be stored even on

[75] Serwin, A.B., "Privacy in an Interconnected World", in *GPSolo Magazine (American Bar Association)*, 2011, n. 28(4), pp. 34-38.

a home computer. This has consequently raised the likelihood that a substantial portion of the intertwined documents retrieved may have no connection to the suspected criminal activity, which initially justified the search and seizure.[76] The complexity of the framework is heightened by the *inversion* in the implementation of this measure, in contrast to physical evidence – a computer is first *seized* and then *searched*. This enables the authority to secure its physical possession even without prior knowledge of its actual content.[77]

Foremost among these strands is the need for procedural guarantees to be afforded to the individual affected by digital SSMs. Legal scholars have commonly emphasized the significance of obtaining prior authorization from an independent authority for intrusive measures. This perspective, widely reflected in both international and European standards, aims to prevent unlawful and arbitrary violations of the right to privacy by investigating authorities. While I generally support this viewpoint, I want to emphasize that the mere presence of prior independent authorization in the context of SSMs does not guarantee *per se* the subsequent implementation is non-arbitrary, especially if the oversight is merely formalistic. However, I contend that the absence of any prior independent control strongly indicates that the subsequent procedure may be tainted by unlawful or arbitrary features.

International standards, as outlined in the jurisprudence and Observations of the HRC, consistently express a robust preference for prior *judicial* oversight concerning intrusive measures affecting the right to privacy, with no exemption for SSMs. This preference is rooted in the legality requirement outlined in Article 17 ICCPR. To prevent this oversight from becoming overly bureaucratic, the concept of freedom from arbitrariness offers valuable guidance, affording the competent authority substantial authority

---

[76] Leacock, C., *op. cit.*, p. 224.

[77] Bartholomew, P., "Seize First, Search Later: The Hunt for Digital Evidence", in *Touro Law Review*, 2014, n. 30(4), pp. 1027-1052.

to scrutinize all pertinent facts in the case, avoiding, in my understanding any stereotyped approach in this field.

Conversely, the European legal framework is more fragmented. While EU law has not directly addressed this matter, the protection provided by Article 8 ECHR is extremely blurred. Firstly, it does not mandate independent authorization when implementing intrusive measures. This aspect applies to digital SSMs as well, as observed in the settled ECtHR's case-law Secondly, the absence of such authorization can be compensated for by a robust *ex post facto* review. This approach seems not being in keeping with the aforementioned international standards. I would argue that this viewpoint poses a risk to the fundamental nature of the right to privacy. Not only does Article 8 of the ECHR fail to endorse a preference for a *judicial* body to conduct prior authorization (a concern that may be acceptable as long as independent oversight is present), but it also allows State Parties to order and execute intrusive measures *without any form of prior control whatsoever*. A very single judgement rendered by the Strasbourg Court has attempted to depart from this framework, stating that an independent oversight is *always* needed as per Article 8 ECHR; still, its findings were not recalled in subsequent decisions. This would demonstrate that, at least in Europe, times are not still mature for such a change of paradigm.

In 1961, John Kaplan suggested that "in such a complex field as search and seizure, it is impossible to suggest one great principle which, if applied, would automatically lead to a perfect and rational balance between the rights of the individual to privacy and the interest of law enforcement agencies, and society itself, in discovering evidence against and apprehending criminals".[78] Perhaps, we should refrain from embarking on such a formidable endeavor, as it might prove to be challenging, time-consuming, and ultimately pointless. On the contrary, attention should be directed towards

[78] Kaplan, J., "Search and Seizure: A No-Man's Land in the Criminal Law", in *California Law Review*, 1961, n. 49(3), p. 503.

DOI: http://doi.org/10.22201/fder.24488933e.2023.287.86913

procedural guarantees that could enhance the legality, reduce arbitrariness, and increase fairness in the implementation of digital SSMs. Introducing *a priori* independent, substantial, specific, and thorough scrutiny of these measures, to be carried out by judicial bodies, might be an initial, albeit modest, stride in that direction.