Revista Ítalo-Española de Derecho Procesal
Num. 1 (2023) | pp. 73-119
Madrid, 2023
DOI: 10.37417/rivitsproc/1475
Marcial Pons Ediciones Jurídicas y Sociales

ISSN: 2605-5244
Recibido: 04/05/2023 | Aceptado: 20/06/2023

SEARCHES AND SEIZURES OF ELECTRONIC DEVICES IN EUROPEAN CRIMINAL PROCEEDINGS: A NEW PATTERN FOR INDEPENDENT REVIEW?*

Lorenzo Bernardini**
Francesco Sanvitale***

ABSTRACT: There is a lack of comprehensive EU discipline in the area of digital search and seizure. Accordingly, the Authors will explore the scope and content of Article 8 ECHR in order to identify the minimum standards that it entails, with regard to the need for both prior and *ex post* independent oversight, should a digital search and seizure be ordered by the prosecution authorities. Against this background, the Italian legal framework will be used as a benchmark to determine the extent to which the aforementioned guarantees are safeguarded and the impact that the relevant ECtHR's case-law could have at the domestic level.

KEYWORDS: Search and seizures; Electronic devices; Article 8 ECHR; Independent oversight; Data retention

* The present paper is the result of a joint research carried out by both Authors. However, §§ 1 and 3 have been written by Lorenzo Bernardini, while §§ 2 and 4 have been written by Francesco Sanvitale. The Authors shared the writing of § 5.

** Postdoctoral Researcher in Criminal Law (Faculté de Droit, d'Économie et de Finance – FDEF), University of Luxembourg/LU. Email: *lorenzo.bernardini@uni.lu* (ORCID: 0000-0002-9768-7579).

*** Ph.D. in Criminal Procedure (Department of Legal and Human Sciences – DISTU), University of Tuscia/IT. Email: *francesco.sanvitale@unitus.it* (ORCID: 0009-0009-1369-3778).

1. THE PLAYGROUND OF THE ANALYSIS: THE LACK OF AN EU DISCIPLINE ON SEARCHES AND SEIZURES OF ELECTRONIC DEVICES

The utilization of electronic devices has become ubiquitous in contemporary society, and their importance as sources of evidence in criminal proceedings cannot be overstated. In order to ensure the preservation of relevant digital evidence during the investigations, European criminal justice systems have customarily employed searches and seizures measures, which allow the competent authorities to temporarily seize such items, preventing the owner of the electronic device from altering, transferring, converting or deleting any data contained therein. These orders thus serve as an indispensable tool for securing digital evidence and ensuring that it remains intact during the preliminary investigations and, eventually, the trial.

In other words, searches and seizures of electronic devices are issued almost always for evidence-related issues. Ordinarily, national authorities implement them in the context of investigations into serious criminal offences such as fraud, money laundering, and cybercrime, among others. Yet, searching and seizing of these items could conceivably occur should investigations for other crimes be carried out (e.g., manslaughter, robbery or drug trafficking), given their widespread employment in everyday life and hence their helpfulness for criminal justice authorities. In any case, searches and seizures measures play a crucial role in ensuring the preservation of digital evidence by guaranteeing that the integrity of the electronic device's content is maintained. Currently, almost every criminal investigation is faced with the necessity to access electronic data, for the purpose of reconstructing the procedural truth.

It is important to understand that the technological development brought unexpected changes to criminal proceedings, specifically as regards digital evidence and all the procedures related thereof. As has been interestingly observed:

> 'Computer searches … are much different from ordinary searches for physical evidence due to the complexity of information stored within a computer or hard drive as well as the technical expertise required to retrieve such evidence. Often times, the police seize a suspect's computer and take it to a police laboratory for extensive examination by forensics experts. These forensic examinations may take days, months, or even years'[1].

[1] Bartholomew (2014), p. 1027.

Against this background, it shall be taken into account that the exponential growth in the usage of electronic tools has led to an unprecedented amount of personal data being generated, stored, and transmitted on a daily basis, thereby giving rise to several privacy and security concerns. This is especially so in the realm of criminal proceedings, should the contents of electronic devices constitute the focus of investigation. It is thus crucial to consider that the implementation of searches and seizures of electronic devices in criminal proceedings must be in balance with the protection of the individual's right to privacy. While the preservation of personal data proves to be essential, it is equally imperative that the use of such measures does not result in an unjustifiable infringement of the right to private life.

Despite the significance of the matter, as will be explained, no EU piece of legislation deals *explicitly* with the grounds and modalities of searches and seizures of IT 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 solely to a limited extent.

Indeed, beside traditional kinds of freezing orders, which may be labelled as 'evidentiary' or 'probatory' ones, another cluster of measures have progressively been employed by the criminal authorities, that is, the freezing orders with the purpose of confiscation (i.e. 'economic seizures'). In this instance, frozen property—even an electronic device—is deemed relevant not because of its *content* or its *informative attitude* as 'evidence', but rather because of its *economic value*.

The purpose of seizures/freezing orders in view of subsequent confiscation is based on the fact that criminal organizations take advantage of free movement of goods, services and individuals within the EU to carry out their nefarious activities with relative ease, and as such, pose a significant threat to the security and stability of the region[2]. These organizations, because of their complex and sophisticated structures, pose a formidable challenge to national law enforcement agencies in their efforts to disrupt and dismantle them. One approach that has proven effective in combating these organizations is the targeting of their financial assets, which are vital to their continued operation and sustained success[3]. Freezing orders, along with subsequent confiscation measures, may constitute an efficacious strategy in disrupting the activities of criminal organizations. By preventing these organizations from accessing and using their assets, they are impeded in their ability to continue their criminal endeavours. Furthermore, the implementation of freezing orders serves as a deterrent to potential criminal actors, as the hypothetical loss of assets serves as a disincentive for engaging in illicit activities.

---

[2] See, in this regard, the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025 (COM(2021) 170 final), 14 April 2021.

[3] Cfr. the Europol report *Out of their hands: Europol and asset recovery*, 13 March 2023 (*https://www.europol.europa.eu/media-press/newsroom/news/out-of-their-hands-europol-and-asset-recovery*).

It is in this context that the EU has begun to reflect on the opportunity to build up a regulatory system in this respect[4]. Accordingly, in the last decade, the attention paid by the EU to freezing orders for the purpose of confiscation has increased. Notably, only the perspective of targeting illegal assets has been considered by the EU legislature when regulating criminal seizures/freezing orders. This is apparent from the wording of Directive 2014/42/EU[5], whose purpose was to lay down minimum rules related to confiscation and freezing orders in criminal matters.

The aim of the aforementioned Directive was thus based on the necessity to target the assets of criminal organizations. In other words, the objects of seizures/freezing orders and confiscation measures are those items—including electronic ones[6]—deemed to constitute 'instrumentalities' or 'proceeds' of certain criminal offences[7]. The Directive has therefore espoused an economics-driven approach, linked to the need to identify, confiscate and reuse criminal assets[8]. Accordingly, merely freezing orders for the purpose of confiscation have received a comprehensive regulation within the EU legal framework.

From a material standpoint, no distinction may be drawn between the *implementation* of 'evidentiary' or 'economic' seizures—both imply a provisional ban on certain behaviours related to the property at stake (e.g., its disposal or destruction), leading to the temporary control or custody of such assets by the competent authority (e.g., the public prosecutor, or the investigating judge)[9]. Furthermore, both measures can affect electronic devices. What makes the difference here is the *purpose* of the measure at stake: either to secure evidence or to prevent the dissipation of property. It is only in the latter case that the EU has laid down specific rules.

---

[4] For the sake of completeness, it is noteworthy that, since 2001, the EU adopted several provisions addressing the issue of seizures/freezing orders in criminal proceedings. *Inter alia*, it is worth recalling Framework Decisions 2001/500/JHA on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime [OJ L 182, 5.7.2001, p. 1-2] and 2005/212/JHA on Confiscation of Crime-Related Proceeds, Instrumentalities and Property [OJ L 68, 15.3.2005, p. 49-51]. It is clear that the action taken by the EU legislature was driven by an economics-based approach.

[5] 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].

[6] It is no surprise that one could think that also electronic devices may be embodied within such definition, as they have a rather high economic value and are oftentimes either an instrumentality or proceeds of a criminal offence. An electronic tool, e.g., a smartphone or a laptop, could be employed in order to commit several of the offences listed in Article 3 of Directive 2014/42. Such a circumstance leads to the assumption that those devices could be labelled as 'instrumentalities' as per Article 2(3) of the Directive, that is, any property 'used or intended to be used, in any manner' for the aforementioned purpose. Analogously, they could also constitute 'proceeds' of the crime of money laundering or drug trafficking, should those tools be bought with money derived from the latter.

[7] See Article 2(2), Directive 2014/42/EU.

[8] The latter aimed to approximate domestic legislations facilitating mutual trust among the Member States, establishing minimum rules concerning the definition of sanctions in the areas of particularly serious crime with a cross-border dimension for the crimes listed in Article 83(1) TFEU.

[9] See Article 2(5), Directive 2014/42/EU.

At the same time, the Directive aiming at defining minimum rules, there shall be no prejudice to the possibility, up to the Member States, to provide 'more extensive powers in their national law, including … in relation to their rules of evidence'[10]. The EU legislature was indeed conscious that not only 'property' does have a relevance for its monetary value, but it also proves to be essential as *evidence* throughout criminal proceedings. As long as confiscation measures will not eventually be hindered, 'property' can be employed as evidence[11]. This holds true *also*—and especially—with regard to electronic devices, as the data they contain may be profoundly relevant in order to carry out wide-ranging and effective investigations. Hence, such items might be frozen with a view to subsequent confiscation but, in the meanwhile, may be used as evidence due to their content, provided that such an operation should not hamper the subsequent confiscation measure. Against this backdrop, it can be inferred that the Directive 2014/42 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*.

More correctly, nonetheless, one could focus on the very issue triggered by this matter, namely, the huge amount of data that are contained inside IT tools and, in the last instance, the interference with the fundamental rights to privacy and the protection of personal data of the individuals concerned. Indeed, breaches of these fundamental rights may produce significant outcomes (e.g., a serious damage to reputation; the disclosure of high-sensitive information concerning medical treatments or sexual orientation; the dissemination of bank accounts credentials; a breach of confidentiality which should cover certain conversations, for instance, among lawyers and their clients). Accordingly, to seize laptops or smartphones could be problematic not due to their economic value, but rather frequently because of the massive amount of personal data enclosed therein (serving as *digital evidence*) and which, as a matter of fact, might relate also to individuals other than the device's possessor.

Against this background, one cannot but acknowledge that the widespread employment of new forms of communication reshaped the attitude through which personal data are looked at (and consequently retained) by individuals. Such a phenomenon may have a significant influence *vis-à-vis* the whole structure of criminal proceedings[12]. In carrying out their activities, national authorities may become aware of a huge amount of data. Historically, personal information concerning a suspect might have been obtained *inter alia* through witnesses, phone tapping and material evidence (e.g., tax documents). Nowadays, things have profoundly changed. To take a concrete example, smartphones and personal computers have become the strongbox in which individuals collect personal information, the latter belonging not

[10] Recital 22, Directive 2014/42/EU.

[11] Recital 28, Directive 2014/42/EU.

[12] There has been a 'change of paradigm that technological progress has generated in this area of law', according to Bachmaier Winter (2022), p. 4.

only to the latter but also to third parties. Their employment as helpful means in the context of criminal investigations is thus not at issue.

Foremost among the aforementioned topics is the issue of *procedural guarantees* to be ensured to the individual concerned—being the latter either the suspect/accused person or a third party—in the face of the huge power which oftentimes is retained by prosecuting authorities in searching and seizing electronic devices.

In this regard, our analysis will focus on the Italian domestic framework –specific provisions of the Italian Code of Criminal Procedure (hereinafter: 'CCP') provides the public prosecutor with the power to search and seize IT tools without any prior or *ex post facto* judicial oversight. As will be explained, that lack of any control on the public prosecutor's activities might be problematic in light of the fundamental right to private life and correspondence, acknowledged both by the European Convention on Human Rights (hereinafter: 'ECHR'), as interpreted by the European Court of Human Rights (hereinafter: 'ECtHR'), and by the EU Charter of Fundamental Rights (hereinafter: 'the Charter'), as interpreted by the Court of Justice of the European Union (hereinafter: 'CJEU'). Such circumstance may serve as a benchmark for assessing the degree of guarantees which shall be in place avoid any arbitrary infringement of those prerogatives.

Accordingly, a brief analysis of the Italian legal framework will be depicted (§ 2). Subsequently, the settled ECtHR's case-law on digital searches and seizures will be scrutinised, in order to set the minimum standard of procedural prerogatives (i.e., the existence of an independent oversight) that stem thereof and its impact on the Italian legal framework (§§ 3-4). Conclusively, final remarks will be developed with some proposals *de iure condendo*, in the light of the unceasing cross-fertilisation between the two European legal frameworks (§ 5).

2. BALANCING POWERS WHEN IMPLEMENTING DIGITAL SEARCHES AND SEIZURES: OLD AND NEW CHALLENGES IN THE ITALIAN CRIMINAL JUSTICE SYSTEM

The Law No. 48/2008, which transposed in Italy the Council of Europe Convention on Cybercrime, the so-called 'Budapest Convention'[13], has chosen to regulate investigative operations aimed at obtaining and using electronic data in criminal proceedings, in the context of inspections, searches and seizures[14], through specific amendments of the Code of Criminal Procedure[15].

---

[13] Cfr. the Convention on Cybercrime of the Council of Europe, done on 23 November 2001 (*https://rm.coe.int/1680081561*).

[14] An analogous choice has been made by many other EU Member States. See Bartoli, Lasagni (2021).

[*Nota 15 en página siguiente*]

The admissibility of digital evidence in criminal proceedings has challenged the doctrinal boundaries and relationships between 'inspections', 'searches' and 'seizures'[16]. Faced with an electronic device, it is legitimate to question, for example, whether the opening of a folder should be classified as an 'inspection' or a 'search', or whether the seizure should be deemed to pertain to the device containing the electronic data or to the data themselves. However, there is at least one feature which is common to the three aforementioned measures—they can be ordered and executed by the public prosecutor without the need for any sort of (independent) authorisation. In other words, whether the search or a seizure of an IT tool is needed, Italian public prosecutors can act *motu proprio*. This circumstance, as will be seen, plays a pivotal role in emphasising the inadequacy of the Italian criminal justice system in protecting the (fundamental) right to private life and correspondence.

In any case, different procedural rules apply depending on the legal qualification of the act. In particular, the available legal remedies differ: for instance, an effective judicial review (*riesame*) is available solely to challenge the seizure warrant (Article 257 CCP). Hence, there is still some merit in trying to sketch the boundaries among the aforementioned measures.

In doctrinal circles, it has been argued that should the activity at stake consist solely in the mere *observation* of the device or of what it contains at the time of its finding, such activity may constitute an 'inspection'. If searches are conducted, even just by opening a file or folder, then such activity should be classified as a 'search'[17]. Should files be copied using specific devices (e.g., a USB pen drive) or techniques (e.g., the 'bit stream image'), a 'seizure' of the files is carried out. This is the solution suggested by the Italian Court of Cassation, that distinguishes between the 'seizure' of the file itself and the device that contains it: when, for instance, a personal computer is seized, not only the device is considered to be the object of the seizure warrant, but also any file that has been copied and retained[18].

In particular, 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[19]. As

---

[15] About searches and seizures, see Braghò (2019). Specifically on seizures, see Monti (2019). With regard to Article 354(2) CCP, concerning urgent checks of the *locus commissi delicti*, objects and persons and in particular on the preservation of the electronic data acquired in that context, see Lorenzetto (2019).

[16] In a nutshell, 'inspections' aim at ascertaining traces or other material effects of the offence on persons, in places or things (Articles 244-246 CCP); 'searches' consist in the examination of a person's body, property or other area which the person would reasonably be expected to consider as private by a law enforcement officer for the purpose of gathering evidence (Articles 247-252a CCP); finally, 'seizures' consist in the act of taking property, including cash, real estate, vehicles, *etc.*, that has been used in connection with or acquired through illegal activities (Articles 253-263 CCP).

[17] Cuomo (2022), pp. 631-632.

[18] Court of Cassation, Joint Chambers, 20 July 2017, No. 40963, Andreucci, ECLI:IT:CASS:2017:40963PEN, paras. 8-13.

[19] See Cascone (2022), p. 134 and Torre (2019), pp. 1433-1437. Additionally, see Felicioni (2019).

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[20].

As one can easily understand, the right to private life may be under threat should digital investigations be carried out by the prosecuting authorities. As already said, these investigations can potentially reveal an unlimited amount of information, far beyond what is feasible through 'traditional' inspections, searches and seizures[21]. In this regard, it is evident that the right to private life is breached, for instance, where the creation of a forensic copy of a certain device is implemented by prosecuting authorities.

Against this background, the Decree-Law No. 132/2021 provides for the need for a judicial authorisation should the prosecutor aim at acquiring digital data collected by internet service providers[22]. Thus, one may question the appropriateness of the Italian prosecutors' power to issue searches and seizures warrants *motu proprio* for the purpose of gathering evidence, without a prior judicial authorisation. Indeed, there is no doubt that, through the aforementioned measures, the same data collected by Internet service providers can be obtained[23].

The issue becomes even more problematic when one considers the increasing practices of investigative authorities to store data in data banks for extremely long periods time, as those activities are not governed by strict rules protecting the secrecy of the data contained therein[24].

On the matter, the Italian Court of Cassation established that, as a general rule, a seizure of all the data stored in a certain digital device, without any prior selection, is not admissible[25]. Otherwise, there is a risk of nebulous and wide seizures, adopted to fasten investigation without a proper justification and reference to a specific crime.

The Court of Cassation also dealt with another interesting feature—the existence of an effective remedy through which the individual concerned may challenge the seizure warrant, eventually asking for the latter's review. According to previous jurisprudence, once the device has been returned to its

---

[20] See the Interpol *Guidelines for digital forensics first responders. Best practices for search and seizure of electronic and digital evidence*, March 2021. In this regard, see Bartoli (2018), p. 16; Lorenzetto (2019), pp. 153-154; Ziccardi (2019), pp. 165-177.

[21] 'Inspections', 'searches' and 'seizures' related to physical evidence, and thus other that digital data, affect primarily the rights to domicile, personal liberty or property.

[22] Article 132 Legislative Decree No. 196/2003, i.e., Privacy Code.

[23] Chelo (2022).

[24] In this regard, it is worth mentioning a document issued by the Public Prosecutor's Office of Trento ('*Nota d'indirizzo organizzativo*', 22 October 2021), which highlights the lack of clarity of the provisions and the questionable practices of the investigative bodies.

[25] Court of Cassation, 24 February 2015, No. 24617, ECLI:IT:CASS:2015:24617PEN. Additionally, see, among others, Court of Cassation, 28 September 2021, No. 38460, ECLI:IT:CASS:2021:38460PEN; Court of Cassation, 5 July 2021, No. 32761, ECLI:IT:CASS:2021:32761PEN; Court of Cassation, 9 December 2020, No. 6623, ECLI:IT:CASS:2021:6623PEN.

owner, that person should no longer have access to the judicial remedy, since his/her right to property had been restored[26].

Nevertheless, recent case-law has overruled this approach. Particularly, the Italian Court of Cassation has set forth that the interest in challenging a seizure warrant is not diminished should the files extracted from the (already) returned device be *still in the possession of the investigative authorities*, as there is a material and current interest in the exclusive availability of the data[27].

Finally, the lack of a remedy in the case of a search without subsequent seizure was another issue. The ECtHR found that the Italian legislation was not in keeping with Article 8 ECHR[28] and, accordingly, a change in the domestic legal framework was clearly needed. To this end, the Legislative Decree No. 150/2022 (the so-called 'Cartabia reform') introduced a specific provision within the CCP (i.e., Article 252a CCP), which provides the individual concerned with a new remedy, specifically devoted to challenging the search warrant issued by the public prosecutor in the event that no subsequent seizure has taken place[29].

It is likely that the ECtHR will trigger further changes in the near future, as it seeks to circumscribe the boundaries of digital investigations, alongside their world-wide spreading. The broad scope of application of Article 8 ECHR makes it a perfect and flexible paradigm to encompass any violation of the digital environment by public authorities. The following paragraphs will analyse the judicial oversight paradigm in the field of digital searches and seizures that stems from the ECtHR's case-law.

3. SEARCHES AND SEIZURES OF ELECTRONIC DEVICES AND *EX ANTE* INDEPENDENT CONTROL. THE NEED FOR A NEW STANDPOINT

In this Section, it will be advocated that searches and seizures of electronic devices should *solely* be carried out once a prior authorisation, rendered by an independent body, has been granted (i.e., 'independent review'). While this practice does not appear to be widespread across the EU[30], it appears none-

---

[26] Court of Cassation, Joint Chambers, 24 April 2008, No. 18253, Tchmil, ECLI:IT:CASS:2008:18253PEN.

[27] Court of Cassation, Joint Chambers, No. 40963/2017, supra note 18, paras. 19-21. Beforehand, the same principle was established by Court of Cassation, No. 24617/2015, supra note 25, paras. 7-7.3. More recently, see Court of Cassation, 3 February 2022, No. 18502, ECLI:IT:CASS:2022:18502PEN, paras. 2.1-2.2.

[28] *Brazzi v. Italy*, App. No. 57278/11 (ECtHR, 27 September 2018), ECLI:CE:ECHR:2018:0927JUD005727811.

[29] The same Legislative Decree No. 150/2022 laid down an equivalent remedy in Article 352(4a) CPP, in case the search was conducted directly by the police.

[30] We have already dealt with the Italian legal framework. It is also noteworthy that in the Spanish legal system, seizures for evidence-related purposes are deemed to be measures that do not affect

theless that the need for a preventive oversight—albeit not being an absolute requirement of Article 8 ECHR—is embodied within the relevant ECtHR's case-law on the right to private and family life.

For the purpose of depicting these findings, it will first be necessary to glance *whether* and *to what extent* the abovementioned rights are ensured within the ECHR legal framework. Emphasis will be put upon the scope and the content of Article 8 ECHR (§ 3.1). Against this background, it will be explained that the ECtHR has dealt on several occasions with the issue of surveillance measures in the context of criminal proceedings—the relevant case-law may provide insightful guidance which help in carving out the significance of a prior independent oversight stemming from Article 8 ECHR (§ 3.1.1). What is more, the Strasbourg Court gave illustrious examples which foster the idea that an *ex ante* independent oversight is of paramount importance in order to avoid arbitrary action by public authorities when carrying out searches and seizures of IT devices (§ 3.1.2). An additional paragraph will provide a concise portrayal of the main advantages that may be seen in this line of reasoning, delving into any unresolved questions that may persist (§ 3.2).

3.1. 'You shall not pass'. Avoiding Arbitrariness Through Prior Oversight: Searches and Seizures of Electronic Devices Before the ECtHR

Whereby searches and seizures of electronic devices in the context of criminal proceedings may raise several and different fundamental rights issues, the modest aim of this Section will focus on the right to private life and correspondence, to which every individual is entitled under Article 8 ECHR. We will focus, in particular, on the '*protection classique*' acknowledged by the Convention with regard to the intimate personal relations, which shall be safeguarded from any sort of external interference[31].

Aside from a first, absolute, acknowledgement of this prerogative[32], the wording of Article 8 ECHR reveals that the latter may be restricted should specific grounds be met in the material case[33]. It is worth recalling that, as

---

fundamental rights, and therefore do not require a prior judicial authorisation to be carried out by the police or the public prosecutor. See De Lucchi López-Tapia, Jiménez López (2022), p. 172. In Germany, under Article 98 *Strafprozeßordnung* (StPO), while freezing orders are normally to be ordered by a court, the public prosecutor or the police may also execute *motu proprio* a seizure 'in urgent circumstances'. In this latter case, judicial review is still automatically ensured *ex post facto*, within three days, but solely in certain cases (e.g., the individual concerned was not present during the operations or an objection against the seizure has been lodged). Finally, it is worth recalling the Belgian domestic framework—the public prosecutor may autonomously seize objects for a wide range of evidentiary purposes, in particular '*de tout ce qui pourra servir à la manifestation de la vérité*' (see Articles 35 and 28a(3) *Code d'Instruction Criminelle*).

[31] See Renucci (2021), p. 279, with further references cited therein.

[32] Article 8(1) ECHR.

[33] Greere (2006), p. 257.

a preliminary question, the ECtHR shall assess whether the measure under scrutiny constitutes an 'interference' as per Article 8 ECHR[34]. Where such assessment has been positively fulfilled, the ECtHR will examine: (i) whether there is a legal basis in domestic law for the implementation of the measure at stake[35]; (ii) whether the interference is necessary in a democratic society[36]; (iii) whether the interference furthers a legitimate aim (e.g., the prevention of crime)[37].

As has been reiterated by the ECtHR, the purpose of this threefold test is to protect individuals from arbitrary interference with their private life[38]. Although cited very frequently in the ECtHR's case-law on Article 8 ECHR, it is noteworthy that there is no consensus among legal theory scholars on the content of the notion of 'arbitrariness'[39]. While it is not the purpose of this essay to explore such issue, it is important to circumscribe the notion of 'arbitrariness', the avoidance of which is the very aim of the establishment of independent review mechanisms. To break through this deadlock, it could be argued that such a notion encompasses both illegal conducts and those behaviours which are characterised by elements of inappropriateness or injustice[40]. Accordingly, those interferences implemented against individuals that are neither necessary nor proportionate nor reasonable in the material case may be deemed arbitrary, albeit implemented in accordance with domestic law provisions[41]. This line of reasoning, which stems directly from international law, is in keeping with the relevant ECtHR's case-law, which notably tends to discern 'unlawful' conducts from 'arbitrary' ones[42].

That being said, it is apparent that the scope of Article 8 ECHR relies on to the need to avoid haphazard behaviours by public authorities in very sensitive areas, such as those relating to private life and communications—for what is relevant here, such a provision acknowledges a *negative* prerogative, a sort of 'right to be left alone'[43].

---

[34] See, for instance, *Vinci Construction and GTM Génie Civil et Services v. France*, App. Nos. 63629/10 and 60567/10 (ECtHR, 2 April 2015), ECLI:CE:ECHR:2015:0402JUD006362910, para 63 and, more recently, *Särgava v. Estonia*, App. No. 698/19 (ECtHR, 16 November 2021), ECLI:CE:ECHR:2021:-1116JUD000069819, para 85.

[35] Amongst other authorities, see *Modestou v. Greece*, App. No. 51693/13 (ECtHR, 16 March 2017), ECLI:CE:ECHR:2017:0316JUD005169313, paras. 30-38.

[36] See, for instance, *Naumenko and SIA Rix Shipping v. Latvia*, App. No. 50805/14 (ECtHR, 23 June 2022), ECLI:CE:ECHR:2022:0623JUD005080514, paras. 50-63.

[37] See *inter alia Adomaitis v. Lithuania*, App. No. 14833/18 (ECtHR, 18 January 2022), ECLI:CE:ECHR:2022:0118JUD001483318, para 84.

[38] *P. and S. v. Poland*, App. No. 57375/08 (ECtHR, 30 October 2012), ECLI:CE:ECHR:2012:-1030JUD005737508, para 94.

[39] See *inter alia* Harnold, Harris (2017), pp. 55-70 and Valentini (2017), pp. 817-832.

[40] See the HRC report *CCPR General Comment No. 16: Article 17 (Right to Privacy)*, 8 April 1998, para 4.

[41] See the HRC report *The right to privacy in the digital age*, A/HRC/27/37, 30 June 2014, paras. 21-27.

[42] See, in this regard, *Mozer v. the Republic of Moldova and Russia*, App. No. 11138/10 (ECtHR, 23 February 2016), ECLI:CE:ECHR:2016:0223JUD001113810, para 196.

[43] Schabas (2015), p. 366.

Among other guarantees, such aim is customarily pursued—albeit not exclusively—by the establishment of independent control mechanisms over the State's activities. In every branch of law, indeed, it is a settled belief that government actions 'that deviate from their legal authority, whether accidentally or deliberately, may not be permitted'[44]. For this to happen, public authorities should be aware that their behaviour may be subject to scrutiny by another 'power' (*pouvoir*), according to the old-fashioned Montesquieu's standpoint, which is deemed to possess a certain degree of independence and impartiality[45]. While such an assessment may take place either *before* or *after* the act at stake, traditional doctrine focused on the pre-eminent role of prior independent review as the most effective tool to prevent arbitrariness.

In the context of criminal proceedings, this line of reasoning is of pivotal importance under several aspects. Markedly, suspects and accused persons may be subjected to coercive measures during the investigation phase, and it would be arbitrary not to have a *prior* check on the lawfulness of the latter. Pre-trial detention or house arrest may be examples of legal tools that should be authorised *ex ante* by an independent body, for the sake of ensuring that the action of public authorities is provided for by law, is necessary in the material case and is proportionate to the aim pursued. It is noteworthy that, when it comes to the right to personal liberty, domestic legislations proved to be very cautious in granting the investigating authorities the autonomous power to restrict this right without a proper, anticipated control, which is ultimately assigned to the judicial authority.

While prior independent review mechanisms have been progressively entrenched in contemporary criminal justice systems, there is nonetheless a lack of understanding as to whether such review is *also* required when interests other than the right to personal liberty are jeopardised. To come back to private life and correspondence, it might be debatable whether such prior protection should *always* be afforded where the abovementioned prerogatives are threatened, e.g., during preliminary investigations.

A fairly common activity, the search and seizure of an IT device could be tantamount of gathering almost *all* personal information relating to that person and, oftentimes, to third parties[46]. Accordingly, such measure could be particularly severe, even more so than other traditional means of surveillance, such as wiretappings[47]. It therefore deserves adequate guarantees, aimed at preventing prosecuting authorities from collecting such a large amount of evidence through arbitrary behaviour.

---

[44] Smith (2015), p. 215.

[45] Montesquieu (1965).

[46] See Kerr (2005), pp. 531-585 and, for a comparative perspective, Winik (1994), pp. 75-128.

[47] The data contained in an electronic device could depict a nearly complete portrait of the person under investigation. Not only photos or videos, but also the content of emails, SMS messages, traffic and location data may be inspected and retained by the investigating authorities. Conversely, wiretappings disclose solely partial, albeit relevant, pieces of information, such as the suspect's conversations at the moment they are made. A constant reference to the discipline of wiretapping, as shaped by the ECtHR, is thus of some relevance in that it could provide a benchmark for our analysis.

It is against this background that the relevance of Article 8 ECHR arises[48], acting as a solid gatekeeper for the privacy and data protection rights of the individuals involved in criminal proceedings whose electronic devices are searched and seized for the purpose of collecting evidence. Indeed, several judgements rendered by the ECtHR have addressed this issue. Here, the question that arises is the following—to what extent does Article 8 ECHR provide an acceptable level of protection for individuals when the abovementioned measures are taken by public authorities in the context of criminal proceedings? And, in particular—is the need for a prior review embodied in the protection ensured by Article 8 ECHR?

3.1.1. Minimum Guarantees in the Field of Surveillance Measures Before the ECtHR

In order to sketch the minimum ECHR standards to be applied should searches and seizures of IT devices be implemented, it is worth recalling the relevant case-law on surveillance measures in the context of criminal proceedings.

More generally, the existence of a *prior* authorisation burden on prosecution authorities composes 'an important safeguard against abuse'[49]. The Court has made it clear that the safeguards against arbitrariness include the existence of an 'effective scrutiny' of measures encroaching on Article 8 ECHR[50]. Accordingly, one of the factors typically taken into account by the ECtHR in assessing whether surveillance procedures are not ordered in an arbitrary fashion relates to the possible existence of an authority that grants such operations *a priori*. Remarkably, attention should be paid to the extent and the quality of such an assessment[51]. This evaluation is embodied within the 'third test' encompassed in Article 8 ECHR—whether a certain measure is 'necessary in a democratic society'—, given that, while national authorities hold a certain margin of discretion in assessing the need for an interference, this discretion shall go 'hand in hand with European supervision'[52].

In a famous passage of *Roman Zakharov*, the Grand Chamber underlined 'the risk that a system of secret surveillance set up to protect national security

---

[48] Although not the focus of the present analysis, it is noteworthy that searches and seizures of electronic devices have also raised issues under Article 10 ECHR, when IT tools are owned by a journalist. See, among other authorities, *Sergey Sorokin v. Russia*, App. No. 52808/09 (ECtHR, 30 August 2022), ECLI:CE:ECHR:2022:0830JUD005280809.

[49] *Kamić v. Croatia* (dec.), App. No. 37517/16 (ECtHR, 20 September 2021), ECLI:CE:ECHR:2021:-0928DEC003751716, para 23.

[50] *Lambert v. France*, App. No. 23618/94 (ECtHR, 24 August 1998), ECLI:CE:ECHR:1998:-0824JUD002361894, para 34.

[51] A mere formal assessment does not suffice for this purpose. See, for instance, *Vinci Construction*, supra note 34, para 79.

[52] *Funke v. France*, App. No. 10828/84 (ECtHR, 23 February 1993), ECLI:CE:ECHR:1993:-0225JUD001082884, para 55. Such a need shall be 'convincingly established'.

may undermine or even destroy democracy under the cloak of defending it'[53]. Although the implementation of IT searches and seizures cannot apparently be equated to bulk surveillance mechanisms, it should not be underestimated that the theoretical possibility for a public prosecutor to carry out these activities without any prior control whatsoever might lead to their haphazard employment *en masse*. Furthermore, in both cases, the domestic bodies need to act in the lack of the individual's awareness, which makes it unlikely that the suspect will have an effective remedy before the measure is issued. What is more, the access to data stored in an electronic device—if implemented without a prior assessment of its necessity and proportionality *in concreto*—might hamper the protection afforded by Article 8 ECHR, given that those activities may nowadays endanger not only the suspect's personal data but also those of third parties.

It descends that, from a practical perspective, one of the most effective means of preventing investigating bodies from arbitrarily infringing Article 8 ECHR would appear to be a prior review of the undertakings carried out by investigating authorities, *a fortiori* 'in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole'[54]. Albeit written in 1978 and referring to surveillance measures, it is apparent that this quote from *Klass* retains its relevance in relation to searches and seizures of digital devices.

As for the kind of authority competent to authorise the surveillance, the ECtHR developed a nuanced line of reasoning. 'In principle'[55], it would be a judicial authority, which provides the highest guarantees of 'independence, impartiality and a proper procedure'[56]. Yet, the Court was open to acknowledge that, should a certain body be sufficiently independent of the executive, such circumstance may not be seen incompatible, as such, with the Convention[57]. In the landmark *Big Brother Watch* judgement, the Court expressed its 'preference' for judicial review but stressed that this was not a 'necessary requirement'[58]. In a nutshell, what is relevant for the ECtHR is the high degree of independence that shall characterise the body which is ultimately charged with assessing the necessity and proportionality of the measure in question.

A rich case-law of the ECtHR addressed the need for a prior independent review in the light of Article 8 ECHR in cases of telephone tapping. In *Dumitru Popescu (No. 2)*, the Court found a breach of the abovementioned provision

---

[53] *Roman Zakharov v. Russia* [GC], App. No. 47143/06 (ECtHR, 4 December 2015), ECLI:CE:ECHR:2015:1204JUD004714306, para 232.

[54] *Klass and Others v. Germany* [Plen.], App. No. 5029/71 (ECtHR, 6 September 1978), ECLI:CE:ECHR:1978:0906JUD000502971, para 56.

[55] Ibid.

[56] Ibid., para 56 *in fine*.

[57] See, among other authorities, *Roman Zakharov*, supra note 53, para 258 and the case-law cited therein.

[58] *Big Brothers Watch and Others v. the United Kingdom* [GC], App. No. 58170/13 *et al*. (ECtHR, 25 May 2021), ECLI:CE:ECHR:2021:0525JUD005817013, paras. 197 and 351.

in that, *inter alia*, the prosecutor's authorisation to intercept communications was not subject to any *a priori* review by a judge or other independent authority, either *ex officio* or at the request of the person concerned[59]. The same line of reasoning—redolent of the well-know *Klass and Others* judgement[60]—was then adopted by the Grand Chamber in *Roman Zakharov*[61]. Notably, the ECtHR held that no breach of Article 8 ECHR may be found where phone tapping measures were implemented after a judicial authorisation assessing their necessity *in concreto*[62]. To this acknowledgement, it is worth recalling that in *Dragojevič*, the ECtHR took particular account of the existence of a robust mechanism for obtaining prior authorisation to carry out wiretappings:

> 'The domestic law thereby provides for prior authorisation of the use of secret surveillance measures which must be sufficiently thorough and capable of demonstrating that the statutory conditions for the use of secret surveillance have been met and that the use of such measures is necessary and proportionate in the given circumstances. Strictly speaking, every individual under the jurisdiction of the Croatian authorities, when relying on these provisions of the relevant domestic law, should be confident that the powers of secret surveillance will be subjected to prior judicial scrutiny and carried out only on the basis of a detailed judicial order properly stipulating the necessity and proportionality of any such measure'[63].

What is more, the judicial order on which a surveillance measure is based cannot be drafted in such nebulous terms as to leave 'room for speculation', without properly identifying the person concerned by the measure at stake[64].

Interestingly, the same held true in relation to home searches[65]. In this regard, the Court has customarily emphasised the positive obligations of the Contracting States in safeguarding the guarantees stemming from Article 8 ECHR. As already said, they must provide concrete safeguards against abusive behaviour towards the individual concerned[66]. For instance, the lack of 'any requirement of a *judicial* warrant' as a basis for the actions of customs authorities in carrying out house searches and seizures was considered an important factor to be taken into account in finding a breach of Article 8

---

[59] *Dumitru Popescu v. Romania (No. 2)*, App. No. 71525/01 (ECtHR, 26 April 2007), ECLI:CE:ECHR:2007:0426JUD007152501, paras. 72-73. Other circumstances that led the Court to find a violation of Article 8 ECHR were the lack of independence of the prosecutors and, remarkably, the lack of any *ex post* review of the legality of the intrusive measure under investigation.

[60] *Klass and Others*, supra note 54, para 55.

[61] *Roman Zakharov*, supra note 53, para 258

[62] See *İrfan Güzel c. Turquie*, App. No. 35285/08 (ECtHR, 7 May 2017), ECLI:CE:ECHR:2017:-0207JUD003528508, paras. 78-79.

[63] *Dragojević v. Croatia*, App. No. 68955/11 (ECtHR, 15 January 2015), ECLI:CE:ECHR:2015:-0115JUD006895511, para 92.

[64] *Azer Ahmadov v. Azerbaijan*, App. No. 3409/10 (ECtHR, 22 July 2021), ECLI:CE:ECHR:2021:-0722JUD000340910, para 71 and the case-law cited therein.

[65] *Kamić*, supra note 49, paras. 23-24. See also *Wolland v. Norway*, App. No. 39731/12 (ECtHR, 17 May 2018), ECLI:CE:ECHR:2018:0517JUD003973112, para 76.

[66] *Wieser and Bicos Beteiligungen GmbH v. Austria*, App. No. 74336/01 (ECtHR, 16 October 2007), ECLI:CE:ECHR:2007:1016JUD007433601, para 57.

ECHR[67]. Nevertheless, the lack of an *a priori* independent authorisation does not automatically lead to a violation of the Convention. Indeed, the existence of an *ex post facto* oversight on home searches warrants may, on a case-by-case basis, compensate for the lack of a preventive review[68]. Conversely, the absence of any assessment of the lawfulness of the measure at stake (both *ex ante* and *ex post*) may automatically lead to a breach of Article 8 ECHR[69].

To take it in a nutshell, an independent review shall be carried out at least once during the criminal proceedings, so that the person concerned can challenge the (alleged) necessity, proportionality and duration of the measure in question. Should the *ex post facto* review do not explain whether the issuing authority (e.g., the prosecutor) had sufficient and relevant grounds for issuing a search warrant, Article 8 ECHR is violated[70]. Criminal proceedings are thus analysed 'as a whole' by the ECtHR, echoing the (questionable) 'fairness as a whole' test, developed in relation to Article 6 ECHR[71], and based on the idea that certain counterbalancing factors can 'compensate' for a breach of the Convention (and ultimately render 'fair' a procedure that could not, otherwise, be so defined)[72].

Against this background, the benchmark of the guarantees stemming from Article 8 ECHR *in parte qua* could be summarised as follows: (i) in principle, there is a need for an effective and comprehensive *prior* oversight upon the necessity and proportionality of the intrusive investigative measure; (ii) such review may be carried out by either a judicial or an administrative body, provided that the latter authority is sufficiently independent of the executive; (iii) the lack of a preventive assessment of an intrusive measure is not, in itself, in breach of the Convention, provided that other counterbalancing factors are present in the material case, e.g., an *ex post facto* review.

3.1.2. Prior Independent Oversight Under Article 8 ECHR: How floue *Is the ECtHR Approach?*

When it comes to seizures and searches of digital evidence, the standpoint of the Court of Strasbourg mirrors the framework already outlined. Indeed, it

---

[67] *Funke*, supra note 52, para 57, emphasis added. The Court stressed that 'above all' the absence of a prior judicial oversight led the restrictions foreseen in the domestic law 'too lax and full of loopholes for the interferences with the applicant's rights to have been strictly proportionate to the legitimate aim pursued'.

[68] *Smirnov v. Russia*, App. No. 71362/01 (ECtHR, 7 June 2007), ECLI:CE:ECHR:2007:-0607JUD007136201, para 45 *in fine*. See § 4.1.

[69] *DELTA PEKÁRNY a.s. v. the Czech Republic*, App. No. 97/11 (ECtHR, 2 October 2014), ECLI:CE:ECHR:2014:1002JUD000009711, paras 88-94.

[70] *Dorożˇ v. Poland*, App. No. 71205/11 (ECtHR, 29 October 2020), ECLI:CE:ECHR:2020:-1029JUD007120511, para 28.

[71] See Caianiello (2017) and Kostoris (2020).

[72] For what concerns searches and seizures of electronic devices, the existence of an independent *ex post facto* review may be seen as a counterbalancing factor that compensates for the lack of a prior oversight *in parte qua*.

is apparent that searches and seizures of electronic devices as such constitute an interference with 'private life' and 'correspondence'[73], within the meaning of Article 8 ECHR[74]. In past years, several cases have been brought before the ECtHR on this specific issue. On a first sight, their findings could be considered to be in line with the established case-law on data protection.

One of the earliest rulings on searches and seizures of electronic data was *Wieser and Bicos*[75]. The first applicant was an Austrian lawyer and owner and general manager of the second applicant, a holding company. A search was carried out by Austrian police at the registered office of the first applicant's company, which was also his law firm—these activities also embodied the analysis of the first applicant's computer and the copying of the data contained therein[76]. Those operations were executed within the limits set out in the search warrant[77].

In finding a breach of Article 8 ECHR, the ECtHR attached greater relevance to the mismatch between the procedural guarantees ensured to the applicants and their implementation in the material case. While acknowledging that the intrusive measures had been preventively authorised by the investigating judge, the Court found *inter alia* that the applicants had not been provided with a report on the police activities at the end of the latter, nor had the officers carrying out the investigations made any communication concerning the outcome of the research. Nevertheless, these guarantees were laid down in domestic law[78]. Furthermore, the *manner* in which the searches and seizures activities were carried out was taken into consideration by the ECtHR, as the duty of professional secrecy surrounding lawyers' activities might have been hampered should an *arbitrary* collection of data be allowed *vis-à-vis* a legal counsel[79]. Hence, these shortcomings, taken as a whole, were deemed relevant in finding a violation of Article 8 ECHR on the part of the Austrian authorities[80].

Several interesting considerations stem from this judgement. As for the nature of the preventive oversight carried by the investigating judge, the Court

---

[73] *Vinci Construction*, supra note 34, para 63.

[74] *Posevini v. Bulgaria*, App. No. 63638/14 (ECtHR, 19 January 2017), ECLI:CE:ECHR:2017:-0119JUD006363814, para 65. The Court referred to the 'search of residential and business premises entailing … the seizure of equipment containing electronic data'.

[75] *Wieser and Bicos*, supra note 66.

[76] The domestic court, upon a request for legal assistance from Italian authorities, 'ordered the seizure of all business documents revealing contacts with the suspected persons and companies' (ibid., para 7 *in fine*).

[77] Ibid., para 59.

[78] Ibid., paras. 58-63.

[79] Ibid., para 65. In this respect, the Court quoted *Niemietz v. Germany*, App. No. 13710/88 (ECtHR, 16 December 1992), ECLI:CE:ECHR:1992:1216JUD001371088, para 37, in which it interestingly set forth that 'where a lawyer is involved, an encroachment on professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 (art. 6) of the Convention'. The Court additionally stressed that the electronic data seized contained broadly the same information as the paper documents seized, some of which were returned to the first applicant by the investigating judge as being covered by professional secrecy.

[80] Ibid., para 66.

was apparently satisfied that such an assessment would have constituted an 'adequate and effective'[81] safeguard against any abuse or arbitrariness. Moreover, although the existence of an *ex post facto* review was not explicitly mentioned, the individual concerned had the formal possibility of requesting that seized objects be sealed and submitted to the investigating judge, in order to exclude their employment as evidence in the investigations[82], a decision that could have been taken by a judicial body (i.e., the Review Chamber)[83]. Yet, it is noteworthy that the police officers searched and seized a massive amount of data without providing the applicant-lawyer with the opportunity, on the one hand, to object and have the disks sealed and, on the other hand, to receive a detailed and precise list of the data seized and eventually copied together with the search criteria adopted in the material case[84]. These circumstances played a key role in exacerbating the prejudice suffered by the applicant-lawyer under Article 8 ECHR[85].

Five years later, a similar situation—involving an Austrian lawyer, Mr Robathin, whose electronic data had been searched and seized—was examined before the ECtHR[86]. In this case, however, the police officers apprehended *all* the files contained in the applicant's computer system, pertaining to his law firm. Subsequently, and solely on the proposal of the representative of the Bar Association who was present during the operations, these data were split into four CDs. Solely one of the latter contained the files relating to R. and G., alleged victims of the applicant's conducts of fraud, theft and embezzlement[87].

As in *Wieser and Bicos*, the search warrant was issued by the investigating judge and gave details in respect of the alleged acts, the time at which they were committed and the damage allegedly caused[88]. Nevertheless, and in contrast to that judgement, the wording of the warrant was so much vague that it led *de facto* to unlimited searches and seizures of almost all documents,

---

[81] These two expressions have been frequently quoted in the ECtHR's case-law on this issue. See, among others, *Société Colas Est and Others v. France*, App. No. 37971/97 (ECtHR, 16 April 2002), ECLI:CE:ECHR:2002:0416JUD003797197, para 48.

[82] *Wieser and Bicos*, supra note 66, para 64.

[83] Ibid., para 15 in conjunction with para 33. The Court observed that such guarantee applies both to paper documents (as explicitly written in domestic law) and, *mutatis mutandis*, to electronic data.

[84] Still, it is of a certain interest that 'the search was carried out using the name of the companies involved and the names of the suspects in the Italian proceedings' (ibid., para 12). In spite of other shortcomings, this *modus operandi* could be considered compatible with Article 8 ECHR, in that it prevents investigating authorities from coping and apprehending almost *all* electronic material contained in electronic devices (ibid., para 59).

[85] Yet, as will be explained, it could be argued that the danger of such tools is inherent in their nature. The risk of disproportionate intrusion into the private sphere of individuals through searches and seizures for the purpose of collecting digital evidence is *in rerum natura*. This aspect is certainly emphasised in certain specific cases, e.g. where a lawyer is involved in a criminal investigations. However, it seems that such a risk is triggered as soon as the abovementioned measures are implemented against any individual.

[86] *Robathin v. Austria*, App. No. 30457/06 (ECtHR, 3 July 2012), ECLI:CE:ECHR:2012:-0703JUD003045706.

[87] Ibid., paras. 7-11.

[88] Ibid., para 45 *in fine* (compare *Wieser and Bicos*, supra note 66, para 58).

personal computers and discs in the applicant's possession [89]. Thus, the Court looked at possible counterbalancing factors which could provide the individual concerned with sufficient protection against arbitrariness, the *ex post* remedy before the Review Chamber being of paramount importance in this respect [90]. Considering the latter to be overly formalistic and unsubstantiated, a breach of Article 8 ECHR was found to have occurred, in that the search of all the applicant's electronic data was disproportionate *in concreto* [91].

At a first sight, *Robathin* seems to attach great importance to the lack of an adequate and effective *ex post facto* oversight of the intrusive measures at stake. The wideness of the content of the search warrant was considered *en passant*, the Court having focused on the assessment subsequently made by the Review Chamber. However, in the last paragraph, the ECtHR observed that where an investigation relates solely to the activities of the suspect in relation to well-identified victims, 'there should be particular reasons to allow the search of *all other data*, having regard to the specific circumstances prevailing in a law office' [92].

This standpoint, albeit articulated at the end of the line of reasoning developed by the ECtHR, revealed interesting features.

Firstly, where a general search of documents or data is envisaged by the authorities, there shall be a thorough assessment of the necessity to adopt bulk intrusive measures, which may involve information other than that relevant for the material case. Secondly, such an assessment should, as a rule, be carried out *before* the start of the relevant operations begin—such approach proves to be the most adequate for the purpose of preventing the investigating authorities from arbitrarily interfering with the individual's right to respect for private life and correspondence. This holds true *a fortiori* when the suspect is a lawyer, who deserves a higher degree of protection on account of his/her duties of professional secrecy. Thirdly, should a prior oversight have not been conducted with regard to the need to search *all* documents or data owned by the suspect, the existence of *ex post facto* guarantees plays a pivotal role in compensating the lack of a preventive control on the necessity and proportionality of the measure in question.

Yet, it is difficult to understand why 'deficiencies in the limitation of the scope of the search and seizure warrant' [93] might not *per se* constitute a breach of Article 8 ECHR. Where those measures are employed for gathering personal data, the risk of collecting irrelevant and personal data unrelated with the material case is exceedingly high. As a matter of principle, the issuing author-

---

[89] Ibid., para 47 (see *a contrario Wieser and Bicos*, supra note 66, para 59). See, as a recent authority, *Kruglov and Others v. Russia*, App. Nos. 11264/04 *et al*. (ECtHR, February 2020), ECLI:CE:ECHR:2020:-0204JUD001126404, para 127 and the case-law cited therein.

[90] Ibid., para 51.

[91] Ibid., paras. 51-52. Compare *Vinci Construction*, supra note 34, paras. 78-79.

[92] Ibid., para 52, emphasis added. The Court was ready to accept that 'there were no such reasons either in the search warrant itself or in any other document'.

[93] Ibid., para 47.

ity should carry out a preventive screening of the relevant information, i.e. before the start of the operations, unless such a screening proves impossible for specific reasons which must be set out exhaustively in the warrant. This view would aim at strengthening the right of everyone not to be subjected to haphazard intrusions into their private sphere. Still, in light of the precedent established in *Robathin*, it may be deemed permissible, under certain circumstances and with the presence of solid *ex post facto* counterbalancing factors, that the collection of data against the suspect in a general manner does not constitute a violation of Article 8 ECHR.

Reference is to be made to the fact that, while police officers searched and seized all the applicant's data, 'all the copied discs were sealed and could only be examined under the control of the Review Chamber'[94]. Accordingly, the investigating authorities could not employ those pieces of information until a decision issued by a judicial body[95]. Indeed, such mechanism could be seen as an alternative[96] pattern aimed at preventing the bulk, non-necessary and non-proportionate employment of intrusive measures for the purpose of gathering electronic evidence, as the collected material was 'frozen' as soon as the applicant objected to the search of the data.

In 2017, the ECtHR rendered another judgement related to searches and seizures of equipment containing electronic data. In *Posevini*, the intrusive measures—i.e., the searches of the applicant's home and his photography studio—were based on judicial warrants, a fact which the Court emphasised in distinguishing the material case from other previous decisions[97]. For the sake of completeness, a list of the electronic elements seized from the applicant's premises would provide a comprehensive portrait of the intrusiveness of the operations: eleven SIM cards, a laptop computer, three mobile Internet dongles, a mobile telephone, three desktop computers, two video cameras, two still cameras, several flash memory cards and flash memory drives[98].

Against this background, the Court reiterated that the mere existence of a prior independent oversight is not *per se* a sufficient safeguard for the purposes of Article 8 ECHR, as it is the *manner* in which such assessment is carried out that is of paramount importance[99]. As the domestic judge analysed in-depth all the relevant material at his/her disposal, the Court accepted that

---

[94] Dissenting Opinion of Judges Kovler and Lorenzen, attached to *Robathin*, supra note 86.

[95] The situation would have been different if, for instance, the authorities had been able to *make immediate use* of the data obtained in a generalized manner, pending the decision of the judicial body to which the interested party had appealed. In such a case, the infringement of privacy and correspondence would already have occurred, and *ex post facto* control could at most exclude certain evidence from the proceedings, but could not, for example, prevent the authorities from becoming aware of it in any case.

[96] It is worth recalling that, in the context of the present analysis, the existence of a prior independent oversight over an intrusive measure may be seen as the most important means to avoid arbitrariness on the part of public authorities may be avoided.

[97] *Posevini*, supra note 74, paras. 67 and 70 and the case-law cited therein.

[98] Ibid., paras. 14-15.

[99] Ibid., para 70.

the judicial warrants were based on a reasonable suspicion [100]. Yet, these warrants were drafted in very broad terms, allowing for the search and seizure of all objects related to the criminal offence under investigation. May this fact be detrimental to the quality of *ex ante* independent scrutiny? Following a case-by-case approach [101], the Court's answer was in the negative and was essentially influenced by the speed with which the Bulgarian investigative authorities were obliged to act in the material case. What is more, the ECtHR considered that the identification of the, object of the search warrant, with. all items related to the criminal offence under investigation. was 'sufficient *in the circumstances*' to properly limit the margin of manoeuvre given to the investigating bodies [102].

Nevertheless, the Court seems to weaken the importance of a prior independent oversight over extremely intrusive measures. Indeed, it may be questionable whether the 'nature of the alleged offence' can serve as a limit for public authorities in carrying out searches and seizures. Quite the contrary, such standpoint may lead to abusive behaviour on the part of prosecuting authorities, allowing them, for instance, to define the offence under investigation in wide-ranging terms, in order to collect as much data as possible. As is apparent, the identification of the criminal behaviour to be investigated is a task which falls *entirely* in the hands of the public prosecutor—his/her discretionary power in the drafting of criminal charges can in no way serve as a deterrent that can narrow police officers' activities.

Letting the assessment of an intrusive measure be influenced by such ground does not seem to be in keeping with the need to avoid arbitrary behaviour on the part of public powers. Indeed, should such line of reasoning be acknowledged, the margin of discretion of prosecuting authorities would not appear to be subject to any *concrete* limitation, as almost every IT tool might be linked—at least 'potentially'—with a certain alleged offence, given that every individual's personal data is *de facto* contained therein nowadays [103]. Against this background, the extent of the *ex ante* independent review appears to be reduced, arguably disregarding the need to ensure that the measures in question shall be kept within reasonable bounds [104].

Shortly after *Posevini*, the ECtHR rendered another judgement concerning searches and seizures of electronic data [105]. In that case, the applicant, Mr Trabajo Rueda, brought a computer to a technician, in order to have it repaired, stating that it was not protected by a password. As soon as the spe-

---

[100] Ibid., para 71.

[101] See *Sher and Others v. the United Kingdom*, App. No. 5201/11 (ECtHR, 20 October 2015), ECLI:CE:ECHR:2015:1020JUD000520111, para 174.

[102] *Posevini*, supra note 74, para 72, emphasis added.

[103] Ibid., para 72 *in fine*.

[104] In this regard, see *Ernst and Others v. Belgium*, App. No. 33400/96 (ECtHR, 15 July 2003), ECLI:CE:ECHR:2003:0715JUD003340096, para 116.

[105] *Trabajo Rueda v. Spain*, App. No. 32600/12 (ECtHR, 30 May 2017), ECLI:CE:ECHR:2017:-0530JUD003260012.

cialist discovered child pornography material within the device, he informed the police, who searched and then seized it. The applicant was subsequently arrested[106]. It is noteworthy that no prior independent warrant was issued due to the urgency that, according to the police, existed in the material case—searches and seizures without a preventive independent authorisation were foreseen in domestic law. However, the applicant challenged *inter alia* the existence of such urgency ground.

The standpoint taken by the Strasbourg Court in *Trabajo Rueda*—in finding a breach of Article 8 ECHR—looks like an attempt to strengthen the role of *ex ante* judicial review over intrusive measures. Looking at the domestic framework, the ECtHR established that the urgency situation that may lead to omit such control shall exist *in concreto* and cannot be presumed by the police. In the material case, the ECtHR found that the Spanish authorities did not properly justified the need to act without any prior authorisation (which, notably, could have been obtained '*relativement rapidement*'), thus rendering the search and the seizure of the applicant's computer disproportionate *per se* and, as a consequence, unnecessary in a democratic society within the meaning of Article 8(2) ECHR[107].

But the kernel of the judgement lies elsewhere. Indeed, for the first time, the ECtHR emphasised the pivotal role of the prior oversight in the following terms:

> 'La Cour constate que, en ce qui concerne l'accès au contenu d'un ordinateur personnel par la police, la jurisprudence du Tribunal constitutionnel a établi la règle de l'autorisation judiciaire préalable, condition exigée *en tout état de cause* par l'article 8 de la Convention (*qui requiert la délivrance d'un mandat par un organe indépendant*) lorsqu'une atteinte à la vie privée d'une personne est en jeu'[108].

In the light of the previous case-law, this *obiter dictum* depicts unprecedented—and valuable—aftermaths. In fact, referring to the settled Spanish Constitutional Court's case-law, the ECtHR elucidates that an *ex ante* independent oversight is a circumstance entrenched *in any event* in the content Article 8 ECHR. The extent of the wording adopted (*en tout état de cause*) cannot but lead to this crystal-clear conclusion. What is more, the Court seems open to granting individuals with an *absolute* prerogative to have any intrusive measure likely to threaten the right to private life assessed by an independent body *before* it is implemented. In a nutshell, rather than distinguishing different situations and multifaceted controls over intrusive measures on a case-by-case basis, the Strasbourg Court seems here to cast light on a new 'universalistic' perspective on the procedural guarantees stemming from Article 8 ECHR—the need to foresee a prior independent authorisation in all cases where an intrusive measure is to be implemented by the prosecuting authorities.

---

[106] Ibid., paras. 5-7.
[107] Ibid., paras. 45-47.
[108] Ibid., para 35, emphasis added.

Whereby isolated and limited to the material case[109], such 'U-turn' may nonetheless reveal the inconsistency of the fuzzy *status quo* within the settled ECtHR's case-law on procedural guarantees arising from Article 8 ECHR, as emphasised above. This holds true *a fortiori* should one consider that the ECtHR quoted two judgements in order to support this line of reasoning which, however, did refer to wiretappings (and not to digital searches and seizures)[110]. As subsequent judgements have (again) upheld the traditional blurred approach of the Strasbourg Court, we cannot but blame the 'imprecise direction'[111] taken by the ECtHR in denying the significance of a mandatory prior independent supervision in all cases where intrusive measures involving electronic devices are taken against an individual in the context of criminal proceedings.

3.2. Legal Challenges *Pro Futuro*

'How many of us can claim to keep an impenetrable wall between the personal and professional data held within our smartphones?'[112]. The query posed by Judge Pavli sketches the main issue surrounding searches and seizures of electronic devices, as depicted above. We have highlighted that the risk of investigative authorities obtaining (quite easily) a massive amount of data pertaining to a potentially undefined number of individuals is extraordinarily high. What is more, the information gathered may be unrelated to the ongoing criminal investigation and may disclose sensitive data about third parties. Finally, the data collected from a smartphone or a laptop, even when related to the suspect, may reveal extremely private circumstances (e.g., sexual orientation) which shall not be taken into account, in any manner, in a criminal investigation. The impact of these three circumstances on the fundamental rights to personal private life and correspondence cannot be underrated.

Spontaneously, one could think that, in order to avoid haphazard behaviour on the part of investigating authorities, it would be a suitable idea to set up a prior independent scrutiny mechanism. In contrast to those legal systems in which the public prosecutor can *autonomously* implement the aforementioned measures, a shift towards a new standpoint on this issue ought to be reached. Accordingly, independent oversight can (and should) become the cornerstone of the procedure in which searches and seizures of IT tools by the investigating authorities are envisaged.

---

[109] Still, it is noteworthy that *Trabajo Rueda* was essentially decided without this standpoint being significant for the verdict.

[110] *Iordachi and Others v. Moldova*, App. No. 25198/02 (ECtHR, 10 February 2009), ECLI:CE:ECHR:2009:0210JUD002519802 and *Dumitru Popescu*, supra note 59.

[111] Mistilegas et al. (2022), p. 32.

[112] *Särgava*, supra note 34, Concurring Opinion of Judge Pavli.

Against this background, as discussed above, the position taken by the ECtHR in its settled case-law proves to be blurred. What can be observed here is a nuanced line of reasoning that the Strasbourg Court has followed within its settled case-law. The core of the analysis is that an *ex ante* independent oversight is not needed *per se* under Article 8 ECHR. Still, the existence of such control is a factor to be duly taken into consideration by the Court, albeit it is not a necessary ground, the absence of which may automatically lead to a breach of the Convention.

If our reading is correct, and in the light of the above, there is a major flaw in this line of reasoning. We can label it as a 'qualitative' inadequacy. Here we refer to the 'quality' of the intrusive measure at stake which shall meet all the grounds laid down in Article 8 ECHR (and hence *inter alia* be necessary and proportionate in the material case).

Whereby it is true that a prior oversight would not render, in itself, the whole procedure non-arbitrary, we have no difficult in sharing the view that the lack of any previous independent authorisation clearly risks providing public prosecutors or police officers with a wide-ranging power to collect electronic evidence—this clearly runs counter with the well-established need to ensure that any interference with fundamental rights is necessary and proportionate in the material case. Indeed, the lack of any previous scrutiny in this field could plainly lead to abuses, as the investigating authorities may decide, for instance, to search and seize *every* IT tool owned by an individual for evidentiary purposes. Without any prior review, the above considerations do not appear to be mere speculations.

Against this background, we are aware that there might be domestic frameworks that would struggle to comply with these *dicta*. To take a concrete example, as has already been explained, Italian public prosecutors hold a wide power in ordering searches and seizures of electronic devices for the purpose of gathering evidence. Paraphrasing *Funke*, they hold 'exclusive competence to assess the expediency, number, length and scale of inspections'[113].

Given the profound differences between State Parties in this respect, the ECtHR's self-restraint *in parte qua* can be easily understood. However, when it comes to assessing the firmness of human rights, political implications stemming from certain decisions should be set aside. Arguably, the Court's nuanced reluctance to impose a prior independent oversight on every search or seizure of electronic devices was one of those (frequent) instances where politics have regrettably overwhelmed the very substance of a fundamental right.

[113] *Funke*, supra note 52, para 57.

4. PROMOTING A WIDE-RANGING MODEL OF *EX POST* INDEPENDENT REVIEW: IS IT TIME FOR A NEW PARADIGM?

The pivotal role of an *ex post facto* control over digital searches and seizures will be depicted in this Section. Firstly, the relevant ECtHR case-law will be examined. It will be observed that the *ex post facto* oversight is listed among the safeguards that can be put in place against State's arbitrariness. Moreover, it will be noted that such subsequent assessment holds a peculiar characterisation, since it may become the very moment in which the existence *in concreto* of all grounds to be met in the material case as per Article 8 ECHR can be conducted, *after the implementation of the measure at stake* and thus *from a comprehensive standpoint* (§ 4.1). That being said, our analysis will focus on shaping the structure and content of the proportionality test to be carried out within this phase (§ 4.2). Finally, a comparison will be made between different paradigms of subsequent independent review in order to assess which could be the most feasible at the domestic level (using the Italian legal framework as a benchmark), for the same purposes (§ 4.3).

4.1. Hints from the ECtHR

The ECtHR has famously stated that 'the rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure'[114].

In a nutshell, judicial control is inextricably connected to the need to ensure the effectiveness to fundamental rights and is, in turn, closely linked to the rule of law. However, the question remains as to why an independent oversight is particularly needed when it comes to digital searches and seizures, and what legal interest need to be safeguarded by such a mechanism.

In relation to investigative measures that may impact the privacy of individuals, the ECtHR assesses the consistency of national systems of judicial review with the Convention under the 'necessity in a democratic society' test under Article 8(2) ECHR.

The Strasbourg Court found numerous infringements of the right to private life. As briefly mentioned, in *Klass and Others*, the issue of secret surveillance was at the centre of the judgement. In this context, the question of an *ex post* judicial control was closely tied to the matter of subsequent notification, since a long time could elapse before the person was aware that he or she was being secretly monitored. The rules governing secret operations thus appear

[114] *Klass and Others*, supra note 54, para 85.

to be different from those that are applicable to searches and seizures, of which the person is aware immediately before they are carried out.

However, as regards the existence of an independent oversight, the Court's approach remains constant and unvarying: there is a sort of 'independent control degree' that has to be achieved, to be established in the light of an overall consideration of many factors, first of all the existence of both an *ex ante* and *ex post* control or only one of them[115], but also whether the search concerns a natural or a legal person[116] and whether other rights are at stake, such as the lawyers' professional privilege[117]. In any event, the Court did not go far enough in acknowledging the absolute necessity of an *ex post facto* assessment of those measures which may threaten the scope of Article 8 ECHR to be foreseen in domestic frameworks—analogously to what has already been explained about prior independent oversight, the ECtHR's position in this field proves to be blurred, as it analyses the existence of such subsequent control as *one of the factors* to be considered within its line of reasoning.

The Court has thus developed a case-by-case approach. Despite starting from the same wide-ranging principles and even in the presence of similarities between legal systems, the jurisprudence on digital searches and seizures has sometimes varied[118]. Allegations of inconsistency and unpredictability are not without merit. Nevertheless, it may be possible to identify the key considerations for the ECtHR and understand the underlying rationale behind the requirement for an *ex post* independent review of digital searches and seizures.

The Court listed a number of factors which are deemed relevant in ascertaining whether effective safeguards against abuse or arbitrariness are available under domestic law for the purposes of Article 8 ECHR. Certainly, the existence of independent supervision of the measure at stake plays a key role. But other circumstances should also be carefully scrutinised. Firstly, the seriousness of the offence under investigation[119]. Secondly, the status of

---

[115] *K.S. and M.S. v. Germany*, App. No. 33696/11 (ECtHR, 6 October 2016), ECLI:CE:ECHR:2016:-1006JUD003369611, para 45. The Court argued that an *ex ante* independent oversight would not in itself necessarily amount to a sufficient safeguard against abuse; still, it implicitly assumes that it plays a key role. The same was held in *Vinks and Ribicka v. Latvia*, App. No. 28926/10 (ECtHR, 30 January 2020), ECLI:CE:ECHR:2020:0130JUD002892610, para 104 that refers to *Posevini*, supra note 74, para 70.

[116] *Niemietz v. Germany*, supra note 79, para 31; *Bernh Larsen Holding a.s. and Others v. Norway*, App. No. 24117/08 (ECtHR, 14 March 2013), ECLI:CE:ECHR:2013:0314JUD002411708, para 159.

[117] *Kruglov and Others*, supra note 89; *Smirnov*, supra note 68; *Yuditskaya and Others v. Russia*, App. No. 5678/06 (ECtHR, 12 February 2015), ECLI:CE:ECHR:2015:0212JUD000567806.

[118] *Bernh Larsen Holding a.s.*, supra note 116 and *DELTA PEKÁRNY a.s.*, supra note 69. Both judgements concerned the application of administrative inspection measures against legal persons. In the first case, the inspection was held to be lawful even though there was no judicial oversight at any stage of the proceedings. In the second case, even though an *ex post* judicial review was foreseen, such control was considered ineffective and, accordingly, the ECtHR found a violation of Article 8 ECHR. Notably, *Kruglov and Others*, supra note 89 should be considered as a peculiar case—both *ex ante* and *ex post* judicial controls were provided for, but they were nonetheless considered insufficient to prevent a violation of Article 8 ECHR.

[119] In *K.S. and M.S.*, supra note 115, para 48, tax evasion was considered a serious offence and this element was particularly relevant in the Court's reasoning.

the person concerned, in particular whether he/she was already suspected of having committed a criminal offence or having engaged in unlawful activities[120]. Thirdly, whether there was a reasonable suspicion of criminal activity[121]. Fourthly, whether the scope of the investigative measure was reasonably limited[122]. Then, the manner in which the search was executed[123]. Finally, whether some kind of redress or legal consequences[124] were provided by the domestic system in the event of a violation of the individual's rights[125].

As previously stated, the degree of independence of the authority that issued the warrant, as well as the existence of an *ex post facto* judicial review, are listed among these circumstances.

However, it is noteworthy that the ECtHR casts light on the necessity of an effective *ex post facto* independent review, *a fortiori* in those cases in which an *ex ante* independent control has not been carried out[126]. In determining the effectiveness of the review, one can easily notice that all the grounds listed above reappear—an independent authority must be able to assess all of them. Thus, the rationale behind the necessity to establish an *ex post facto*

---

[120] *Smirnov*, supra note 68, para 46; *Kruglov and Others*, supra note 89, para 126.

[121] For instance, see *Modestou*, supra note 35, para 44. In this case, the ECtHR highlighted the fact that the search took place at an early stage of the investigation, when the risk of investigative measures being taken 'as a means of providing the police with compromising evidence relating to individuals who have yet to be identified as suspects in relation to an offence' was extremely high.

[122] *Kruglov and Others*, supra note 89, para 127. Ibid., paras. 128-137: the ECtHR identified numerous shortcomings in both the *ex ante* and *ex post* judicial reasonings and safeguards, with regard to the purpose of the measure in question and the selection of the material to be searched and seized. The same happened in *Smirnov*, supra note 68, para 47 and *Modestou*, supra note 35, para 46. In *K.S. and M.S.*, supra note 115, para 54 the Court considered it positive that the scope of the warrant was limited to what was strictly necessary in the circumstances of the case, also by making an explicit and detailed reference to the tax evasion offence under investigation and, also, by specifying the items sought as evidence. The same reasoning proves to have had an influence on *Bernh Larsen Holding a.s.*, supra note 116, para 173.

[123] In *Modestou*, supra note 35, para 51 a relevant circumstance was that the person was not present at any time during the search. In *Smirnov*, supra note 68, para 48, the ECtHR emphasised the lack of safeguards to avoid interference with the suspect's professional privilege (because he was a lawyer).

[124] In *Bernh Larsen Holding a.s.*, supra note 116, para 171, the Court emphasised the lack of a rule imposing the destruction of irrelevant data. In other cases, the exclusion of evidence was considered a sufficient consequence attached to the ascertained invalidity of the warrant (*Panarisi v. Italy*, App. No. 46794/99 (ECtHR 10 April 2007), ECLI:CE:ECHR:2007:0410JUD004679499, paras. 76-77; *Uzun v. Germany*, App. No. 35623/05 (ECtHR 2 September 2010), ECLI:CE:ECHR:2010:0902JUD003562305, paras. 71 e 72; *Trabajo Rueda*, supra note 105, para 37).

[125] *Inter alia*, in case of digital searches and seizures affecting lawyers, also the presence of a special observer during the search and the possible repercussions on the work and the reputation of the affected persons by the search play a central role (*Kruglov and Others*, supra note 89, para 125; *Yuditskaya and Others*, supra note 117, para 27). Interestingly, in *K.S. and M.S.*, supra note 115, para 56, the latter requirement was taken in consideration, even if the case did not concern a lawyer.

[126] In *DELTA PEKÁRNY a.s.*, supra note 69, para 91, the limitations on the scope of the judge's prerogative of review played a key role in the ECtHR's line of reasoning. See also *Vinci Construction*, supra note 34, para 78. *Smirnov*, supra note 68, para 45, where the lack of an *ex ante* judicial oversight on a search warrant was not counterbalanced by the (excessively formal) *ex post facto* review. Even the timing of the subsequent review may have an influence on the latter's effectiveness—in *Modestou*, supra note 35, para 52, a prosecutor issued the warrant and delegated its execution to the police. In finding a breach of Article 8 ECHR, the Court highlighted the fact that the judicial review took place more than two years after the event.

independent control can ultimately be depicted—to check the proportionality of the *entire investigative operation*, taking into consideration its merits and subsequent execution. In order to be effective, the independent review cannot be limited to assessing the formal aspects surrounding the lawfulness of the procedure. For this reason, should a superficial and merely formal *ex post* independent review take place, the Court has oftentimes found this practice to be incompatible with Article 8 ECHR[127].

Therefore, the pivotal role of the principle of proportionality proves to be the very reason why an independent subsequent review is needed. But proportionality is a shapeshift standard and it is crucial to clearly define its boundaries. This may shed light on the differences between *ex ante* and *ex post* independent review.

4.2. The *Fil Rouge* Between Proportionality and *Ex Post* Independent Review: Deconstructing the Puzzle

It is of utmost importance to distinguish between two stages of violation of the right to private life when gathering digital data.

The first stage pertains to the infringement of the data owner's privacy, which occurs when a police officer or any other individual is granted access to the data[128]. As stated above, this type of violation necessitates a judicial control *prior* to the execution of the measure at stake, as only an *ex ante* independent authorisation can provide a legal basis for a breach of the fundamental right to private life and correspondence. Furthermore, in order to ensure transparency and compliance with the principle of proportionality, various rules can be introduced to regulate live forensic procedures, such as provisions to preserve the integrity of the chain of custody or to impose the involvement of an expert from the first access to the digital data.

With this in mind, further and subsequent interferences of the right to private life may occur. Specifically, when the data become known to other people and, in particular, when they become public, other violations take place[129].

The problem is that the initial judicial authorisation *cannot encompass subsequent infringements*[130]. In order to mitigate the initial risk and to prevent unnecessary and unjustified violations of privacy rights, we believe that a *second* independent control should be established. This is due to the impossibility of foreseeing in advance the content of the electronic device at stake. In this light, it is noteworthy that live forensic best practices dictate that the forensic expert shall make an integral copy of the device, in order to preserve

---

[127] This was the case in *Bernh Larsen Holding a.s.*, supra note 116, and *Kruglov and Others*, supra note 89.

[128] Caprioli (2021), p. 1148.

[129] Ibid.

[130] Kerr (2005), pp. 575-576.

and avoid altering the evidence. Arguably, such a circumstance may reveal the need to ensure a *second* assessment (after the first one carried out without knowing the nature of the data contained in the IT tool).

Against this background, the concern is not only to assess whether the search or seizure was lawful but also, and more critically, to promptly *identify* all relevant material. Remarkably, the right to private life that has already infringed holds the same characterisation that it had at the time of the first intrusion; yet, the potential for the interference is even greater at this stage, as the selected data are now at the disposal of the investigating authorities, who can use them to launch further investigations. Furthermore, those pieces of information may also become public at trial. The need for independent scrutiny becomes even more pressing.

An *ex post* independent review may solely take place once all relevant information has been disclosed to the individual concerned, as the measure at stake (e.g., the search) has already been implemented. Therefore, fair trial rights can be upheld at this stage: adversarial procedure, a neutral and impartial judge, rights of the defence, the right to become aware of the grounds underlying the measure in question and the right to an effective remedy[131]. An adversarial context is also the best way to establish the facts under investigation, as nothing is more valuable than a confrontation with the data owner in order to understand the meaning of the information and assess its relevance to the case. To the contrary, 'warrant applications are *ex parte*; a judge must try to judge whether the search protocol is appropriate based only on the government's presentation of the empirical picture'[132]. This asymmetry can thus be balanced through a *subsequent* assessment of the circumstances that led the first authority to issue a search or a seizure order. In other words, the (limited) knowledge of the judge who previously authorised the intrusive operations ought to be 'corrected' setting up a *new* assessment, to be carried out in *full knowledge* of the circumstances of the case (among which, notably, the *content* of the data seized is of pivotal importance).

In this light, two different proportionality standards may be applied by the authority in charge of the *ex post facto* independent review, in order to select relevant data and protect the right to private life. These standards, to be applied cumulatively, rely upon the hints coming from the ECtHR listed in the previous paragraph.

A first, retrospective, proportionality test, would assess the *lawfulness* of the search or seizure. The competent authority shall put itself in the position of the prosecutor or judge who authorised it, by examining whether the grounds for taking the investigative measure—based on the prognostic assessment possible at the time—existed from the outset. The grounds to be taken into account, and to be weighed against the individual's privacy, would

[131] On fair trial standards with regard to its jurisdictional grounds, see Alonzi (2011), p. 146.
[132] Kerr (2005), p. 575. Additionally, see Zappalà (1994), p. 474.

be the necessity of the act at stake for the investigation (i.e., the act shall result suitable to its objectives and no other less intrusive shall be available *in concreto* in order to reach the same objective), along with the seriousness of the offence and the reasonable suspicion of criminal activity at the time of the search. The latter can be referred to as 'the proportionality *stricto sensu* stage'—even if the measure under scrutiny would appear appropriate and efficient compared to its objective, it is the objective as such that must be examined to determine whether it justifies the State's interest overriding the individual's interest.

At the same time, the *manner* in which the search or seizure was carried out would be assessed as part of this retrospective review of the investigative process. Any errors or abuses committed by the police or experts would be taken into account. Possible grounds in this regard would include the need to preserve human dignity, respect for the scope of the warrant and the rules on maintaining the integrity and reliability of data.

In case this first test fails, the main consequences are twofold: on the one hand, there should be financial redress for the individual concerned; on the other hand, the evidence gathered thereby should not be admitted at trial[133].

Conversely, should the retrospective test find the investigative measure to be lawful, a second, *prospective*, proportionality test would apply.

Remarkably, despite the fact that investigating authorities have acted in accordance with the law, the right to private life and correspondence still holds the potential to be breached. To mitigate this risk, the parameters relating to the admissibility of evidence in the domestic legal system must be taken into account in order to assess whether there is a *real need to use them at trial*, also in the light of the seriousness of the interference carried out in the material case. In particular, the proportionality assessment would relate to *each piece of information and its usefulness in the trial*. It is essential to ensure that the irrelevant material is destroyed, as required by the ECtHR[134]. In particular, the data should be suitable to prove the fact under investigation and should not be redundant, i.e. if the same fact can be established through other evidence, there is no need of using the digital data gathered. Additionally, the independent authority could again focus on the seriousness of the offence.

Finally, the position of third parties whose data have been searched and eventually seized should be protected too. In fact, it is hard, if not impossible,

---

[133] In our view, the so-called 'fruits of the poisonous tree' doctrine should be applied. As is well known, the doctrine, originated in *Nardone v. United States*, 308 U.S. 338 (1939) judgement delivered by the Supreme Court of the United States, prevents national authorities from employing, to the detriment of the accused, information derived from facts obtained as a result of unlawful acts committed by State agents. In the Italian domestic system, even if it has never been plainly accepted, the doctrine has been applied in some judgements. On the issuing of a seizure warrant after an unlawful search, see Illuminati (2010), pp. 534-535.

[134] *Bernh Larsen Holding a.s.*, supra note 116.

to determine in advance the exact data that are stored in a given device[135]. Furthermore, as already stated, the best practice consists in making a forensic copy of the device as it was found. Therefore, it is only during the *ex post facto* independent review that the exclusion of data belonging to third parties becomes conceivable (and also feasible). In this sense, it can be argued that third parties with a legal interest in the case must have the opportunity to defend themselves against the publication of their data and that other-than-judicial authorities (e.g., Data Protection Supervisors)[136] may be involved in criminal proceedings to ensure the protection of private life, should it be necessary.

To some extent, the pattern of the control envisaged in this paragraph may seem abstract. However, it summarises and organises the otherwise unclear requirements set forth by the ECtHR. Furthermore, such a judicial oversight might not be entirely unfamiliar to investigating authorities (e.g., a similar phase is foreseen for analogous measures, such as wiretappings—this is the approach taken in Italy, where the preliminary investigation judge is tasked with reviewing the pertinent material collected through such means and making a selection thereof).

4.3. Conceptualising a Brand-New Model of *Ex Post* Judicial Oversight

It is possible to distinguish among three main types of *ex post* judicial control of the acts carried out during the investigations. Firstly, a wide-ranging assessment that can be granted by the court deciding on the merits of the case (thus, at the end of the main trial). Secondly, a control of specific measures that can be triggered by the suspect through special remedies. Thirdly, an *ad hoc* control over certain measures, that is not triggered by the suspect, but is automatic (*ex officio*).

The first check is a general one, where the judge applies exclusionary rules. It is oftentimes mentioned by the ECtHR in its overall assessment of the safeguards that provide sufficient protection against arbitrariness[137]. However, this kind of control could eventually take place years after the violation has occurred. This might be inconsistent with the needs underlying the *ex post* judicial review in the context of the preliminary investigations. After all, as has been explained, the Strasbourg Court in *Modestou* emphasised the importance of a *prompt* review[138]. Indeed, the issue is that it may be too late—or too little can be done—to restore the damage. This is why the second form of control is often enforced. It happens in the context of precautionary measures (e.g., pre-trial detention). In Italy, not only coercive precautionary meas-

[135] Kerr (2005), p. 575.
[136] In this regard, see Lasagni (2022), pp. 12-14.
[137] See supra note 124.
[138] *Modestou*, supra note 35, para 52. See § 4.1.

ures can be challenged through a quick remedy, namely the judicial review of the orders imposing a coercive measure (*riesame*), but also seizures are subject to such a control.

In particular, the person affected by a digital seizure for evidence-related purposes can challenge the decree that carried it out. As explained in the first paragraph, the Italian Court of Cassation has held that, even after the return of the seized items, the person has a concrete interest in requesting the destruction of any copies of the data held by the investigating authorities, since the right to private life is at stake and, more specifically, the right to 'the exclusiveness of the informative ownership'[139]. This formula depicts the individual's prerogative to have full control over the data owned by an individual and not to have them in possession of public authorities or whoever else without a proper reason.

Furthermore, it is noteworthy that the Italian case-law has gradually extended many principles originally established for coercive precautionary measures to property-related precautionary measures (e.g., preventive seizures) and, in turn, to seizures issued for the purpose of gathering evidence. This is clearly the case with the principle of proportionality[140].

Thus, the Italian legislation appears to be in line with the requirements laid down by the ECtHR and summed up above—the judicial review of the seizure warrant is a prompt judicial remedy, where the judge is able to rule on all relevant matters of fact and of law and, moreover, holds the power to annul, revise or confirm the measure in question, also on the basis of the principle of proportionality.

Nonetheless, some shortcomings still remain. Firstly, there is no clear set of rules aimed at protecting the chain of custody of the data searched and seized[141]; secondly, the CCP does not provide for the involvement of third parties (that is, they cannot apply for a review of the search and seizure measures) and the protection of their legal interests essentially relies on the decisions taken by the person concerned in response to the seizure; lastly, should an appeal be lodged before the Court of Cassation against the outcome of the review procedure, it may pass a long time for a decision to be taken. This may happen in the case of an annulment 'with referral' by the Court of Cassation, which occurs when the latter annuls the decision, but decides to refer the case back to the judge of the review procedure, for a new decision on the merits.

In this case, no strict time limits are foreseen for the new judgement to start and, in the meantime, the data remains at the disposal of the investigat-

---

[139] Court of Cassation, Joint Chambers, No. 40963/2017, supra note 18, para 19.

[140] Court of Cassation, Joint Chambers, 19 April 2018, No. 36072, Botticelli, ECLI:IT:CASS:2018:36072PEN, para 4.4. Additionally, see, among others, Court of Cassation, 27 January 2022, No. 18649, ECLI:IT:CASS:2022:18649PEN; Court of Cassation, 7 September 2021, No. 39168, ECLI:IT:CASS:2021:39168PEN; Court of Cassation, 2 May 2019, No. 18316, ECLI:IT:CASS:2019:18316PEN, para 2.2.

[141] Articles 259 and 260 CCP are not enough, as they are limited to pose general rules, without any clear indication on how to reach their objective.

ing authorities[142]. Another significant lacuna, as previously discussed, was the one pointed out by the landmark *Brazzi* judgement[143], namely the lack of any remedy in the event of a search that is not followed by a seizure. Notably, the recent reform mentioned above[144], as already said[145], established a new remedy specifically devoted to this eventuality, which is designed as an 'opposition' against the search warrant[146]. However, a crucial point is still not addressed, namely the *repercussions of a successful opposition*. For instance, it remains unclear whether a financial compensation could be granted[147]. In the absence of such compensation, it is challenging to assess the significance of the opposition.

The third model of judicial review can be found, in the Italian legal framework, in the case of arrest. In this context, urgent action is required to validate the already executed arrest warrant and, given the importance of the rights involved and the persistent urgency of the situation, a swift judicial review is mandatory and automatic, except in cases of release. This model is particularly effective in safeguarding the rights of the suspect, and the short time limit is justified by the fact that the right to personal liberty is at stake[148].

The need to select data may recommend a different time limit, but a similar model may be suggested for the protection of digital data in the investigative phase, given: (i) the growing importance of the right involved; (ii) the need for a remedy that protects *ex officio* the rights of third parties even in the absence of any action by the suspect; (iii) the need for a prompt decision in order to mitigate the risk of data leaks.

Indeed, the third model can be found in the Italian provisions on the selection of the materials gathered through wiretappings operations. To be fair, both the second and third models are now applicable in this context, as two different patterns apply, depending on when the prosecutor submits this material. If this happens before the end the of preliminary investigations, the judge's review is automatic (third model). If the public prosecutor submits the results of the interceptions along with the notice of the conclusion of preliminary investigations, it will be up to the public prosecutor to make the initial selection and then, at the request of the defence, the judicial review may take place (second model).

The very idea of entrusting to the prosecutor with the selection of the data is debateable[149]. Moreover, the unclear time limit[150] and the dependence of third-party protection on the suspect's decision raise further questions.

---

[142] Court of Cassation, 15 June 2017, No. 39259, ECLI:IT:CASS:2017:39259PEN.

[143] *Brazzi*, supra note 28.

[144] Legislative Decree No. 150/2022.

[145] See § 2.

[146] Article 252a CCP. See also Article 352(4a) CCP.

[147] Gialuz (2022), p. 49.

[148] In view of the guarantees surrounding this procedure, Alonzi (2011), pp. 186-187 considers it to be the prototype for reforms of the precautionary measures' procedure.

[149] See Scalfati (2020), pp. 2-3. See also Caprioli (2021), p. 1396.

[150] Cabiale (2020), pp. 37-38.

However, compared to the rules governing the review of the 'ordinary' seizure decree, an enhanced data protection is provided by *ad hoc* rules governing their storage in a specific archive (Article 269 CCP)[151].

The first pattern, which provides for an automatic control by the judge, clearly ensures a better protection of the right to private life. However, prosecutors usually submit the pieces of information gathered by means of wiretaps at the conclusion of the preliminary investigations stage (thus avoiding the *ex officio* control by the preliminary investigation judge). In fact, they would have no advantage in disclosing them beforehand. There is therefore a great risk that the first pattern will remain on paper.

Conclusively, we believe that the third paradigm of *ex post* judicial control should be enforced prior to the admission of digital evidence at trial. This model meets all of the ECtHR's requirements for *ex post facto* independent control, and other forms of assessment may not effectively protect the right to private life enshrined in Article 8 ECHR.

5. CONCLUDING REMARKS

The right to private life and correspondence needs strong procedural guarantees in order to be safeguarded, and, among others, both *ex ante* and *ex post* oversights prove to be effective in this respect. Yet, Italian legal framework does not provide for such guarantees. The public prosecutor is 'left alone' with the task of deciding *whether* and *to what extent* a search and seizure of electronic devices would be necessary and proportionate in the material case. The role of the preliminary investigating judge is thus pointless for this purpose.

Certainly, this choice is not in breach of neither the EU law nor the ECHR. The former does not provide any specific rule in this field, while the latter has developed a nuanced case-by-case jurisprudence.

Nevertheless, the line of reasoning advocated here—that is, the need, in any case, for an independent prior and *ex post facto* scrutiny on the measure under investigation—cannot ignore two other (collateral) issues that should be considered, albeit briefly.

Firstly, in the lack of an *ad hoc* discipline concerning IT tools, the CJEU has developed a florid case-law on the access by public authorities to retained data for the purposes of criminal prosecution. The principles developed therein, while not regulating digital searches and seizures, can be considered *mutatis mutandis* as a minimum theoretical framework from which to start, in order to emphasise that, should a prior independent authorisation be needed when external data shall be gathered, such control should exist *a fortiori* when the entire content of an IT tool is to be searched and seized (§ 5.1).

[151] On the secrecy of the data contained therein, see Nappi (2020) and Gialuz (2020), p. 68.

Secondly, fostering more independent review in this field might not be without consequences for the entire structure of criminal procedure. This process of widening judicial prerogatives confronts us with one of the paradoxes at the heart of criminal justice systems, namely the role of the public prosecutor as an independent authority. While, as will be explained, we may agree that the latter lacks independence in the sense envisaged by the CJEU, it cannot be underestimated that this 'shift' towards a major presence of the judge in the preliminary investigations phase would progressively weaken the role of the public prosecutor in accusatorial systems—this may represent a sensitive issue for Member States that are customarily reluctant to share their prerogatives in criminal matters.

5.1. Is There an Elephant in the Room? Looking at the 'Data Retention Saga'

As is known, the expression 'data retention saga' is commonly used to refer to a series of judgements rendered by the CJEU that have progressively imposed strict boundaries on the EU Member States' legal frameworks regarding the retention of digital data by telephone and internet service providers, as well as the access to such data by public authorities for the purpose of prosecuting crime[152]. The 'saga' begun with the landmark *Digital Rights Ireland*[153], which found the Directive 2006/24/EC (the so-called Data Retention Directive)[154] to be invalid and thus determined the Directive 2002/58/EC (the so-called e-Privacy Directive)[155] to come back into force.

Among those judgements, *H.K.*[156] has had a tremendous echo, especially in Italy[157]. In particular, the CJEU has held that the power to authorise access by a public authority to traffic and location data for the purposes of a criminal investigation cannot be conferred upon the public prosecutor's office, 'whose task is to direct the criminal pre-trial procedure and to bring, where

[152] Among the most recent judgements, see Joined Cases C-793/19 and C-794/19, *SpaceNet*, ECLI:EU:C:2022:70 and Joined Cases C-339/20 e C-397/20, *VD*, ECLI:EU:C:2022:703.

[153] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, ECLI:EU:C:2014:238.

[154] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [OJ L 105, 13.4.2006, pp. 54-63].

[155] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [OJ L 201, 31.7.2002, p. 37-47].

[156] Case C-746/18, *H.K.*, ECLI:EU:C:2021:152.

[157] See, among others, Resta (2021) and Spangher (2021). Subsequently, *H.K.* triggered the aforementioned reform, in the 2021, of Article 132 of the Legislative Decree No. 196/2003, i.e., Privacy Code—this provision now foresees the need for a judicial authorisation should the prosecutor aim at acquiring traffic data collected by Internet and telephone service providers (cfr. § 2). In this regard, see Filippi (2022), Malacarne (2021), pp. 1164-1168 and Resta (2021).

appropriate, the public prosecution in subsequent proceedings'[158]. Conversely, the access by the competent national authorities to the retained data must 'be subject to a prior review carried out either by a court or by an independent administrative body'[159].

The position taken by the CJEU was to ensure that the possibility of access to the retained data is assessed in the light of the principle of proportionality[160], with the view of striking 'a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access'[161].

Accordingly, a public prosecutor, albeit formally 'independent' from the Government, proves not to be in the best position to carry out the required proportionality assessment of the access to the data concerned. It is important to note that a public prosecutor does not hold a neutral role in the context of criminal proceedings, due to his/her duty to conduct the investigation and, should it be case, to conduct prosecutions before the courts.

Against this backdrop, the CJEU has further observed that, in any case, the prior review shall be carried out by a body which acts objectively and impartially, free from any external influence, and which must act as a third party *vis-à-vis* the authority requesting access to the data. In other words, it must not be involved in the conduct of the criminal investigation in question, while maintaining a neutral stance *vis-à-vis* the parties to the criminal proceedings[162].

Additionally, it was stated that the existence of a *subsequent* review by a court 'would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met'[163]. In a nutshell, the CJEU seems to think that an *ex post* independent review over the act issued by a prosecutor, would not compensate for the lack of an *ex ante* oversight. In the words of AG Pitruzzella, this is due to the fact that 'otherwise the prior nature of the review would lose its purpose, which is to prevent access to retained data that would be disproportionate to the objective of investigating, prosecuting and sanctioning criminal offences'[164]. In terms of practical consequences, the approach

---

[158] *H.K.*, supra note 156, para 59.

[159] Ibid., para 51.

[160] One of the main grounds relates to the *scope of the access*, which should be granted, as a general rule, 'in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime' (ibid., para 50).

[161] Ibid., para 52. In this regard, see, additionally, Case C-746/18, *H.K.*, Opinion of AG Pitruzzella, ECLI:EU:C:2020:18, para 105.

[162] *H.K.*, supra note 156, paras. 53-54. In this regard, see, additionally, *H.K.*, Opinion of AG Pitruzzella, supra note 161, paras. 110-126.

[163] *H.K.*, supra note 156, para 58.

[164] *H.K.*, Opinion of AG Pitruzzella, supra note 161, para 128.

envisaged in *H.K.* would tend to distinguish the scope and the extent of the two different supervisions. What is more, the CJEU seems to reject the assessment of the proceedings 'as a whole' that the ECtHR has repeatedly advocated in this field.

Interestingly, *H.K.* proves to take into account the peculiarities of *each* assessment; nevertheless, it casts light on the paramount importance of the *ex ante* control of the access to the retained data, the absence of which, in the material case, cannot be made up for by a subsequent review of the material gathered thereby. Accordingly, while there is a blurred symmetry between prior and *ex post facto* review in the eyes of the ECtHR—the lack of the former not entailing, as such, a breach of the right to private life—, the opposite is certainly true at the EU level, where *any* access to electronic data must be authorised *a priori* by a judicial or independent body[165].

We have already made it clear that digital searches and seizures for evidence-related purposes are not, as such, regulated by EU law[166]. Still, it is possible to highlight that the theoretical background that had inspired the CJEU rulings of the 'data retention saga' is proving to be valid in relation to digital searches and seizures for the purpose of gathering evidence in the context of criminal proceedings.

Notably, in the aforementioned *Digital Rights Ireland*, the CJEU stated that the data retained by telephone and internet service providers, such as location data, the calling telephone number and the number called in a telephone communication and the IP address for internet services, 'taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them'[167]. In other words, the retention of and the access to data which make it possible to depict essential aspects of the private life of individuals brings to a serious interference with their right to private life and the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.

This is the very theoretical basis of the whole 'data retention saga', including the need for judicial authorisation established by *H.K.* Foremost among these strands is the ECtHR's commitment to avoid a wide-ranging and extremely invasive collection of data that may relate to aspects of this individuals' life other than those that may be relevant for the purposes of a criminal investigations.

---

[165] See De Terwangne (2022), p. 23.

[166] See § 1.

[167] *Digital Rights Ireland*, supra note 153, para 27. This expression has been frequently quoted within the relevant CJEU's case-law. See, among others, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, para 99.

Additionally, one cannot but acknowledge that digital searches and seizures give public authorities the access not only to the very same data that they can obtain by accessing to the data stored by telephone and internet service providers, but also to the content of SMS, e-mails, notes *etc*.

Thus, the blurred state of the art in EU law is the following—on the one hand, specific safeguards for the access to data retained by telephone and internet service providers are foreseen (and among these safeguards, the prior review on the proportionality of the access by an independent and impartial authority plays a pivotal role), while, on the other hand, no limitations are expressly imposed on prosecuting authorities with regard to digital searches and seizures[168]. As anticipated, Directive 2002/58/EC is currently in force and triggers the EU competence solely in the field of data retention, letting aside the topic under consideration here. This turns into a lack of substantive and procedural guarantees for the suspect or the accused person which has not yet been dealt with by the EU legislature. While this picture is plainly inconsistent with the relevant ECtHR's case-law, it is worth recalling that the absence of EU rules in this field stems from the lack of political consensus in a very sensitive area of criminal procedure.

For the sake of truth, we have to admit that the *ratio* behind the 'data retention saga' also relates to the need to avoid the risk of a sort of bulk private surveillance caused by the retention of a huge amount of data by telephone and internet service providers. The implementation of digital searches and seizures does not raise this issue.

Certainly, it could be argued that the increasingly frequent and widespread use of such investigative measures raises the same concern expressed by CJEU in relation to data retention by telephone and internet service providers. Indeed, this is the likelihood 'to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'[169]. Remarkably, such a perception might stem not only from massive data retention or from secret surveillance methods (e.g., wiretappings), but also from the possibility to search and seize IT devices without the lawfulness of such measures being assessed by a court or an independent body.

That being said, in the lack of any EU piece of legislation specifically addressing this issue, the settled ECtHR's case-law on Article 8 ECHR provides a benchmark against which national authorities may be limited in issuing and executing searching and seizures measures. Albeit not ensuring the same level of protection sketched by the CJEU in the context of the 'data retention saga', it is nonetheless crucial in setting limits to prosecuting bodies while protecting the right to private life and correspondence. It is in this light that

---

[168] In this regard, see Chelo (2022), pp. 1583-1592.

[169] *Digital Rights Ireland*, supra note 153, para 37. In this regard, see, also Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger*, Opinion of AG Cruz Villalón, ECLI:EU:C:2013:845, paras. 52 and 72.

the 'clash between those who seek to defend liberty and those who seek more security'[170] can hopefully be brought to an end.

5.2. Public Prosecutors and Judicial Control: A Never-Ending (Italian) Story

Against the background outlined above, there is still a critical issue to be addressed. Advocating for more independent oversight of certain acts, normally carried out by the public prosecutor, could have consequences for the whole structure of the preliminary investigation phase and, to a wider extent, for the role of the judge and the public prosecutor, and their connections. Essentially, the more the public prosecutor's prerogatives are subject to authorisation by the judge or an independent authority, the less relevant the role of the public prosecutor will be in the whole procedure. What are the practical consequences of this judge-centred tendency, particularly in the field of electronic evidence? Might this approach be effective in ensuring the fundamental rights of the suspect or the accused person?

To answer this question, it is worth recalling some of the findings developed within the Italian academic debate on the role of the public prosecutor and the preliminary investigation judge (*giudice per le indagini preliminari – GIP*).

Before the entry into force of the CCP in 1989, the investigative phase in Italy was dominated, alongside the prosecutor, by the investigating judge (*giudice istruttore*). This examining magistrate was vested with broad inquisitorial powers[171].

Many scholars have argued that, in order to introduce the features of the adversarial system into the criminal trial, that powerful body, which conducted the investigations by means of 'unchecked powers', should have been expunged from the domestic framework[172]. In line with this doctrinal standpoint, the aforementioned CCP abolished the investigating judge figure and gave the prosecutor the leading role in the investigative stage. Such a strong role was (and still is) supposed to be counterbalanced by the fact that what is gathered during the 'preliminary investigations' does not constitute 'evidence' as such—indeed, the 'evidence' that the judge can use for the final decision may only be constituted, as a general rule, by the materials and information gathered in court during the trial, through cross-examination and within adversarial proceedings.

In a nutshell, the idea behind the new structure of the Italian criminal procedure was based on the assumption that the preliminary investigation was a

---

[170] Juszczak, Sason (2021), p. 259.

[171] On the inquisitorial Italian criminal justice system before 1989, see, *inter alia*, Cordero (2012), pp. 86-87.

[172] The idea stemmed from the famous *'bozza Carnelutti'* (see Carnelutti (1963)) and Cordero (1965). For a historical perspective, see Colao (2016), pp. 241-277, Orlandi (2016) and Reale (2018).

phase that was 'neither relevant nor weighty'[173]. The brand-new preliminary investigation judge was (and still is) designed to be confined to supervisory functions to be exercised in exceptional cases, specifically laid down in the CCP and involving the fundamental rights of the suspect at the investigative stage, such as his/her personal liberty. The aim was to create an agile and streamlined stage aimed solely at preparing the trial, in order to put the latter and the adversarial rules in place therein at the core of the proceeding[174].

What has happened is that the investigation stage has quickly become lengthy and burdensome for the suspect, who is subjected to the intrusive investigative measures at the disposal of the prosecutor, oftentimes without adequate counterbalancing powers[175]. This may be the case with searches and seizures for the purpose of gathering evidence (even electronic evidence), the execution of which is not subject to any prior control by the preliminary investigation judge. Furthermore, the control exerted by that magistrate resulted oftentimes to be lax, formalistic and unsubstantiated. In this regard, it is noteworthy that the Italian Court of Cassation had to deal with ordonnances or decrees issued by preliminary investigation judges which were merely a 'copy-paste' of the prosecutor's request[176].

Against this background, the Italian academic debate has also focused on the fact that the public prosecutor, even if controlled by a judicial authority in certain circumstances, could anyway hold a *quasi*-absolute power in the preliminary investigation phase, due to its inherent inquisitorial tendency[177]. Amusingly, this view seems to be shared, to a certain degree, by other scholars who claim that after 1989 the prosecutor is *de facto* the 'evidence master'[178].

This backdrop explains why, over the years, the rights of the defence in the investigative stage have been progressively strengthened (notably, specific regulation on defence investigations has been established)[179]. A number of provisions have been introduced to ensure a proper control by the preliminary investigation judge over prosecutor's acts (e.g., the requirement of an *independent* and specific assessment of the main grounds foreseen for the adoption of precautionary custodial measures)[180]. Recently, as mentioned above, a law was passed to ensure that the public prosecutor has to ask the preliminary investigation judge for authorisation to access to traffic data stored by telephone and internet service providers[181].

---

[173] Nobili (1998), p. 35 *et seq*.

[174] Zappalà (1989), pp. 49-51.

[175] Giuliani (2018), pp. 484-486.

[176] For instance, see Court of Cassation, 24 May 2012, No. 22327, ECLI:IT:CASS:2012:22327PEN.

[177] In 1965, this was the prediction, with regard to the proposal of an investigative stage assigned to the sole public prosecutor, of Nuvolone (1965), pp. 195-197.

[178] Ferrua (1996), p. 51.

[179] Articles 391(a)–391(i), established *ex novo* by Law No. 397/2000.

[180] Article 292(2)(ca) CCP, established *ex novo* by Law No. 47/2015.

[181] Article 132 Legislative Decree No. 196/2003, i.e., Privacy Code, modified by Decree-Law No. 132/2021.

What we described so far is an Italian story. However, the problems that have arisen in Italy may arguably also be found within other domestic systems, where legislators might struggle to strike a balance between efficient investigations and a proper protection of fundamental rights, by introducing an independent control over certain public prosecutors' acts.

In a nutshell, the twin-track system that has been developed in Italy can be summarised as follows. There are some acts that the public prosecutor can implement *motu proprio* and without any control (e.g., searches and seizures of electronic devices for evidentiary purposes), while there are other acts that the public prosecutor can carry out solely once the authorisation of the preliminary investigation judge has been granted (e.g., access to retained data).

What is interesting here is the fact that, from a practical point of view, both the public prosecutor and the preliminary investigation judge are *independent* from the executive according to Italian Constitution (so-called 'external independence'). Focusing on this point alone, one may question the necessity to foresee a sort of 'duplication' of independent bodies within the framework of preliminary investigations.

Yet, there is another factor which needs to be assessed, that is, the 'internal independence' of the magistrate *vis-à-vis* the parties to the criminal proceedings (i.e., impartiality)[182]. But again, at first glance, the Italian system might seem redundant—the public prosecutor is obliged by the CCP to carry out its investigations both *à charge et à décharge*. This is quite evident from the wording of Article 358 CCP: 'the public prosecutor … shall also carry out investigations into facts and circumstances in favour of the person under investigation'.

Admittedly, there is some merit in the view that the presence of a judge alongside the prosecutor, who is supposed to be objective and impartial, is a contradiction in terms[183]. It is certainly true that a certain ambiguity on the part of the prosecutor is unavoidable, since he/she will always share, to a certain extent, the interest of the judge, namely the duty to enact criminal law[184]. The public prosecutor represents, in fact, an essential articulation of jurisdiction and has to promote it within its limits[185].

Nevertheless, the need for a judge during the investigative stage arises from the inevitable bias to which the prosecutor is exposed[186]. Thus, although in presence of an independent and impartial prosecutor, the existence of a preliminary investigation judge is neither illogical nor contradictory. This also explains why, as has been said, such judge should not be 'stronger' than

---

[182] This is quite clear from the wording of *H.K.*, supra note 156, para 50 *et seq*.

[183] Ferraioli (2014), pp. 111-112 and 117.

[184] Caianiello (2003), pp. 11-14. On the importance of a functional distinction between prosecutors and judges, who should at least partly pursue different interests, see Riccio (2011), pp. 352-355.

[185] Orlandi (1999), p. 211. In this regard, see the opinion of Carnelutti (1953), p. 260, according to which the prosecutor is a judge making itself a party, by lowering from its natural position.

[186] Caianiello (2003), pp. 11-12; Orlandi (1999), p. 211; Santoriello (2021).

the prosecutor, but it should be 'more different'[187], meaning that it is crucial not to give the preliminary investigation judge autonomous powers, but to keep the latter away from any duty of conducting the investigation[188]. It could even be argued that the aforementioned *H.K.*'s reasoning on the lack of neutral stance for the prosecutor (see § 5.1) is not an entirely new acknowledgment in the Italian system.

Indeed, the Italian CCP tended to deprive the public prosecutor of any decision-making power regarding the adoption of measures restricting the freedoms protected by the Constitution, also in order to 'purge' the prosecutor of any function that was not compatible with its role as a party[189]. This explains why someone was even surprised that searches and seizures were (and are) left in the hands of the prosecutor[190].

Following this line of reasoning, one could even argue that increasing the occasions for and the intensity of judicial review of the public prosecutors' acts might have the positive effect of reducing the latter's powers and, as a consequence, enhancing a feature that is really important for adversarial proceedings, namely the equality of arms.

5.3. Trying to Pull the Strings, From Italy to Europe

In the light of the foregoing, may the Italian public prosecutor be regarded as *independent* in the sense envisaged in *H.K.*?

If our reading is correct, the answer must be in the negative. As the public prosecutor is responsible for investigating crimes and is therefore fully involved in the criminal proceedings, it may be questionable whether he/she holds a neutral stance towards the parties to the criminal proceedings. In this regard, the aforementioned obligation laid down in Article 358 CCP, by analogy with which was held in *H.K.*, cannot ensure *per se* that the decision to order the access to retained data is assessed by a public prosecutor acting as a third party[191]. After all, this viewpoint seems to be in keeping with what AG Pitruzzella emphasised in his Conclusion in *H.K.*—an authority is to be deemed independent: (i) if it is not subject to external pressures and (ii) if it can perform its activities with objectivity, thus securing impartiality, weighting its decisions as a third party[192].

Certainly, it is somewhat paradoxical that *non-independent* public prosecutors need an *independent* authorisation in order to access retained data, while they can search and seize electronic devices *motu proprio*, without any

[187] Zagrebelsky (1996), pp. 26-27.
[188] Ibid, p. 27. In this regard, see Greci (1988), p. 372.
[189] Alonzi (2011), p. 140.
[190] Angiolini (1992), p. 115.
[191] See, by analogy, Rovelli (2021), p. 208.
[192] Revolidis (2020), p. 323.

sort of oversight. This inconsistency, which is clearly evident when analysing the findings of the ongoing 'data retention saga' (being the ECtHR's case-law more blurred in this field), can also be observed in inquisitorial legal systems, where the independence of investigating judges has recently been questioned—according to Van Muylder, for instance, it cannot be excluded that Belgian investigating judges '*ne présente pas l'indépendance nécessarie pour autoriser l'accès à des métadonnées conserves par les opérateurs*'[193]. Apparently, this might also hold true with regard to other investigating judges (e.g., the French, the Dutch or the Spanish ones).

The ongoing debate on the impact of the 'data retention saga' and the role of public prosecutors within domestic systems clearly sketches the framework within which new rules on searches and seizures of IT tools should be laid down. Given the nuances of the ECtHR's case-law, it will arguably be up to the EU legislature to find a path to achieve consistency between the settled case-law of both the European courts on the one hand and to the protection of the right to private life and correspondence in Europe on the other, trying to equalise procedural guarantees for similar breaches of the aforementioned prerogatives.

After all, criminal proceedings 'feeds on information'[194]. The easier it is to obtain information from individuals, the more solid the procedural guarantees should be. From this perspective, it may be feasible to safeguard the right to private life in its two pivotal elements—as the 'right to be let alone' (i.e., the right of individuals to exclude third parties from their private sphere)[195] and as the right of individuals to freely dispose of their own data (*habeas data*)[196].

BIBLIOGRAPHY

Alonzi, F. (2011). *Le attività del giudice nelle indagini preliminari. Tra giurisdizione e controllo giudiziale*. CEDAM.

Angiolini, V. (1992). *Riserva di giurisdizione e libertà costituzionali*. CEDAM.

Bachmaier Winter, L. (2022). Criminal Investigation, Technological Development, and Digital Tools: Where Are We Heading?. In Bachmaier Winter, L., & Ruggeri, S. (Eds.), *Investigating and Preventing Crime in the Digital Era* (pp. 3-17). Springer.

Bartholomew, P. (2014). Seize First, Search Later: The Hunt for Digital Evidence. *Touro Law Review*, 30(4), Article 10. *https://digitalcommons.tourolaw.edu/lawreview/vol30/iss4/10*

Bartoli, L. (2018, March 5). Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature. *Archivio penale*. *https://archiviopenale.it/sequestro-di-dati-a-fini-probatori-soluzioni-provvisorie-a-incomprensioni-durature/articoli/15338*

Bartoli, L., & Lasagni G. (2021). Antifraud Investigation and Digital Forensics: A Comparative Perspective. In Caianiello, M., & Camon A. (Eds.), *Digital Forensic*

[193] Van Muylder (2022), p. 365.
[194] Orlandi (1998), p. 140.
[195] Van der Sloot (2021).
[196] Pérez-Luño Robledo (2017), p. 215 *et seq.*

Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations (pp. 207-235). CEDAM-Wolters Kluwer.

Braghò, G. (2019). L'ispezione e la perquisizione di dati, informazioni e programmi informatici. In Luparia, L. (Ed.), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)* (pp. 181-196). Giuffrè.

Cabiale, A. (2020). L'acquisizione delle intercettazioni con procedura di controllo giudiziale: ritorni al passato e nuove lacune. In Gialuz, M. (Ed.), *Le nuove intercettazioni. Legge 28 febbraio 2020, n. 7*. *Diritto di Internet*, (annex to Issue 3), 32-48.

Caianiello, M. (2017). You Can't Always Counterbalance What You Want. *European Journal of Crime, Criminal Law and Criminal Justice*, 25(4), 283-298. *https://ssrn.com/abstract=3186642*

— (2003). *Poteri dei privati nell'esercizio dell'azione penale*. Giappichelli.

Caprioli, F. (2021). Intercettazioni e tutela della *privacy* nella cornice costituzionale. *Cassazione penale*, (4), 1141-1152.

Carnelutti, F. (1963). *Verso la riforma del processo penale*. Morano.

— (1953). Mettere il pubblico ministero al suo posto. *Rivista di diritto processuale*, (1), 257.

Cascone, G. (2022). Il sequestro informatico nel prisma del principio di proporzione. *Diritto penale e processo*, (1), 123-138

Chelo, A. (2022). Sequestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma. *Diritto penale e processo*, (12), 1583-1592.

Colao, F. (2016). Per una Storia del Processo Penale «all'Italiana». «Astratte Modellistiche» e «Abitudini Profondamente Radicate». In Meccarelli, M., & Solia Sastre, M.J. (Eds.), *Spatial and Temporal Dimensions for Legal History. Research Experiences and Itineraries* (pp. 241-277). Max Planck Institute for European Legal History. *https://www.jstor.org/stable/j.ctvqhtzn.10*

Cordero, F. (2012). *Procedura penale* (9th ed.). Giuffrè.

— (1965). Linee di un processo accusatorio. In *Criteri direttivi per una riforma del processo penale* (pp. 61-81). Giuffrè.

Cuomo, L. (2022). La prova digitale. In Canzio, G., & Luparia, L. (Eds.), *Prova scientifica e processo penale* (pp. 623-701). CEDAM-Wolters Kluwer.

De Lucchi López-Tapia, Y., & Jiménez López, N. (Eds.). (2022). *The Criminal Justice System in Spain*. Atelier.

De Terwangne, C. (2022). L'illégalité nuancée de la surveillance numérique : la réponse des juridictions belge et française à l'arrêt *La Quadrature du Net* de la Cour de justice de l'Union européenne. *Revue Trimestrielle des Droits de l'Homme*, 129(1), 3-27. https://doi.org/10.3917/rtdh.129.0003

Felicioni, P. (2019). Le ispezioni e perquisizioni di dati e sistemi. In Cadoppi, A., Canestrari, S., Manna, A., & Papa, M. (Eds.), *Cybercrime* (pp. 1377-1436). Utet.

Ferraioli, M. (2014). *Il ruolo di «garante» del giudice per le indagini preliminari*. CEDAM.

Ferrua, P. (1996). Il giudice per le indagini preliminari e l'acquisizione delle prove. In *Il giudice per le indagini preliminari dopo cinque anni di sperimentazione* (pp. 51-65). Giuffrè.

Filippi, L. (2022, February 15). Tabulati telefonici e telematici e rispetto della vita privata. *Diritto di difesa*. *https://dirittodidifesa.eu/la-disciplina-italiana-dei-tabulati-telefonici-e-telematici-contrasta-con-il-diritto-u-e-di-leonardo-filippi/*

Greere, S. (2006). *The European convention on human rights: achievements, problems and prospects*. Cambridge University Press.

Grevi, V. (1988). La garanzia dell'intervento giurisdizionale nel corso delle indagini preliminari. *Giustizia penale*, (1), col. 353-374.

Gialuz, M. (2022, November 2). Per un processo penale più efficiente e giusto. Guida alla lettura della riforma Cartabia (profili processuali). *Sistema penale*. *https://www.sistemapenale.it/it/scheda/gialuz-per-un-processo-piu-efficiente-e-giusto-guida-alla-lettura-della-riforma-cartabia*

— (2020). Segreto a tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni. In Gialuz, M. (Ed.), *Le nuove intercettazioni. Legge 28 febbraio 2020, n. 7*. *Diritto di Internet*, (annex to Issue 3), 61-72.

Giuliani, L. (2018). Indagini preliminari. In Bargis. M. (Ed.), *Compendio di procedura penale*, (9th ed.). CEDAM-Wolters Kluwer, 483-638.

Harnold, S., & Harris, J.R. (2017). What is arbitrary power?. *Journal of Political Power*, 10(1), 55-70. https://doi.org/10.1080/2158379X.2017.1287473

Illuminati, G. (2010). L'inutilizzabilità della prova nel processo penale italiano. *Rivista italiana di diritto e procedura penale*, 53(2), 521-546.

Juszczak, A., & Sason E. (2021). Recalibrating Data Retention in the EU The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?. *EUCRIM*, (4), 238-266. *https://doi.org/10.30709/eucrim-2021-020*

Kerr, O.S. (2005). Searches and Seizures in a Digital World. *Harvard Law Review*, 119(2), 531-585. https://www.jstor.org/stable/4093493

Kostoris, R.E. (2020). Per una 'grammatica' minima del giudizio di equità processuale. *Rivista italiana di diritto e procedura penale*, 63(4), 1675-1698.

Lasagni, G. (2022, July 21). Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della privacy. *La legislazione penale*. *https://www.lalegislazionepenale.eu/wp-content/uploads/2022/07/Lasagni.pdf*

Lorenzetto, E. (2019). Le attività urgenti di investigazione informatica e telematica. In Luparia, L. (Ed.), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)* (pp. 135-164). Giuffrè.

Malacarne, A. (2021). "Gravità" dell'ingerenza e "terzietà" dell'organo titolare del potere autorizzatorio: vecchi e nuovi principi in materia di *data retention*. *Rivista italiana di diritto e procedura penale*, 64(3), 1164-1168.

Mitsilegas, V., Guild E., Kuskonmaz, E., & Vavoula, N. (2022, May 12). Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal*. *https://doi.org/10.1111/eulj.12417*

Montesquieu, C.-L.d.S. (1965). *De l'esprit des lois*. Ernest Flammarion.

Monti, A. (2019). La nuova disciplina del sequestro informatico. In Luparia, L. (Ed.), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)* (pp. 197-217). Giuffrè.

Nappi, A. (2020, April 17). Appunti sulla nuova disciplina delle intercettazioni. *Giustizia insieme*. https://www.giustiziainsieme.it/it/processo-penale/1013-appunti-sulla-nuova-disciplina-delle-intercettazioni-di-aniello-nappi?hitcount=0

Nobili, M. (1998). Diritti per la fase che "non conta e non pesa". In Nobili, M., *Scenari e trasformazioni del processo penale* (pp. 34-49). CEDAM.

Orlandi, R. (2016). Diritti individuali e processo penale nell'Italia repubblicana. *Revista Brasileira de Direito Processual Penal*, 2(1), 7-41. https://doi.org/10.22197/rbdpp.v2i1.15

— (1999). Qualche rilievo intorno alla vagheggiata figura di un pubblico ministero europeo. In Picotti, L. (Ed.), *Possibilità e limiti di un diritto penale dell'Unione europea* (pp. 207-216). Giuffrè.

— (1998). Il processo nell'era di internet. *Diritto penale e processo*, (2), 140-145.

Pérez-Luño Robledo, E.C. (2017). *El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías*. Dykinson.

Reale, F. (2018). Il giudice per le indagini preliminari: un distacco reale o apparente dal giudice istruttore?. *Italian Review of Legal History*, (4), 1-23. *https://doi.org/10.13130/2464-8914/12927*

Renucci, J.-F. (2021). *Droit Européen des Droits de l'Homme* (9th ed.). LGDJ.

Resta, F. (2021, October 2). La nuova disciplina dell'acquisizione dei tabulati. *Giustizia insieme*. *https://www.giustiziainsieme.it/it/processo-penale/1968-la-nuova-disciplina-dell-acquisizione-dei-tabulati-di-federica-resta*

— (2021, March 6). Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna. *Giustizia insieme*. *https://www.giustiziainsieme.it/it/costituzione-e-carta-dei-diritti-fondamentali/1603-conservazione-dei-dati-e-diritto-alla-riservatezza-la-corte-di-giustizia-interviene-sulla-data-retention-i-riflessi-sulla-disciplina-interna*

Revolidis, I. (2020). *H.K. v Prokuratuur*: On Balancing Crime Investigation and Data Protection. *European Data Protection Law Review*, 6(2), 319-324. *https://doi.org/10.21552/edpl/2020/2/20*

Riccio, G. (2001). Equivoci culturali e incertezze semantiche nella soluzione del problema italiano del pubblico ministero. In Mazzamuto, S. (Ed.), *Il Consiglio Superiore della Magistratura. Aspetti costituzionali e prospettive di riforma* (pp. 333-361). Giappichelli.

Rovelli, S. (2021). Case *Prokuratuur*: Proportionality and the Independence of Authorities in Data Retention. *European Papers*, 6(1), 199-210. *https://search.datacite.org/works/10.15166/2499-8249/469*

Santoriello, C. (2021, July 5). Il pubblico ministero ed i cento talleri di Kant. *Archivio penale*. *https://archiviopenale.it/il-pubblico-ministero-ed-i-cento-talleri-di-kant/articoli/28168*

Scalfati, A. (2020, January 7). Intercettazioni: spirito autoritario, propaganda e norme inutili. *Archivio penale*. *https://archiviopenale.it/intercettazioni-spirito-autoritario-propaganda-e-norme-inutili/articoli/21774*

Schabas, W.A. (2015). *The European Convention on Human Rights: A Commentary*. Oxford University Press. 10.1093/law/9780199594061.001.0001

Smith, T. (2015). *Judicial Review in an Objective Legal System*. Cambridge University Press. *https://doi.org/10.1017/CBO9781316335246*

Spangher, G. (2021, May 3). I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali. *Giustizia insieme*. *https://www.giustiziainsieme.it/en/news/74-main/122-processo-penale/1709-i-tabulati-un-difficile-equilibrio-tra-esigenze-di-accertamento-e-tutela-di-diritti-fondamentali*

Torre, M. (2019). Indagini informatiche e principio di proporzionalità. *Processo penale e giustizia*, (6), 1433-1437. *https://www.processopenaleegiustizia.it/indagini-informatiche-e-principio-di-proporzionalita*

Valentini, V. (2017). On the Value of Constitutions and Judicial Review. *Criminal Law and Philosophy*, 11(4), 817-832. *https://link.springer.com/article/10.1007/s11572-016-9390-9*

Van der Sloot, B. (2021). The right to be let alone by oneself: narrative and identity in a data-driven environment. *Law, Innovation and Technology*, 13(1), 223-255. *https://doi.org/10.1080/17579961.2021.1898315*

Van Muylder, C. (2022). La conservation des données de télécommunication à des fins de poursuites pénales – la jurisprudence européenne sur le droit belge. *Droit Pénal de l'Enterprise*, (4), 343-365.

Winick, R. (1994). Searches and Seizures of Computers and Computer Data. *Harvard Journal of Law & Technology*, 8(1), 75-128.

Zappalà, E. (1994). Le garanzie giurisdizionali in tema di libertà personale e di ricerca della prova. *Rivista di diritto processuale*, (2), 470-488.

— (1989). Le funzioni del giudice nella fase delle indagini preliminari. In Gaito, A. (Ed.), *Le nuove disposizioni sul processo penale* (pp. 49-76). CEDAM.

Zagrebelsky, V. (1996). Il giudice per le indagini preliminari nel quadro dell'ordinamento giudiziario, in *Il giudice per le indagini preliminari dopo cinque anni di sperimentazione* (pp. 17-29). Giuffrè.

Ziccardi, G. (2019). L'ingresso della *computer forensics* nel sistema processuale italiano: alcune considerazioni informatico-giuridiche, in Luparia, L. (Ed.), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul* cybercrime *(l. 18 marzo 2008, n. 48)* (pp. 165-177). Giuffrè.