SUSANNA SCHIAVONE

Digital Evidence Seizures in Criminal Proceedings: Ensuring Effective Judicial Oversight in EU and Italian Law

Digitisation has reshaped criminal investigations, heightening the tension between investigative efficiency and fundamental rights. This paper outlines the EU framework for acquiring digital evidence, emphasising proportionality and purpose limitation as key safeguards. It analyses the 2024 CJEU judgment in Case C-548/21, which treats access to mobile devices as highly intrusive and subject to prior independent authorisation. The study then considers its impact on Italian legal system, examining Supreme Court case law declaring the nullity of unauthorised digital seizures while allowing urgent access under ex post *judicial review. It argues that nullity should be grounded in the public prosecutor's functional incompetence and highlights the need to strengthen the judge's role in preliminary investigations to ensure EU-compliant rights protection.*

Il sequestro di prove digitali nei procedimenti penali: garanzie per un controllo giurisdizionale effettivo nel diritto UE e nel diritto italiano

La digitalizzazione ha profondamente alterato il profilo delle indagini penali, accentuando la tensione tra efficienza investigativa e tutela dei diritti fondamentali. Il presente contributo ricostruisce il quadro normativo vigente nell'UE in materia di acquisizione delle prove digitali, mettendo in luce il ruolo centrale dei principi di proporzionalità e di limitazione dello scopo quali presidi di garanzia essenziale. Muovendo dall'analisi della sentenza della Corte di giustizia dell'Unione europea del 2024 (C-548/21), che qualifica l'accesso ai dispositivi mobili (anche in forma tentata) come misura altamente invasiva e, pertanto, subordinata a una preventiva autorizzazione da parte di un'autorità indipendente, lo studio ne indaga le ricadute sull'ordinamento italiano. Si esamina quindi la giurisprudenza con cui la Corte di cassazione ha dichiarato la nullità dei sequestri digitali non autorizzati, pur ammettendo che un accesso urgente sia subordinato a un controllo giurisdizionale successivo. L'A. sostiene che la nullità dovrebbe essere ricondotta alla figura dell'incompetenza funzionale del pubblico ministero, evidenziando la necessità di rafforzare il ruolo del g.i.p. quale garante effettivo dei diritti dell'indagato, in una prospettiva di piena conformità al diritto UE.

SUMMARY: 1. Digital Devices and the Reassessment of Evidentiary Seizure. – 2. EU Safeguards in Digital Evidence Acquisition. – 3. Implications for Domestic Legal Systems. – 4. Italian Case Law Following the CJEU Judgment. – 4.1. Functional incompetence and the Nullity of the Prosecutor's Seizure Order. – 4.2. Reconciling Investigative Needs and EU Fundamental Rights. – 5. Concluding Remarks.

1. *Digital Devices and the Reassessment of Evidentiary Seizure.* The progressive digitisation of social relations has profoundly reshaped the epistemic foundations of criminal investigations[1]. Digital devices – most notably smartphones and personal computers – have become central repositories of personal, relational and behavioural data, providing law enforcement authorities with unprecedented insight into individuals' private lives[2]. Consequently, the seizure of such devices may be considered as an investigative measure that raises profound ethical concerns[3] and exerts a significant impact on fundamental rights[4]. Unlike traditional forms of evidentiary seizure, depriving an individual of a digital device entails not only the temporary removal of a physical object but also potential access to a vast and heterogeneous set of person-

[1] Within the extensive literature on the subject, the evolution of criminal investigations in response to technological developments is most recently explored in the volume, *Indagini e prove nella società digitale. Questioni attuali e prospettive future,* edited by Di Paolo - Pressacco, Trento, 2025, 115 ff. See, also, BELVINI, *Intelligenza artificiale e circuito investigativo*, Bari, 2025, 147 ff.; CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale: un orizzonte denso di incognite*, in *Rev. bras. dir. proc. pen.*, 2019, 3, 1167 ff.; CURTOTTI, *Attività di acquisizione della* digital evidence*: ispezioni, perquisizioni e accertamenti tecnici*, in ATERNO *et al., Cyber Forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Turin, 440 ff.; ERBEŽNIK, *Impact of Digital Evidence Gathering on the Criminal Justice System: A Broader Perspective*, in *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, edited by Franssen - Tosza, Cambridge, 2025, 13 - 42; LASAGNI, *The Impact of Digital Technology on Italian Criminal Proceedings*, in *Zeitschrift für die gesamte strafrechtswissenschaft,* 2023, 135(3), 598-619; LUPARIA DONATI - FIORELLI, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in *Dir. pen. cont.,* 2022, 2, 34 ff.

[2] FLORIDI, *Introduction*, *The Onlife Manifesto: Being Human in a Hyperconnected Era*, edited by Floridi, Berlin, 2014, 2, where the author describes how the development and rapid diffusion of technology are profoundly impacting the human condition, particularly shaping the way individuals understand their own identity ("*our self-conception*") and interact with the surrounding world.

[3] With regard to the ethical challenges arising from data-driven policing, see DAVIS - PURVES - GILBERT - STURM, *Five ethical challenges facing data-driven policing*, in *AI and Ethics*, 2022, 2, 186 ff.

[4] On the interplay between technological advancement and the restriction of fundamental rights, see BACCARI - CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Dir. pen. proc.*, 2021, 6, 711 ff.; BELVINI, *Data protection e accertamento penale nel panorama europeo e nazionale*, in *Arch. pen. web*, 2024, 1, 4, 12 April 2024; ID., *Intelligenza artificiale e circuito investigativo*, Bari, 2025, 45 ff.; CAIANIELLO, *Diritti, libertà e garanzie sostanziali e processuali*, in *Introduzione al diritto penale europeo. Fonti, metodi, istituti, casi,* edited by Manes – Caianiello, Torino, 2020, 285; CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. bras. dir. proc. pen.*, 2017, 2, 485 ff.; FALATO, *L'uso (preventivo e repressivo) di dati personali come compressione di un diritto inviolabile*, in *Giust. pen.*, 2016, 3, 548; NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milan, 2021, 147 ff.

al data, often unrelated to the offence under investigation[5]. This qualitative shift challenges classical procedural categories and raises questions about the adequacy of existing procedural safeguards[6], particularly where access to device contents is authorised without prior judicial scrutiny.

At the EU level, a regulatory framework has emerged to address the specific challenges posed by digital evidence, aiming to reconcile cross-border investigative efficiency with the protection of fundamental rights. Directive 2014/41/EU on the European Investigation Order (EIO), for instance, facilitates swift evidence gathering across member States while grounding the issuance of EIO in the principles of necessity and proportionality[7]. Similarly, the

---

[5] A notable example of these investigative techniques is provided by operations carried out in the context of the cases "EncroChat" and "Sky ECC", examined by by BAJOVIĆ - ĆORIĆ, *Encrochat and Sky ecc Data as Evidence in Criminal Proceedings in Light of the cjeu Decision*, in *Eur. Journal of Crime, Criminal Law and Criminal Justice,* 2 September 2025; DANIELE, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini"*, in *www.sistemapenale.it*, 17 July 2024; ID., *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite*, in *Sist. Pen.*, 11 December 2023; FILIPPI, *Criptofonini SKY-ECC e messaggi criptati: la Corte di cassazione attua i principi di diritto enunciati dalle Sezioni unite*, in *Penale Dir. e Proc.*, 11 April 2024; GAITO, *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC)*, in *this Review*, 2024, 1, 4; GRANDI, *Le garanzie dell'ordine europeo di indagine penale alla prova della vicenda* encrochat, in *Dir. pen. proc.*, 2024, 9, 1245 ss.; LORENZETTO, *Le condizioni per la trasmissione e l'utilizzo dei dati di comunicazioni criptate "Encrochat" acquisiti tramite Ordine europeo di indagine penale*, in *Cass. Pen.*, 2024, 9, 2876 ff.; MARAFIOTI, *Chat criptate e tirannie tecnologiche sulla prova*, in *Il Riformista*, 7 December 2024; MAZZA, *Sky-Ecc e l'ipocrisia del mutuo riconoscimento*, in *Il Riformista*, 7 December 2024; MURRO-NOCERINO, *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini*, in *Pen. Dir. e Proc.*, 21 October 2024; SCHIAVONE, *Equivalenza a doppio standard nell'acquisizione della prova precostituita tramite OEI*, in *Dir. pen. cont.*, 2025, 1, 191 ff.

[6] This aspect has been addressed in detail by BELVINI, *Intelligenza artificiale e circuito investigativo*, Bari, 2025, 111 ff.; NICOLICCHIA, *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla* querelle *giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero*, in *Sist. Pen.*, 2024, 2, 189 ff.

[7] See Article 6(1) (a) of the Directive 2014/41/UE. Within the framework of the European Investigation Order, proportionality operates as a "filter", acting as a benchmark for the legitimacy of investigative measures and ensuring a careful balance between the imperatives of evidence-gathering and the protection of fundamental rights. On this specific topic, see CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Proc. pen. giust.*, 2015, 3, 6 ff.; CALAVITA, *L'ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione europea*, Milan, 2025, 32 ff.; DANIELE, *L'impatto dell'ordine europeo di indagine penale sulle regole probatorie nazionali*, in *Dir. pen. cont.,* 2016, 3, 76; DI PAOLO, sub *Art. 9 d. lgs. n. 108/2012 (Ordine di indagine europeo, Particolari modalità di esecuzione), Codice di procedura penale commentato,* edited by Giarda - Spangher, Milan, 2023, 4, 2749 ff.; FALATO, *La propor-*

more recent "e-Evidence package"[8] introduces European Production and Preservation Orders for electronic data held by service providers, also anchored in proportionality to ensure that the scope and intrusiveness of measures are commensurate with their legitimate aims[9]. Together, these legislative developments indicate that EU law increasingly frames the regulation of digital evidence as an exercise in balancing investigative effectiveness with the risks of indiscriminate access to personal data, with proportionality serving as an essential tool to mediate competing interests.

This normative trend is mirrored in practice, as judicial authorities at both European and national levels increasingly apply the same logic, particularly in

---

zione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale, in *Arch. pen. web*, 2018, 1; GATTO, *Il principio di proporzionalità nell'Ordine europeo di indagine penale*, in *DPC*, 2019, 2, 69 ff.; NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *www.archiviodpc.dirittopenaleuomo.org*, 8 January 2018.

[8] The reference is to Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023, laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of obtaining electronic evidence in criminal proceedings; and to Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023, on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and on the execution of custodial sentences following criminal proceedings. Both legislative texts are available at *www.eur-lex.europa.eu.* To ensure coherent application of the rules and allow sufficient time for implementation and adaptation by the individual national legal systems, the Regulation will enter into force on 18 August 2026, while the Directive must be transposed into the legislation of EU Member States by 18 February 2026. On the topic, see CALAVITA, *L'ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione europea*, Milan, 2025, 309 ff.; FORLANI, *The E-evidence Package. The Happy Ending of a Long Negotiation Saga*, in *Eucrim,* 2023, 2, 174 ff.; GAUDIERI, *Novità in tema di cooperazione giudiziaria: i nuovi ordini europei di conservazione e produzione delle prove elettroniche*, in *Dir. Pen. e Proc.,* 2023, 9, 1231 ff.; JUSZCZAK-SASON, *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. An Introduction to the New EU Package on E-evidence*, in *Eucrim*, 2023, 2, 182 ff.; MURIEL DIÉGUEZ, *Las Órdenes de Entrega y Conservación de Pruebas Electrónicas en el Proceso Penal Europeo*, in *Revista de Estudios Europeos*, 2024, 172 ff.; PFEFFER, *Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln. Aktuelle nationale, europa und völkerrechtliche Entwicklungen*, in *Eucrim*, 2023, 2, 170 ff.; SACHOUILIDOU, *Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation*, in *New Journal of Eur. Crim. Law*, 6 June 2024; TABASCO, *L'acquisizione transfrontaliera delle prove elettroniche*, in *Proc. pen. giust.,* 2025, 4, 969 ff.; TOPALNAKOS, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, in *Eucrim*, 2023, 2, 200 ff.

[9] In this regard, reference can be made, for example, to Article 5(2) and Article 6(2) of Regulation (EU) 2023/1543, which respectively govern the European Production Order and the European Preservation Order.

response to the systemic challenges posed by data-driven policing practices[10]: proportionality guides the design and review of investigative measures, ensuring that interventions targeting digital evidence are both appropriate and minimally intrusive. The judgment of the EU Court of Justice of 4 October 2024 marks a pivotal point in this evolution, articulating a preventive and risk-based approach to data protection in criminal investigations and highlighting the ongoing challenge of translating these principles into effective domestic practice.

2. *EU Safeguards in Digital Evidence Acquisition.* In a landmark judgment of 4 October 2024 (Case C-548/21), the EU Court of Justice delivered a decision of crucial importance for the regulation of digital evidence under EU law. Its relevance is twofold. On the one hand, the EU Court of Justice held that the attempted access to data stored on a smartphone for investigative purposes constitutes «processing of personal data» within the meaning of Directive (EU)2016/680[11], irrespective of whether such an access ultimately proves to be successful[12]. On the other hand, this judgment contributes to reinforcing the

[10] On data-driven policing, as a paradigm of criminal investigation based on the large-scale aggregation, cross-referencing and re-use of data collected through diverse channels and for heterogeneous purposes, and on its implications for criminal investigations and fundamental rights, see DE JONGE - DE VRIES, *Data-Driven Investigations in a Cross-Border Setting*, in *Eucrim*, 2024, Vol. 19(3), 214 - 221; TE MOLDER - FEDOROVA - DUBELAAR - LESTRADE, *The principle of purpose limitation in data-driven policing: A guiding light or an empty shell?*, in *New Journal of Eur. Crim. Law*, 2023, 4, 512 - 533.

[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[12] EUCJ, GC, *CG v. Bezirkshauptmannschaft Landeck*, 4 October 2024 (Case C-548/21). The case arose from the seizure of a mobile phone by Austrian customs police in the context of a criminal investigation concerning drug-related offences. After the suspect refused to disclose the unlocking credentials, law enforcement authorities made several attempts to access the data stored on the device without prior judicial authorisation and without informing the data subject. Although unsuccessful, those attempts were later disclosed in judicial proceedings initiated by the individual concerned, giving rise to doubts as to whether such conduct constituted "processing of personal data" within the meaning of Directive (EU) 2016/680 and whether national legislation permitting such practices was compatible with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union. For early commentary, see FILIPPI, *La CGUE mette i paletti all'accesso ai dati del cellulare*, in *Quot. giur.*, 10 October 2024; MURRO, *Le problematiche del sequestro dello smartphone arrivano alla corte*

application of the principle of purpose limitation in the acquisition of digital evidence[13], by framing access to mobile phone data as a particularly intrusive measure that must be strictly confined within the limits of necessity and adequacy.

By adopting a functional and teleological interpretation of the concept of "processing", the Court decisively detached the applicability of EU data protection guarantees from the empirical outcome of the investigative act[14]. At the same time, this interpretative approach significantly broadened the scope of that concept, expanding the range of situations in which EU data protection safeguards apply and, consequently, strengthening the level of protection afforded to the accused. This expansion is most clearly reflected in the Court's innovative interpretation of the notion of "personal data" within the meaning of Article 3(1) of Directive (EU) 2016/680. According to the EU Court of Justice, this notion encompasses any information stored in the memory of a mobile device insofar as such information is capable of revealing aspects of the private and family life of its owner, including, *inter alia*, lifestyle patterns, places of stay, daily movements, activities pursued and social relationships.

From a systematic standpoint, this amounts to a teleologically oriented conception of personal data, characterised by variable and context-sensitive contours that depend on the informational potential of the data concerned. Therefore, all information contained in a smartphone may fall within the no-

---

di giustizia europea, in *Dir. Pen. e Proc.*, 2025, 10, 1211 ff.; RAUCCI, *Le condizioni per l'accesso ai dati del cellulare per il diritto europeo*, in *Arch. pen. web*, 2025, 2, 20 May 2025; ID., *Sequestro del cellulare e acquisizione dei dati: possibili patologie dell'atto alla luce della recente giurisprudenza europea*, in *Proc. pen. giust.*, 2025, *5*, 1243 ff.; WAHL, *ECJ Ruled on Police Access to Mobile Phone Data*, in *Eucrim*, 2024, 3, 189-191.

[13] An in-depth analysis of the principle of purpose limitation under Directive (EU) 2016/680 is provided in TE MOLDER - FEDOROVA - DUBELAAR - LESTRADE, *The principle of purpose limitation in data-driven policing: A guiding light or an empty shell?*, in *New Journal of Eur. Crim. Law*, Vol. 14, 2023, 4, 512 ff., where it is further specified that the principle of purpose limitation «is generally considered to consist of two building blocks»: *(i)* «purpose specification» (Article 4(1)(b)) and *(ii)* «compatible use, or the non-incompatibility requirement» (Article 4(2)). Each of these components is thoroughly examined in the study cited.

[14] On this point, reference may be made to SCHIAVONE, *Nuove garanzie europee per l'acquisizione della prova digitale*, in *Arch. pen. web*, 2025, 1, 2 April 2025.

tion of "personal data" as construed by the Court, including – a *fortiori* – categories of sensitive personal data, insofar as they are able to disclose the most intimate prerogatives of the individual. The differentiating criterion, that allows personal data to be distinguished from the broader universe of information stored on a mobile device, lies in the data's capacity to penetrate the sphere of personal intimacy of the data subject. The greater the expressive and revelatory power of the information, the broader the level of protection afforded to it under EU law.

Within this framework, the notion of "personal data" covers information retrievable from a mobile device relating to telephone traffic, location data, photographic material, internet browsing history, and even the content of stored communications. As the Court has expressly observed, access to such an aggregated set of data «may enable very precise conclusions to be drawn concerning the private life of the person concerned»[15].

In light of this expansive interpretation, all safeguards under Directive (EU) 2016/680 apply even to mere attempts to access data stored on a mobile device for investigative purposes. Among these safeguards, the principle of purpose limitation, enshrined in Article 4, emerges as a cornerstone of EU data protection law[16]. Pursuant to Article 4(1)(b), personal data must be collected for «specified, explicit, and legitimate purposes» and may not be processed «in a manner incompatible with those purposes», while Article 4(2) permits processing for other purposes only if lawful, «necessary and proportionate». According to this legal framework, investigative data collection remains strictly tied to predetermined objectives, preventing arbitrary or excessive interference with fundamental rights. Hence, the purposes of any access must be defined from the outset, given that, had the attempt succeeded, the data would immediately have fallen under the investigative authority, making prior speci-

[15] See § 93 of the judgment, quoted *verbatim.*

[16] *The EU General Data Protection Regulation (GDPR), A Commentary*, edited by Kuner - Bygrave – Docksey, Oxford, 2020, 315, where it is clarified that the principle of purpose limitation implements the connection between data protection and the right to privacy, prevents the undue concentration of power, and is instrumental in fostering trust in the information society.

fication essential to prevent disproportionate or arbitrary use. On the contrary, excluding attempted access from the scope of processing would undermine the Directive's aim of safeguarding personal data and compromise the ability of data subjects to retain control over their information.

Similarly, proportionality, codified in Article 4(1)(c), acts as a fundamental constraint on investigative powers[17]. Compliance requires that access to mobile data be limited to clearly defined categories of offenses, proportionate to the investigative goal and, except in duly justified emergencies, subject to prior independent oversight.

Under this latter aspect, authorisation for the execution of an evidentiary seizure involving digital devices must, as a rule, be granted prior to the measure by a judicial authority or an independent administrative body, save for duly justified cases of urgency in which subsequent authorisation may be allowed. Building on its established case law on data retention[18], the EU Court of Jus-

---

[17] Among many, for the application of the proportionality principle to investigative measures, see: ARAI-TAKAHASHI, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Intersentia, 2002, 14; CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *archiviodpc.dirittopenaleuomo.org*, 18 June 2014; CAMON, *La prova genetica tra prassi investigative e regole processuali*, in *Proc. pen. giust.*, 2015, 6, 167; CASSIBBA, *"Trasfigurazione" delle indagini preliminari, principio di proporzionalità e controllo giurisdizionale effettivo*, in *this Review*, 25 October 2024; GATTO, *Il principio di proporzionalità nell'ordine europeo di indagine penale*, in *archiviodpc.dirittopenaleuomo.org*, 12 February 2019; NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *www.archiviodpc.dirittopenaleuomo.org*; SIGNORATO, *Indagini e prove digitali*, in *Riv. dir. proc.*, 2024, 4, 1152; TORRE, *Indagini informatiche e principio di proporzionalità*, in *Proc. pen. giust.,* 2019, 6, 1433 ff.; TRIDIMAS, *The General principles of EU Law*, Oxford, 2006, 194; UBERTIS, *Prova penale e proporzionalità*, in *www.sistemapenale.it*, 23 January 2025.

[18] Among the most recent rulings, see EU Court of Justice, GC, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights*, in *Giur. cost.*, 2014, 3, 2948; EU Court of Justice, GC, 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB*, in *Official Journal of the EU*, C 53/11, 20 February 2017; EU Court of Justice, GC, 6 October 2020, Case C-66/18, *La Quadrature du Net and A.,* in *Official Journal of the EU*, C-392, 29 October 2018. For a comprehensive overview of the legal framework shaped by these rulings and a critical analysis thereof, see the studies by: ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milan, 2008, 120-125; CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Cass. Pen.*, 2005, 596-599; DE AMICIS, *La Corte di Giustizia si pronuncia sull'acquisizione dei tabulati telefonici e sull'accesso ai dati delle comunicazioni elettroniche nel processo penale*, in *Cass. Pen.,* 2021, 7-8, 2556 ff.; DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in

tice rules out that this function may be entrusted to the public prosecutor, who, by reason of its partisan role in the proceedings[19], does not provide the level of independence required to perform such a supervisory role. Therefore, it is for a judge or an independent administrative authority to ensure compliance with the principles enshrined in EU law. In particular, observance of the principle of proportionality requires these bodies to exercise effective control over the gravity of the interference, the sensitivity of the data concerned, the importance of the investigative objective pursued and the existence of a concrete connection between the owner of the device and the suspected offence. Such an assessment ensures that access to digital devices and the searches conducted therein are confined to what is strictly necessary and are employed only as an *ultima ratio*.

The Court ultimately identified three cumulative conditions for EU-compliant access to mobile device data: (i) the nature or categories of offenses must be precisely defined in advance; (ii) processing must respect the principle of proportionality; and (iii) except in duly substantiated urgent cases, access attempts must be subject to prior review by a judicial or independent administrative authority.

3. Implications for Domestic Legal Systems. The CJEU judgment has profound implications for domestic criminal legal systems, particularly regarding

---

www.sistemapenale.it, 29 April 2021; DI STEFANO, *La Corte di giustizia interviene sull'accesso ai dati di traffico telefonico e telematico e ai dati di ubicazione a fini di prova nel processo penale: solo un obbligo per il legislatore o una nuova regola processuale?*, in *Cass. Pen.*, 2021, 7-8, 2563 ff.; IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, in *Cass. Pen.*, 2014, 12, 4274 - 4282; LASAGNI, *Dalla riforma dei tabulate a nuovi modelli di integrazione fra diritti di difesa e tutela della privacy*, in *Leg. Pen.*, 21 July 2022; NEGRI, *Data retention, impatto critico sui procedimenti già aperti*, in *Guida al dir.*, 39, 2021, 41; RAFARACI, *Verso una* law of evidence *dei dati*, in *Dir. pen. proc.,* 2021, 7, 853 ff.; RESTA, *Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla* data retention*. I riflessi sulla disciplina interna*, in *www.giustiziainsieme.it*, 6 March 2021; SPANGHER, Data retention*: le questioni aperte*, in *www.giustiziainsieme.it,* 9 October 2021; WHAL, *CJEU: Data Retention Allowed in Exceptional Cases*, in *Eucrim*, 2020, 3, 184 ff.

[19] On this point, see ZANON, *Pubblico ministero e Costituzione*, Padua, 1996, 88-89; SECHI, *Convalidare il sequestro probatorio da parte del p.m. non è esercizio di funzione giudicante*, in *Giur. cost.*, 2002, 2, 788.

the protection of fundamental rights in the digital environment. By framing access to mobile devices as a highly intrusive measure, the Court makes clear that such access must comply with the principles enshrined in Directive (EU) 2016/680.

In practical terms, this requires that national procedures ensure investigative measures are strictly proportioned to achieve a legitimate objective and that the purposes for which personal data may be accessed are clearly defined in advance.

The judgment underscores that fundamental rights – including the right to privacy, the right to an effective defence, equality of arms, and effective judicial protection – cannot be subordinated to investigative expediency[20]. In particular, proportionality imposes a gatekeeping limit on the intensity of interference, the selection of investigative means and the treatment of sensitive personal data, while purpose limitation ensures that data are accessed only for clearly predetermined objectives. As a result, member States must reassess procedural rules, embedding these EU principles into national practice to prevent arbitrary or excessive intrusion and guaranteeing that access to digital evidence is permitted only as a last resort under prior independent oversight[21].

Ultimately, the judgment reinforces the idea that the effectiveness of criminal investigations cannot be pursued at the expense of the essence of fundamental rights and that proportionality operates as an *ex ante* condition of legality for digital investigative measures.

4. *Italian Case Law Following the CJEU Judgment.* Recent Italian case law reflects a growing awareness of the need to balance investigative powers with judicial safeguards. In particular, a line of reasoning developed within the juris-

[20] In this respect, see MALACARNE, *Sequestro probatorio (informatico): proporzionalità, segreto professionale e garanzie dell'attività difensiva*, in *Dir. di internet*, 2025, 131 ff.; MURRO, *Lo* smartphone *come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Padua, 2024, 253 ff.

[21] From this point of view, see LASAGNI, *Tackling Phone Searches in Italy and the United States: Proposals for a Technological Rethinking of Procedural Rights and Freedoms*, in *New Journal of European Criminal Law*, 2018, 394.

prudence of the Italian Supreme Court affirms the nullity of evidentiary seizures of digital devices carried out in the absence of adequate judicial authorisation.

In the following sections, two recent rulings of the Supreme Court will be examined to illustrate the overall impact of this jurisprudence on the criminal procedural system[22]. On the one hand, it emerges that any act by which the public prosecutor orders a seizure is invalid if prior judicial approval is lacking. On the other hand, the case law recognises circumstances in which a subsequent judicial review is sufficient, particularly in cases of necessity and urgency, allowing law enforcement authorities to act promptly while still safeguarding fundamental rights.

4.1. *Functional incompetence and the Nullity of the Prosecutor's Seizure Order.* In its judgment No. 13585/2025, the Italian Supreme Court addressed the legal significance of accessing the contents of digital devices. The Court acknowledged that such access constitutes a qualitatively distinct investigative act, which cannot be assimilated to traditional forms of seizure.

Consistent with the principles articulated by the EU Court of Justice, the absence of prior judicial authorisation does not merely affect the evidentiary value of the data acquired but renders the procedural act itself formally null[23]. Significantly, the Court framed the issue in terms of nullity rather than mere unlawfulness or evidentiary inadmissibility, highlighting the structural importance of judicial oversight within the criminal procedure[24].

---

[22] Cass., Sec. VI, 1 April 2025, n. 13585; Cass., Sec. III, 20 January 2026, n. 2218.

[23] After declaring the act null due to a «lack of authority», the Court proceeds with reasoning that is somewhat inconsistent, further justifying the invalidity on the basis of a principle previously established in the "*Encrochat"* case (§ 131): namely, that evidence obtained without giving the defendant the opportunity to exercise their right of defense by addressing the evidence collected against them must be excluded from criminal proceedings. For a more comprehensive analysis, see SCHIAVONE, *L'incompetenza funzionale del p.m. travolge il sequestro probatorio*, in *Cass. Pen.*, 2026, 1, 167.

[24] According to this line of interpretation, followed by Cass., Sec. VI, 1 April 2025, n. 13585, the absence of prior judicial authorisation in relation to the seizure of an electronic device does not, on the one hand, entail the inadmissibility of the evidence; rather, it gives rise to the nullity of the act. On the other hand, such a defect does not allow the invalidity to be raised where the seizure has been reviewed

This approach signals a shift towards a more robust conception of procedural guarantees in the digital context, ensuring that the balance between investigative efficiency and fundamental rights is maintained. However, a compelling question concerns the dogmatic qualification of the invalidity affecting the evidentiary seizure of digital devices ordered or executed without judicial authorisation.

Beyond the traditional concept of nullity, such invalidity may be construed as resulting from the public prosecutor's functional incompetence[25]. From this perspective, the public prosecutor lacks the functional competence to authorise or validate an investigative measure that entails a particularly serious interference with fundamental rights, whereas EU law reserves such power to an independent judicial authority. This flaw does not lie merely in the manner in which the power is exercised, but in the very attribution of the power itself. As a matter of fact, the notion of functional competence is grounded in the relationships between procedural bodies and their respective activities, even when pertaining to the same body. Compared to other forms of competence, its distinctive purpose lies in coordinating the actions of different bodies to ensure the proper administration of justice, specifying which body is responsible for issuing particular measures at each stage of the proceedings[26].

This construction offers several systematic advantages. It aligns domestic procedural law with the requirements of EU law and the Charter, reinforces the

by the *Tribunale del riesame*, since this judicial intervention ensures an effective and independent assessment of the necessity, proportionality and minimisation of the data acquisition.

[25] For the sake of completeness, reference is made to the definition set out in full by RICCIO, *La competenza funzionale nel diritto processuale penale*, Turin, 1959, 62 ff.: functional competence (or competence by procedural stages and levels) «should be understood as jurisdiction determined by reference to a procedural situation involving a relationship between judicial bodies or a relationship between activities; more precisely, as jurisdiction determined by reference to a procedural relationship between judicial bodies, which manifests itself in situations of dependency, correlation, parity, and coordination of functions, or in a relationship between the activities to be performed and the preceding activity». See also, MAZZA, *I soggetti, La procedura penale*, X ed., Turin, 2025, 108 ff.

[26] With regard to its relationship with other forms of judicial competence, see DELLA MONICA, *Competenza (Dir. proc. pen.)*, in *Enc. giur.*, Rome, 2000, 3, 18: functional competence presupposes the application of the statutory criteria for allocating jurisdiction – by subject matter, territory, and connection – and it is precisely the combination of these criteria that enables a judicial body to exercise its powers in a functional manner.

principle of separation of functions within criminal proceedings, ensures robust protection of the rights of the suspect and provides a clear framework for handling future cases involving digital investigations, thereby enhancing legal certainty[27].

On a distinct yet equally significant level, this approach logically leads to the conclusion that, in light of the public prosecutor's functional incompetence, the authority to authorize the seizure of evidence appropriately rests with the judge responsible for preliminary investigations. Such judicial oversight entails a careful preliminary assessment of compliance with EU law, particularly with the principles of purpose limitation and proportionality.

Nevertheless, this control must contend with the inherent limitations of this judicial figure within the Italian legal framework, which may compromise its capacity to exercise fully effective oversight. In fact, under criminal procedural law, the judge assigned to the investigative phase operates predominantly in a passive and subordinate capacity, serving as a guarantor within a segment of the proceedings that largely falls outside his control[28]. As a matter of law, his cognizance of the investigation is limited to what is strictly necessary for the exercise of the powers entrusted by law under Article 328(1) of the Italian Code of Criminal Procedure, functioning primarily as an "*ad acta*" judge[29].

---

[27] For this purpose, see the study by SCHIAVONE, *L' incompetenza funzionale del p.m. travolge il sequestro probatorio*, in *Cass. Pen.*, 2026, 1, 161 ff.

[28] Jurisdiction in the preliminary investigation phase revolves around two fundamental functions: control and the safeguarding of fundamental rights. Control is exercised through the monitoring of the legality of investigative activities until the conclusion of the investigation or the filing of charges, functioning in itself as a form of safeguard. The safeguarding function, in the strict sense, concerns judicial review of investigative measures that affect the fundamental freedoms of the person under investigation. For a general discussion on the topic, see FERRAIOLI, *Il ruolo di «garante» del giudice per le indagini preliminari*, Padua, 2014; GALANTINI, *Le indagini preliminari*, *La procedura penale*, X ed., Turin, 2025, 508 ff.; RUGGIERI, *La giurisdizione di garanzia nelle indagini preliminari*, Milan, 1996; VALORI, *Pubblico ministero e giurisdizione nelle indagini e nell'esercizio dell'azione penale: il punto di vista del giudice per le indagini preliminari*, in *Quest. giust.*, 2018, 1, 30 ff.

[29] In doctrinal literature, the judge is characterized as a judge of individual acts, emphasizing the distinction between exercising authority over discrete procedural steps and overseeing the investigation as a whole. During the investigative phase, the third and impartial judge, while structurally indispensable, therefore exercises powers in a highly specific and fragmented manner, acting on individual acts rather than on the entirety of the investigation. This reconstruction provides the basis for the investigation by

Doctrine has consistently depicted this judicial figure as «without eyes», due to limited awareness of investigative activities; «without arms», reflecting the lack of substantive corrective or integrative authority; and «without ears», given that decisions are frequently rendered *inaudita altera parte*, intervening chiefly on acts already filtered and prepared by the prosecutor[30].

This structural fragility is further exacerbated by a steady tendency to attribute increasing weight to the preliminary investigation phase[31], within which the public prosecutor assumes a hegemonic role, selectively filtering and privatizing investigative materials[32]. In practice, statutory safeguards have often proven insufficient to fulfil their intended purpose, resulting in a jurisdiction confined to the monitoring of discrete investigative acts. This, in turn, has given rise to the opening of selective "windows of jurisdiction", through which judicial control is exercised only episodically and fragmentarily on specific acts or procedural junctures, without amounting to a comprehensive governance of the preliminary investigation phase[33].

Taken together, these considerations show that while the judge in charge of the investigative phase constitutes the appropriate authority to authorize evi-

---

MARANDOLA, *Le finestre di giurisdizione e il giudice del procedimento*, in *Proc. pen. giust.,* 2023, 1, 7 ff.

[30] With regard to the figure of the judge for preliminary investigations in the original codified framework, NOBILI, *La nuova procedura penale. Lezioni agli studenti*, Bologna 1989, 192. See also, BECONCINI, *Verso il potenziamento del giudice per le indagini preliminari: una effettiva ridefinizione dei controlli?,* in *www.lalegislazionepenale.eu,* 6 December 2023.

[31] CAMON, *La fase che non conta e non pesa: indagini governate dalla legge?*, in *Dir. pen. proc.*, 2017, 4, 425 ff. revisiting NOBILI, *Diritti per la fase che "non conta e non pesa"*, in *Scenari e trasformazioni del processo penale*, Padua, 1988, 34; F. CASSIBA, *Le indagini preliminari fra innovazione e continuità, in Riforma Cartabia. La nuova giustizia penale*, edited by CastronuovoDonini-Mancuso-Varraso, Milan, 2023, 605.

[32] In this respect, see BACCARI, I nuovi meccanismi per superare le stasi procedimentali dovute all'inerzia del pubblico ministero, *La riforma Cartabia: codice penale, codice di procedura penale, giustizia riparativa,* edited by Spangher, Pisa, 2022, 263 ff.; SANNA, *I rimedi alla stasi delle indagini nella riforma "Cartabia", tra tutela della legalità e gigantismo delle Procure*, in *www.discrimen.it*, 21 December 2023.

[33] On this topic, see MARANDOLA, *Le finestre di giurisdizione e il giudice del procedimento*, in *Proc. pen. giust.*, 2023, 1, 7 ff. For a critical assessment of the opening of "windows of jurisdiction", see RUTA, *Il nuovo volto delle indagini preliminari ed il rischio della fuga dalla giurisdizione*, in *Quest. giust.,* 2023, 2, 23 ff.

dence seizures and to ensure compliance with EU principles, the effectiveness of such control ultimately depends on a decisive reinforcement of his role. To secure genuinely effective judicial oversight, it is therefore necessary to move beyond a model of merely episodic intervention and to further strengthen the powers and involvement of the judge responsible for preliminary investigations. In this direction, the approach outlined by the most recent reforms – characterized by the progressive opening of selective "windows of jurisdiction" – should be consolidated and developed into a more coherent framework of judicial governance of the investigative phase. Such an evolution would allow judicial control to operate as a meaningful counterbalance to prosecutorial dominance, while remaining compatible with the practical requirements of investigating complex, particularly digital, forms of criminality.

4.2. *Reconciling Investigative Needs and EU Fundamental Rights.* A recent decision of the Supreme Court adds a significant contribution to the ongoing process of implementing the principles established by the EUCJ. In particular, in its judgment No. 2218/2026, the Italian Supreme Court addresses the conditions under which law enforcement authorities may access and extract data from electronic devices in urgent circumstances, clarifying the interplay between domestic criminal procedure and EU law.

Drawing on the CJEU's judgment (Case C-548/21), the Court held that, under the Italian Code of Criminal Procedure, the judicial police may lawfully access data stored on an electronic device, including mobile phones, without prior judicial authorisation when duly substantiated urgency exists – such as situations where data might be altered, dispersed, or otherwise compromised[34]. The Supreme Court emphasized that the legality of such access under EU law depends on the availability of effective, independent, and prompt judicial review able to assess the necessity, proportionality, and scope of the measure. This model of "*ex post*" judicial control ensures that the absence of prior judicial authorisation does not automatically render the data acquisition invalid

[34] See Cass., judgment No. 2218/2026, § 2.1.

or unusable as evidence. Importantly, the Court distinguished between the immediate need for intervention and the procedural safeguards required to protect fundamental rights, thereby reconciling operational investigative requirements with the constitutional and EU law guarantees of privacy and data protection[35].

The decision also illustrates the practical application of these principles. In the case at hand, law enforcement officers accessed data on a personal computer within a commercial establishment during an institutional verification of compliance with betting regulations. The access was strictly limited to information necessary to assess the lawful conduct of betting activities and subsequent seizure of additional documents and financial instruments was performed. The Court confirmed the lawfulness and usability of the data obtained, highlighting that the procedural framework allowed for rapid judicial scrutiny through a review procedure, which effectively verified the urgency and proportionality of the intervention[36].

Overall, the ruling at issue consolidates the process of harmonizing Italian criminal procedure with EU law standards, confirming that judicial police can intervene in urgent situations to access electronic data, provided that prompt and effective judicial oversight is ensured thereafter.

5. Concluding Remarks. The digitisation of social relations and the centrality of digital devices in criminal investigations have reshaped both investigative practices and the scope of fundamental rights. EU law has responded with a framework designed to balance investigative efficiency with rights protection, embedding proportionality and purpose limitation as core guiding principles. The European Investigation Order and the "e-Evidence package" exemplify this approach, using proportionality as a filter to ensure that investigative measures are legitimate, necessary and minimally intrusive.

[35] See Cass, judgment No. 2218/2026, § 2.2.
[36] See Cass., judgment No. 2218/2026, § 2.3.

This legislative orientation is mirrored in judicial practice. The CJEU judgment of 4 October 2024 (Case C-548/21) framed access to mobile devices as a highly intrusive act requiring strict adherence to proportionality and purpose limitation. Italian Supreme Court rulings, including No. 13585/2025 and No. 2218/2026, translate these principles into practice. In particular, the former establishes the nullity of any measure ordered by the public prosecutor without prior judicial authorisation, while the latter allows urgent access to electronic data under effective and independent *ex post* judicial review, thereby ensuring that interventions are strictly necessary, proportionate, and purpose-bound.

Together, these developments underline that effective judicial oversight defines a substantive condition for lawful digital investigations. Within the Italian legal system, invoking the functional competence of the judge responsible for preliminary investigations requires that the judge's powers be meaningful and fully operative, rather than episodic. The progressive introduction of selective "windows of jurisdiction" represents a step in this direction, but to realise the full potential of judicial oversight, these powers must be consolidated into a coherent model of governance. Such reinforcement would provide a genuine counterbalance to prosecutorial dominance while accommodating the practical demands of data-driven investigations.

Ultimately, EU and domestic law converge on a single insight: the legitimacy and effectiveness of digital investigations depend on calibrating investigative powers with procedural safeguards, with judicial oversight grounded in proportionality and purpose limitation serving as the cornerstone of rights-compliant criminal justice.