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

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0282 • articolo sottoposto a peer review • pubblicato in anteprima il 20 lug. 2026

Roberto Flor – Beatrice Panattoni

Il concetto di criminalità grave e la sfida della proporzionalità nelle indagini digitali

Il contributo analizza il ruolo del principio di proporzionalità nelle indagini penali digitali, con particolare attenzione alla nozione di "criminalità grave" quale criterio di delimitazione dell'impiego degli strumenti investigativi maggiormente invasivi. Muovendo dalla giurisprudenza della Corte di giustizia dell'Unione europea, l'analisi si concentra su due *case studies* emblematici: la *data retention* e l'accesso alle comunicazioni cifrate. Mentre nel primo ambito la Corte ha progressivamente elaborato un modello di bilanciamento fondato sul rapporto tra gravità dell'ingerenza e gravità del reato perseguito, nel secondo la riflessione si è concentrata prevalentemente sulle garanzie procedurali e sull'utilizzabilità della prova. Il contributo propone una lettura integrata del principio di proporzionalità che tenga insieme diritto processuale penale, diritto della protezione dei dati personali e diritto penale sostanziale, evidenziando come la nozione di "criminalità grave" possa fungere da parametro sostanziale per orientare tanto le scelte legislative quanto il controllo giudiziale sulle investigazioni digitali.

Proporzionalità – Data Retention – Criminalità grave – Indagini digitali – Diritti fondamentali

The concept of serious crime and the challenge of proportionality in digital investigations

This paper examines the role of the principle of proportionality in digital criminal investigations, focusing on the notion of "serious crime" as a criterion for limiting the use of the most intrusive investigative powers. Drawing on the case law of the Court of Justice of the European Union, the analysis addresses two key case studies: data retention and access to encrypted communications. While the Court has progressively developed, in the field of data retention, a framework based on the relationship between the seriousness of the interference and the seriousness of the offence investigated, the debate concerning encrypted communications has mainly focused on procedural safeguards and admissibility of evidence. The article proposes an integrated understanding of proportionality combining criminal procedure, data protection law, and substantive criminal law, arguing that the notion of "serious crime" should serve as a substantive benchmark for both legislative choices and judicial review in the regulation of digital investigations.

Proportionality – Data Retention – Serious Crimes – Digital investigations – Fundamental rights

Roberto Flor è professore ordinario in diritto penale presso il Dipartimento di Scienze Giuridiche dell'Università degli Studi di Verona (autore dei par. 1 e 3)

Beatrice Panattoni è ricercatrice post doc in diritto penale presso la Faculty of Law, Economics and Finance dell'Università del Lussemburgo e docente a contratto presso il Dipartimento di Scienze Giuridiche dell'Università degli Studi di Verona (autrice dei par. 2 e 4)

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2,* a cura di Gaetana Morgante e Gaia Fiorinelli

Sommario: 1. Investigazioni digitali: bilanciamento tra lotta al crimine e tutela dei diritti fondamentali. – 2. Il *case study* della *data retention*. – 3. *Encryption, lawful hacking* e accesso alle comunicazioni cifrate: la proporzionalità nelle investigazioni su larga scala. – 4. Proporzionalità e "criminalità grave".

1. Investigazioni digitali: bilanciamento tra lotta al crimine e tutela dei diritti fondamentali

La progressiva digitalizzazione della società ha prodotto una trasformazione profonda del panorama investigativo, imponendo una riconsiderazione dei mezzi tradizionalmente impiegati nella ricerca della prova. L'aumento esponenziale dei flussi di comunicazione elettronica, la pervasività dei dispositivi digitali nella vita quotidiana e la conseguente disponibilità di enormi masse di dati hanno radicalmente mutato le modalità attraverso cui le autorità accedono alle informazioni rilevanti ai fini investigativi[1], dovendo fronteggiare forme di criminalità altrettanto segnate da una marcata digitalizzazione. Di fronte a tale scenario, è ormai indispensabile confrontarsi con una duplice esigenza: da un lato, dotare gli organi investigativi di strumenti adeguati per contrastare fenomeni criminali sempre più complessi e tecnologicamente sofisticati; dall'altro, garantire che l'esercizio di tali "poteri investigativi" avvenga nel rispetto dei diritti fondamentali e delle garanzie individuali[2].

L'impatto della trasformazione digitale sulle investigazioni penali non si esaurisce tuttavia nell'introduzione di nuovi strumenti tecnici. Più profondamente, esso investe la stessa struttura epistemica dell'accertamento penale. Il crescente patrimonio informazionale derivante dalla disponibilità di dati generati dalle attività quotidiane degli individui, ossia dai diversi processi di *datafication*, ha infatti favorito l'emersione di un nuovo paradigma investigativo, frequentemente descritto attraverso l'espressione *data-driven investigations*[3]; formula che racchiude in sé un duplice mutamento.

Da un lato, essa evidenzia come nell'ambiente digitale "*evidence is all about data*"[4]. Le attività investigative si traducono in operazioni di raccolta, conservazione, selezione, elaborazione e correlazione di informazioni digitali provenienti dalle fonti più disparate: comunicazioni elettroniche, dispositivi personali, servizi online, piattaforme sociali, sistemi di geolocalizzazione, infrastrutture cloud e banche dati pubbliche e private.

Dall'altro lato, il paradigma *data-driven* introduce una trasformazione qualitativa ancora più significativa. Le caratteristiche dell'ecosistema

1. La letteratura sul punto è ormai alquanto ampia e difficilmente riassumibile. Tra i principali riferimenti nel contesto domestico cfr. Caianiello 2025; Di Paolo–Pressacco 2025; Flor–Marcolini 2022; Caianiello 2019; Lasagni 2018. A livello europeo cfr. Vavoula 2026; Oerlemans–Royer 2023; Bachmaier Winter 2022. Tra le ricerche empiriche cfr. Lavorgna–Ugwudike 2021.
2. Sachoulidou 2026; Lasagni 2018.
3. In particolare, le ultime frontiere del tema hanno portato la comunità scientifica ad interrogarsi sull'impatto dell'impiego dei sistemi di intelligenza artificiale nel contesto delle indagini penali. Anche su questo la letteratura è ormai numerosa. Tra i più recenti si vedano i contributi raccolti in Ligeti 2026.
4. Cfr. l'editorale di Galič–Stevens–Koops 2023, e i contributi raccolti nella *special issue* di "New Journal of European Criminal Law", 14(4), 2023.

digitale rendono infatti meno centrale, o addirittura ostacolano, la ricerca mirata di informazioni relative a fatti e soggetti determinati e favoriscono, invece, la raccolta preventiva e generalizzata di enormi quantità di dati, da analizzare successivamente attraverso tecniche automatizzate. La logica dell'investigazione tende così a spostarsi dall'individuazione reattiva di prove riferibili a un reato commesso e ad un sospettato già identificato verso la costruzione preventiva di una più ampia *information position* – quale tecnica derivante propriamente dalle attività di *intelligence*[5] – funzionale non soltanto all'accertamento di reati già realizzati, ma anche all'individuazione preventiva di rischi e minacce[6]. La trasformazione in atto implica quindi un parziale mutamento della razionalità investigativa. Nelle investigazioni digitali contemporanee, la disponibilità di grandi quantità di dati consente spesso di individuare correlazioni, schemi comportamentali e profili di rischio. L'attenzione tende così a spostarsi dalla ricostruzione di eventi già verificatisi alla costruzione di una conoscenza preventiva del fenomeno criminale. In tale prospettiva, le investigazioni digitali acquisiscono sempre più frequentemente, per l'appunto, la veste di attività di *intelligence*, in un contesto che si caratterizza per una imprescindibile vocazione transnazionale.

La possibilità di raccogliere e conservare preventivamente enormi quantità di dati di traffico, dati di localizzazione e, in alcuni casi, persino dati relativi al contenuto delle comunicazioni, accentua ulteriormente tale tendenza. Il modello della sorveglianza mirata (*targeted surveillance*), costruito attorno a uno specifico soggetto o a uno specifico fatto di reato, tende progressivamente a confrontarsi con pratiche di raccolta generalizzata delle informazioni che, pur perseguendo finalità investigative legittime, presentano tratti riconducibili a una c.d. *mass surveillance*. La distinzione tra raccolta selettiva e raccolta indiscriminata dei dati diviene pertanto meno netta rispetto al passato, con conseguenze particolarmente rilevanti sul piano delle garanzie individuali[7].

Il grado di invasività delle investigazioni digitali risulta infatti strutturalmente più incisivo rispetto a quello delle tecniche investigative "convenzionali". Come ha chiarito la Corte di giustizia dell'Unione europea (CGUE) in diverse occasioni, la raccolta massiva di dati di traffico e localizzazione – anche a prescindere dall'accesso al contenuto delle comunicazioni – può consentire di trarre conclusioni assai precise sulla vita privata delle persone interessate, incluse le loro abitudini, i loro luoghi di residenza, gli spostamenti quotidiani, le attività svolte, nonché le relazioni personali e l'ambiente sociale[8]. In questo contesto assume particolare rilievo il quadro di tutela offerto dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza), considerato come le investigazioni digitali incidano dunque sulla tutela del diritto al rispetto della vita privata e familiare e sul diritto alla protezione dei dati personali, rendendo necessario un sistema di garanzie che tenga conto della specifica capacità informativa delle tracce digitali generate dagli individui.

Le investigazioni digitali pongono pertanto un problema di "traduzione"[9] delle regole tradizionali. Come è stato osservato, l'avvento delle tecnologie digitali impone di ripensare le basi teoriche dei diritti e delle libertà protette dalle Carte europee, al fine di elaborare regole procedurali capaci di garantire un adeguato livello di tutela nell'ambiente digitale[10]. Si tratta, peraltro, di una questione che coinvolge la maggior parte degli ordinamenti,

5. Si parla infatti di "intelligence-led policing". Cfr. Goldstein 1990.
6. Cfr. de Jonge–de Vries 2024.
7. Su questo cfr. Mitsilegas–Guild–Kuskonmaz–Vavoula 2023.
8. Si vedano riferimenti in par. 2 e 3.
9. Come evidenzia Caianiello 2019, richiamando Washington–Richards 2019: la rivoluzione digitale "squarely presents the problem of translation for constitutional rules. It requires courts to answer the question how (or if) we will translate our hard-won protections of civil liberties into the digital environment […] Translating ancient principles and doctrines to emerging technologies such as the cloud, location tracking, and encryption has proven so difficult as to threaten civil liberties themselves. One way or another, our response to this challenge will become our generation's defining legacy of civil liberties".
10. Lasagni 2018.

compresi quelli oltreoceano, come l'ordinamento statunitense, in cui da tempo sono emerse analoghe riflessioni, che hanno evidenziato come la crescente difficoltà di applicare categorie elaborate per il mondo analogico a fenomeni caratterizzati dalla continua produzione e circolazione di informazioni digitali debba condurre al ripensamento di alcuni istituti e diritti[11].

In questo tentativo di "traduzione", quindi, vi sono due questioni particolarmente rilevanti con cui occorre interfacciarsi: quella dell'atipicità e quella della proporzionalità.

Per quanto riguarda la prima, ossia l'atipicità che può connotare questi mezzi investigativi, si osserva come gli strumenti investigativi vigenti – *rectius* i mezzi di ricerca della prova – pensati in un'epoca in cui le comunicazioni assumevano forme ben definite e le tracce dell'attività umana erano prevalentemente materiali, possano rivelarsi inadeguati a disciplinare la complessità e la varietà delle tecniche investigative digitali attualmente disponibili. Ne risultano significativi deficit in punto di legalità, che si manifestano non soltanto nell'assenza di un quadro normativo organico, ma anche nell'inadeguatezza delle categorie concettuali tradizionali a cogliere la specificità dell'atto digitale[12]. Questa circostanza pone questioni non solamente in relazione alle modalità d'acquisizione, ma anche in relazione alla quantità e alla qualità delle informazioni che possono essere ricavate da tali attività. Un ulteriore elemento distintivo consiste, infatti, nel potenziale coinvolgimento di una pluralità di soggetti estranei al procedimento. Le tecniche di raccolta massiva di dati incidono frequentemente su persone che non rivestono la qualità di indagati e che non risultano in alcun modo collegate ai fatti oggetto di accertamento. Le informazioni raccolte possono riguardare interlocutori occasionali, utenti appartenenti alla medesima piattaforma digitale, soggetti geograficamente prossimi alla persona investigata o, più in generale, individui i cui dati vengono acquisiti incidentalmente nel corso delle operazioni investigative[13].

Il panorama delle investigazioni digitali appare inoltre estremamente eterogeneo. Risulta alquanto complesso ricomprendere in un quadro sistematico il ricco insieme di attività che possono essere ricondotte entro il cappello di "indagini digitali", considerato che ognuna di esse pone poi questioni assai tecniche e specifiche. Volendo fare uno sforzo di sintesi, rientrano in questo insieme attività d'indagine digitale occulte (come è il caso del controllo occulto dei dispositivi, ossia il c.d. *lawful hacking*), palesi (come sono i sequestri informatici), attività di *open source intelligence* (come le stesse *social network analysis*), attività d'indagine che si servono di sistemi di intelligenza artificiale, così come attività di cooperazione con attori privati, e in particolare, con *online service providers*, a cui possono essere rivolti ordini di produzione di dati in loro possesso. A ciò si aggiunge la dimensione frequentemente transnazionale che caratterizza tali operazioni, con le conseguenti trasmissioni e scambi di ingenti dataset tra autorità appartenenti a ordinamenti diversi.

Non è tuttavia su queste specifiche attività, e sull'atipicità che le può connotare in relazione ai mezzi di ricerca della prova disciplinati dal codice di procedura penale, che si soffermerà l'analisi. Adottando una prospettiva interdisciplinare, che tenga conto non soltanto del diritto processuale penale ma anche del diritto della protezione dei dati personali e del diritto penale sostanziale, l'attenzione sarà rivolta alla seconda questione appena richiamata, ossia quella attinente alla proporzionalità quale parametro di legittimità dell'azione investigativa digitale. Studi recenti hanno iniziato a valorizzare la necessità di creare un dialogo interdisciplinare sul punto tra diritto processuale penale e diritto della protezione dei dati personali, valorizzando il contributo che quest'ultimo può offrire nella definizione dei limiti all'esercizio dei poteri investigativi[14]. A tale prospettiva può essere affiancata una terza dimensione, rappresentata dal diritto penale sostanziale, poiché la delimitazione dei poteri investigativi più invasivi presuppone inevitabilmente una scelta circa i fenomeni criminali che giustificano il sacrificio dei diritti fondamentali coinvolti, assicurando al contempo l'*habeas data*, inteso quale

11. Kerr 2024.
12. Cfr. Nicolicchia 2024; Škorvánek–Koops–Newell–Roberts 2019; Newell–Timan–Koops 2018.
13. Cfr. par. 3.
14. Galič–Stevens–Koops 2023.

base fondativa dei diritti di libertà della persona nella dimensione immateriale dell'infosfera[15].

Il principio di proporzionalità, quale concetto e categoria polimorfica che esprime un approccio relazionale volto al bilanciamento armonioso tra punti contrapposti[16], nel contesto che qui interessa svolge una funzione di bilanciamento tra l'efficienza dell'accertamento penale e la tutela dei diritti individuali[17]. Esso viene definito, nell'ordinamento multilivello, attraverso il riferimento all'art. 52 della Carta di Nizza, il quale richiede che limitazioni all'esercizio di diritti e libertà siano previste dalla legge, necessarie, rispondano effettivamente a finalità di interesse generale (come è la lotta al crimine)[18]. Viene poi articolato, più nello specifico nell'ambito della procedura penale, nei sub-criteri della idoneità, necessità e proporzionalità in senso stretto[19].

Tale parametro non opera tuttavia soltanto come criterio applicativo, ma assume anche forti declinazioni politico criminali. Esso presuppone una scelta di fondo circa le forme di criminalità rispetto alle quali le ingerenze investigative più penetranti possono essere considerate tollerabili in una società democratica, con conseguenti ricadute sul concetto, indeterminato e controverso, di ciò che intendiamo con "criminalità grave".

Come si vedrà, infatti, la progressiva emersione della nozione di "criminalità grave" nella giurisprudenza europea appare, sotto questo profilo, particolarmente significativa. Quanto maggiore è la capacità intrusiva dello strumento investigativo, tanto più forte diviene l'esigenza di circoscriverne l'utilizzo a fenomeni criminali ritenuti particolarmente lesivi degli interessi fondamentali della collettività. Il problema si sposta così dall'individuazione della misura investigativa alla definizione dell'obiettivo che può giustificarla.

Entro questa cornice, il presente contributo si propone di analizzare, muovendo dalla giurisprudenza europea, le recenti linee evolutive che caratterizzano la proporzionalità nelle investigazioni digitali, con particolare riguardo al ruolo assunto dalla nozione di "criminalità grave" quale criterio selettivo dell'intensità dell'interferenza investigativa ammissibile. A tal fine, dopo aver esaminato i *case studies* dati da due ambiti particolarmente rilevanti nel contesto delle indagini digitali, ossia quello della *data retention* e quello delle comunicazioni *encrypted* (par. 2 e 3), si procederà a una valutazione della funzione della nozione di criminalità grave all'interno del test di proporzionalità (par. 4).

2. Il *case study* della *data retention*

Un primo osservatorio privilegiato per analizzare il rapporto tra investigazioni digitali, tutela dei diritti fondamentali e principio di proporzionalità è rappresentato da un settore particolare della cooperazione tra pubblico e privato e, nello specifico, dagli ordini di produzione di dati che possono essere inviati a fornitori di servizi telematici e dalla disciplina della conservazione dei dati di traffico delle comunicazioni elettroniche, comunemente nota come *data retention*. Tale ambito assume particolare rilevanza non soltanto per il ruolo centrale che i dati di traffico svolgono nelle indagini, ma anche perché è proprio in questo settore che la CGUE ha elaborato, nel corso dell'ultimo decennio, una ricca giurisprudenza.

Come noto, si tratta di una materia segnata da una movimentata evoluzione. Il punto d'inizio è stato segnato dalla disciplina originariamente prevista dalla direttiva 2006/24/CE (c.d. Data Retention Directive), poi invalidata dalla famosa sentenza *Digital Rights*, dove si è affermato che la conservazione generalizzata dei dati di traffico e localizzazione relativi alle comunicazioni effettuate dagli utenti sia contraria al principio di proporzionalità[20]. Si è infatti inizialmente chiarito come non sia sufficiente che una misura limitativa dei diritti fondamentali sia prevista dalla legge e che

15. Cfr. Di Paolo 2024.
16. Billis–Knust–Rui 2021; Lacey 2016; Cognetti, 2011; Hickman 2008.
17. Cfr Caianiello 2025; Caianiello 2014.
18. Si tornerà più diffusamente sul punto nel par. 4.
19. Caianiello 2014.
20. C. giust. UE, 8 aprile 2014, *Digital Rights Ireland Ltd*, C-293/12 e C-594/12, par. 34, 36, 42, 38, 54. Cfr. Flor–Marcolini 2022; Formici 2021; Marcolini 2019; Fabbrini 2015; Flor 2014.

persegua un obiettivo legittimo di interesse generale, ma occorra altresì verificare se il legislatore abbia predisposto un sistema sufficientemente preciso e dettagliato di garanzie idonee a circoscrivere l'ingerenza entro quanto strettamente necessario al perseguimento delle finalità perseguite.

A partire da tale sentenza è poi iniziato un lungo percorso giurisprudenziale nel quale la CGUE ha progressivamente affinato i criteri di legittimazione del regime della *data retention*[21], con numerose ricadute nei diversi ordinamenti europei, i quali hanno portato a recenti dettagliati studi comparati sul punto[22].

Dalla giurisprudenza europea emerge come il collegamento tra gravità dell'ingerenza derivante dal regime di *data retention* e gravità del reato perseguito assuma una formulazione particolarmente esplicita. La Corte afferma infatti in diverse occasioni che una grave interferenza nei diritti fondamentali garantiti dagli artt. 7 e 8 della Carta può essere giustificata soltanto da obiettivi di lotta contro forme gravi di criminalità, dove quindi il principio della "minima interferenza" nei diritti fondamentali violati nel raggiungimento dello scopo può e deve dirsi "contenutistico", nel senso che per rispettarlo non è sufficiente che trovi una cornice formale nel diritto positivo, ma occorre investigare come il legislatore abbia esercitato la riserva di legge formale[23].

Dalle critiche volte alla Data Retention Directive, che consentiva l'esercizio del diritto di accesso delle autorità pubbliche per reati genericamente definiti come "gravi", con inaccettabile rinvio per la specificazione di tale concetto ai legislatori nazionali[24], si è iniziato a raffinare questa categoria in sentenze successive. Si è affermato che "in conformità al principio di proporzionalità, una grave ingerenza può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come 'grave'"[25]. Nel caso *La Quadrature du Net 'I'* si è delineata una gerarchia tra gli obiettivi di interesse pubblico che possono giustificare una restrizione nella protezione dei diritti, distinguendo tra esigenze di sicurezza nazionale, ordine pubblico e lotta contro il "*serious crime*", evidenziando come quest'ultimo non possa essere equiparato a minacce alla sicurezza nazionale, che tradizionalmente legittimano forme più intense d'attività di *intelligence*[26].

All'interno di questo percorso evolutivo si arriva così alla recente sentenza della CGUE del 30 aprile 2024[27], che ha coinvolto in particolare l'ordinamento italiano e la disciplina interna in materia di *data retention*[28]. La pronuncia trae infatti origine da un rinvio pregiudiziale promosso dalla Procura di Bolzano nell'ambito di un procedimento riguardante alcuni episodi di furto di telefoni cellulari, in

21. Sulle vicissitudini che hanno caratterizzato l'ambito e l'interpretazione dell'obbligo di *data retention* e, in particolare, la copiosa giurisprudenza europea che si è pronunciata in punto, si è già dedicato un altro contributo nel presente fascicolo, cfr. Bonetti 2026, a cui si rimanda, il quale approfondisce in particolare il tema da una prospettiva privatistica, confermando così la necessità di un approccio interdisciplinare al tema, che consideri le specificità della materia della protezione dei dati personali.
22. Kosta–Kamara 2025.
23. Flor–Marcolini 2022.
24. C-293/12 e C-594/12, cit., par. 60: "la suddetta mancanza generale di limiti si aggiunge il fatto che la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Al contrario, la direttiva 2006/24 si limita a rinviare, all'articolo 1, paragrafo 1, in maniera generale ai reati gravi come definiti da ciascuno Stato membro nel proprio diritto interno".
25. C. giust. UE, 18 gennaio 2018, *Ministerio Fiscal*, C-270/16, par. 56.
26. C. giust. UE, 6 ottobre 2020, *La Quadrature du Net et al.*, C-511/18, C-512/18, C-520/18, par. 61-63. Cfr. Mitsilegas 2026.
27. C. giust. UE, 30 aprile 2024, *Ignoti c. Italia*, C-178/22.
28. Cfr. i commenti alla sentenza: Parodi 2025; Dalla Torre 2024; Albanese 2024; Grisonich 2024; Marino 2024.

cui, nel corso delle indagini, il PM aveva richiesto l'autorizzazione all'acquisizione dei dati conservati dagli operatori telefonici ai sensi dell'art. 132, comma 3, del d.lgs. n. 196/2003 (codice privacy). Nello specifico si era richiesto di acquisire "tutti i dati in possesso delle compagnie, con metodo di tracciamento e localizzazione, chiamati/chiamanti, siti visitati/raggiunti, orario e durata della chiamata/connessione (…)"[29], quindi, sia dati relativi al traffico, sia dati relativi all'ubicazione, i quali permettono evidentemente di trarre precise conclusioni sulla vita privata dei titolari, qualificandosi come ingerenza grave nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta.

La possibilità di procedere in tal senso è dovuta al fatto che la disciplina italiana dell'art. 132 comma 3 prevede che le autorità possano procedere con la richiesta di acquisizione dei dati conservati dai *provider* nel caso in cui le indagini riguardino reati per i quali si prevede la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, così come per i reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, nel caso in cui la minaccia, la molestia e il disturbo siano gravi, nel caso in cui tali dati siano rilevanti per l'accertamento dei fatti o per le ricerche di un latitante.

La soglia dei tre anni dunque permette che rientrino nell'ambito di applicazione di questo strumento investigativo anche "reati che destano solo scarso allarme sociale e che sono punitivi solo a querela di parte"[30], come i furti di scarso valore (ossia quelli che interessavano il caso di specie), senza che il giudice italiano disponga di un sufficiente margine di discrezionalità per negare l'autorizzazione in questi casi, dal momento che è sufficiente, affinché venga rilasciata, essere in presenza di "sufficienti indizi", e che i dati richiesti "siano rilevanti ai fini dell'accertamento del reato". Attraverso il rinvio alla CGUE si è dunque sollevata la conformità al diritto europeo della disciplina italiana, e in particolare il fatto che la formulazione adottata non lasci ai giudici un margine di valutazione in ordine alla concreta gravità del reato oggetto d'indagine.

Nella sua decisione, la CGUE ribadisce anzitutto il proprio orientamento, ormai consolidato, secondo cui l'accesso ai dati di traffico e localizzazione costituisce una grave ingerenza nei diritti garantiti dagli artt. 7 e 8 della Carta e può pertanto essere giustificato soltanto da obiettivi di lotta contro forme gravi di criminalità o di prevenzione di gravi minacce alla sicurezza pubblica[31]. Tuttavia, la parte più interessante della pronuncia riguarda il tentativo di precisare il contenuto della nozione di "*serious crime*".

La CGUE prende parzialmente posizione sul punto. Coscienziosamente, viene ribadito che la competenza sul punto spetta e rimane in capo agli Stati membri, ma si specifica che essa deve essere esercitata nel rispetto del diritto dell'Unione. Nello specifico, si afferma che gli ordinamenti nazionali non possono "'snaturare' la nozione di 'reato grave', e, per estensione, quella di 'grave criminalità', includendovi reati che manifestamente non sono gravi, alla luce delle condizioni sociali esistenti nello Stato membro interessato, sebbene il legislatore di tale Stato abbia previsto di punirlo con la pena della reclusione non inferiore nel massimo a tre anni"[32].

È proprio su questo punto che emerge con particolare evidenza la duplice dimensione del giudizio di proporzionalità. Da un lato, vi è una dimensione astratta, affidata al legislatore, il quale individua *ex ante* le categorie di reati ritenute sufficientemente gravi da giustificare determinate forme di interferenza investigativa. Dall'altro lato, permane una dimensione concreta, che richiede una valutazione della specifica fattispecie oggetto di indagine e dell'effettiva gravità del fatto rispetto all'ingerenza richiesta. La sentenza sembra dunque suggerire che il rispetto del principio di proporzionalità non possa essere assicurato esclusivamente mediante il ricorso a soglie legislative fondate sulla pena edittale, per quanto venga allo stesso tempo affermato che la tecnica di fissazione di soglie a partire dalla pena massima per giustificare che il reato sia qualificato come grave "non è necessariamente

29. C-178/22, cit., par. 17.
30. *Ivi*, par. 21.
31. *Ivi*, par. 42.
32. *Ivi*, par. 50.

contraria al principio di proporzionalità"[33] (anche se rimane la criticità della mancata considerazione del limite della pena minima)[34].

Seppur, dunque, un criterio oggettivo rimanga imprescindibile, in quanto capace garantire un minimo livello di prevedibilità e certezza del diritto, viene evidenziato come, da solo, rischi di risultare eccessivamente rigido, ove non accompagnato dalla possibilità di una valutazione in concreto della gravità della fattispecie – come peraltro ritroviamo espresso anche nella giurisprudenza domestica[35].

La difficoltà principale risiede tuttavia nel parametro individuato dalla Corte per orientare tale valutazione. Il riferimento a reati "manifestamente non gravi alla luce delle *condizioni sociali* esistenti nello Stato membro interessato" appare infatti caratterizzato da un elevato grado di indeterminatezza. Non risulta immediatamente chiaro quali siano le "condizioni sociali" rilevanti, né quali criteri il giudice debba utilizzare. Osservazioni interessanti si possono invece ricavare dalle conclusioni dell'Avvocato generale, che suggeriva di utilizzare un criterio meglio definito, quale quello delle "circostanze che caratterizzano lo specifico caso di cui trattasi", compresi i danni causati alle vittime di reato e i rischi per i terzi coinvolti[36]. Il rischio derivante da una simile formulazione è dunque quello di attribuire al giudice un margine di discrezionalità particolarmente ampio, suscettibile di incidere sulle stesse scelte di politica criminale compiute dal legislatore[37].

Le ricadute che questa pronuncia della CGUE avranno nel contesto interno riguarderanno infatti la possibilità per i giudici interni di compiere un autonomo sindacato di proporzionalità in concreto sulla gravità del reato seguendo un criterio così indeterminato; possibilità che secondo alcuni commenti dovrebbe essere negata, preferendo piuttosto attendere un intervento chiarificatore del legislatore o un coinvolgimento della Corte Costituzionale, anche attraverso un ulteriore rinvio alla CGUE che chieda di esplicitare in modo più preciso tale criterio[38], mentre altre voci lasciano aperta tale possibilità per i giudici nazionali[39].

Nonostante le criticità rilevate, la pronuncia della CGUE mette bene in luce la centralità della delimitazione di ciò che può definirsi "criminalità grave", con evidenti ricadute sia in sede di politica criminale, in relazione alla disciplina di mezzi investigativi tecnologicamente connotati e altamente intrusivi, sia in sede giudiziale, in relazione alla applicazione del c.d. test di proporzionalità. Il caso della *data retention* mostra dunque con particolare chiarezza come la proporzionalità operi attraverso l'individuazione di criteri sufficientemente rigorosi per stabilire quali forme di criminalità siano in grado di giustificare il sacrificio dei diritti fondamentali coinvolti. È proprio quest'ultimo profilo a costituire il punto di collegamento con il successivo ambito di analisi, relativo all'accesso alle comunicazioni cifrate, nel quale il rapporto tra gravità dell'ingerenza e gravità del reato appare assai meno definito rispetto a quanto avvenuto nel settore appena richiamato.

3. *Encryption*, *lawful hacking* e accesso alle comunicazioni cifrate: la proporzionalità nelle investigazioni su larga scala

Se il settore della *data retention* costituisce il principale laboratorio entro cui la CGUE ha progressivamente elaborato il rapporto tra gravità dell'ingerenza investigativa e gravità del reato perseguito, un secondo osservatorio particolarmente significativo è rappresentato dalle investigazioni aventi ad oggetto comunicazioni protette da sistemi di cifratura (*encryption*). Anche in questo ambito emerge con forza la tensione tra esigenze investigative e tutela dei diritti fondamentali. Diversamente da quanto avviene nel caso della

33. *Ivi*, par. 58.
34. *Ivi*, par. 57.
35. Cfr. Cass. pen., sez. III, 25 settembre 2019, n. 48737, in "OneLegale", dove si evidenzia che tale principio "mal si presta ad una preventiva, rigida codificazione".
36. Cfr. Conclusioni dell'avvocato generale A.M. Collins, presentate l'8 giugno 2023.
37. Dalla Torre 2024.
38. *Ibidem*.
39. Albanese 2024; Todaro 2024.

conservazione dei dati di traffico, tuttavia, la questione si presenta in termini in parte differenti, poiché il problema non riguarda soltanto l'accesso a informazioni già detenute da soggetti privati, ma investe la possibilità stessa di superare le barriere tecnologiche predisposte a tutela della riservatezza delle comunicazioni direttamente da parte delle autorità pubbliche.

La cifratura costituisce oggi una delle principali infrastrutture tecnologiche della sicurezza digitale. Attraverso la trasformazione delle informazioni in dati intelligibili esclusivamente ai soggetti autorizzati, essa garantisce la riservatezza delle comunicazioni, la protezione dei dati personali, la sicurezza delle transazioni economiche e, più in generale, l'affidabilità dell'ambiente digitale. Essa rappresenta uno strumento essenziale per la protezione della vita privata nell'ambiente digitale. Come è stato osservato, la cifratura contribuisce alla creazione di una vera e propria "zona di privacy", funzionale all'esercizio di diritti fondamentali quali la libertà di opinione e di espressione[40].

Proprio perché svolge una funzione cruciale nella tutela dei diritti individuali, l'*encryption* pone questioni particolarmente delicate sotto il profilo investigativo. Le autorità di contrasto si confrontano infatti con una crescente diffusione di servizi e dispositivi caratterizzati da elevati livelli di protezione crittografica, che possono rendere estremamente complesso l'accesso alle comunicazioni rilevanti ai fini probatori. Tale fenomeno emerge con evidenza nei noti casi di *EncroChat*[41] e *Sky ECC*[42], che hanno rappresentato alcune delle più vaste operazioni investigative digitali realizzate in Europa negli ultimi anni. Entrambe le piattaforme offrivano servizi di comunicazione fortemente protetti mediante cifratura end-to-end e ulteriori funzionalità volte a rafforzare l'anonimato degli utenti. Pur essendo formalmente accessibili a chiunque, esse risultavano frequentemente utilizzate nell'ambito di attività riconducibili alla criminalità organizzata transnazionale e al traffico internazionale di stupefacenti.

Le indagini condotte dalle autorità francesi hanno consentito di acquisire l'accesso alle infrastrutture tecnologiche di tali servizi mediante tecniche di *lawful hacking*, permettendo la raccolta di enormi quantità di comunicazioni successivamente condivise con numerose autorità investigative europee. Nel caso *EncroChat*, le autorità sono riuscite ad acquisire centinaia di milioni di messaggi; nel caso *Sky ECC*, il numero delle comunicazioni raccolte ha superato il miliardo. I dati ottenuti sono stati successivamente oggetto di processi di selezione e analisi automatizzata attraverso ricerche per parole chiave, sistemi di correlazione e altre tecniche tipiche delle investigazioni *data-driven*.

Tali casi si inseriscono dunque appieno nel quadro appena delineato sollevando la questione attinente al bilanciamento tra l'esigenza di accesso ai dati da parte delle autorità pubbliche e la tutela di infrastrutture digitali progettate per garantire la riservatezza delle comunicazioni e quindi la sicurezza dell'ecosistema digitale, senza considerare le problematiche relative ai modelli di "trasferimento probatorio" e di "raccolta transnazionale della prova" (che non sono oggetto specifico del presente studio).[43]

A differenza delle tradizionali intercettazioni, l'oggetto dell'intervento investigativo non coincide con una singola comunicazione o con uno specifico soggetto previamente individuato. L'operazione

40. Kaye 2015.

41. C. giust. UE, 30 aprile 2024, *M.N. (EncroChat)*, C-670/22; C. giust. UE, 4 luglio 2024, *M.R.*, C-288/24; Corte EDU, 17 ottobre 2024, *A.L. e E.J. c. Francia*, ric. nn. 44715/20 e 47930/21. Cfr. Bajović–Ćorić 2025; Lassalle–Lannier 2025.

42. Oerlemans–Royer 2023.

43. Si rinvia a Di Paolo 2024. L'Autrice evidenzia "l'eterno problema – dovuto al fatto che manca a tutt'oggi un'armonizzazione, seppur minima, delle discipline probatorie nazionali – è quello della utilizzabilità della prova allogena e, a monte, quello della disciplina applicabile per la sua raccolta (*lex loci* o *lex fori*). Si tratta di una criticità in parte affievolita dall'ibridismo che connota il sistema dell'ordine europeo di indagine penale (O.E.I.), nell'ambito del quale, per assicurare la spendita del 'risultato' probatorio raccolto *ultra fines*, si prevede espressamente la possibilità che la prova sia confezionata dall'autorità di esecuzione secondo le "indicazioni" formali e procedurali richieste dall'autorità emittente, con sostanziale prevalenza della *lex fori*. Altro aspetto degno di nota è l'espresso riferimento, nella direttiva relativa all'O.E.I., al principio di proporzionalità, elevato a parametro di controllo sulla legittimità dell'attività probatoria richiesta, sia per l'autorità di emissione che per l'autorità di esecuzione".

investe invece un'intera infrastruttura comunicativa – si parla infatti di *bulk interception* – consentendo l'acquisizione simultanea delle comunicazioni generate da migliaia di utenti[44]. Diviene così sempre più complesso distinguere tra singole acquisizioni investigative e formazione progressiva di grandi patrimoni informativi suscettibili di impieghi successivi. Il rischio è che la nozione stessa di raccolta massiva finisca per perdere capacità selettiva, dal momento che quasi ogni indagine digitale produce oggi dataset potenzialmente riutilizzabili per ulteriori finalità investigative.

Questi casi hanno suscitato lunghe e complesse vicende giudiziali nell'ambito di diversi ordinamenti europei, dal momento che i dati collezionati dalle autorità francesi sono poi stati oggetti di trasferimenti transfrontalieri in diversi ordinamenti, come quello tedesco, olandese, inglese e anche italiano, fino poi ad arrivare, in alcuni casi, anche alle corti europee[45]. Molto clamore queste vicende hanno suscitato in relazione alla questione delle salvaguardie procedurali e i diritti di difesa che dovrebbero essere garantiti durante queste investigazioni, nonché al nodoso problema dell'ammissibilità della prova in un contesto di investigazioni *cross-border*.

In tale contesto, il principio di proporzionalità assume dunque una funzione centrale, anche e soprattutto in relazione alla protezione dei terzi che risultano coinvolti nelle attività investigative, imponendo di valutare non solo l'impatto delle misure adottate sui diritti degli utenti e sulle caratteristiche del servizio oggetto dell'intervento, ma anche la gravità dei reati perseguiti. In questo contesto particolare rilievo assumono quindi non solo il momento dell'acquisizione dei dati, ma soprattutto le lavorazioni eseguite a posteriori, ossia i criteri con i quali l'accusa seleziona progressivamente i dati rilevanti per le indagini, evidenziando come la proporzionalità debba essere garantita sempre non solo *ab initio*, ma anche *in itinere*: prospettiva che, come è stato evidenziato, sembra essere stata messa in secondo piano dalle difese nelle sentenze domestiche sul caso *Sky ECC*, dove ci si è prevalentemente concentrati sull'utilizzo dell'algoritmo di decrittazione[46].

Il dibattito sviluppatosi attorno a tali vicende si è naturalmente concentrato prevalentemente sulle garanzie procedurali. Le principali questioni affrontate hanno riguardato la qualificazione giuridica delle attività compiute dalle autorità straniere, i presupposti per il trasferimento transfrontaliero dei dati, i diritti della difesa e le condizioni di utilizzabilità delle informazioni raccolte; mentre limitata attenzione è stata invece dedicata al tema delle condizioni sostanziali che dovrebbero giustificare il ricorso a forme investigative caratterizzate da un livello di intrusività così elevato. La CGUE ricorre alla proporzione solamente per minacciare la conseguente esclusione della prova nel caso in cui sia stata preclusa alla difesa la possibilità di commentare le prove digitali prodotte dall'accusa[47].

Sotto questo profilo emerge una significativa differenza rispetto all'evoluzione registrata nel settore della *data retention*. Come si è visto, in quel contesto la giurisprudenza europea sta progressivamente costruendo un sistema di garanzie fondato anche sul rapporto tra gravità dell'ingerenza e gravità della criminalità perseguita. Nei casi relativi alle comunicazioni cifrate, invece, la nozione di "criminalità grave" è rimasta sostanzialmente sullo sfondo del dibattito giuridico. La circostanza appare particolarmente significativa se si considera che le operazioni *EncroChat* e *Sky ECC* sono state giustificate proprio in ragione del coinvolgimento di fenomeni riconducibili alla criminalità organizzata transnazionale e al traffico internazionale di stupefacenti. In altri termini, le autorità investigative hanno operato all'interno di un contesto caratterizzato dalla presenza di forme di criminalità unanimemente considerate particolarmente gravi. Tale dato fattuale ha probabilmente contribuito a ridurre l'attenzione verso la necessità di elaborare criteri generali idonei a delimitare il ricorso a tali strumenti investigativi.

44. Oerlemas–van Toor 2022. Interessante in questo senso anche il caso *Podchasov v. Russia*, Cfr. Corte EDU, 13 febbraio 2024, appl. 33696/19; nonchè il caso *Big Brother Watch and Others v. the United Kingdom*, Corte EDU, 25 maggio 2021, appl. 58170/13, 62322/14, 24960/15.

45. Lassalle–Lannier 2025.

46. Caianiello 2025.

47. C-670/22, cit. Cfr. Panzavolta–Maes 2022.

Tuttavia, proprio la straordinaria capacità intrusiva di queste tecniche suggerirebbe la necessità di una riflessione più approfondita sul rapporto tra gravità dell'ingerenza e gravità del reato perseguito. Quanto maggiore è la capacità di uno strumento investigativo di incidere simultaneamente sui diritti di un elevato numero di soggetti, tanto più forte dovrebbe essere l'esigenza di circoscriverne l'utilizzo a fenomeni criminali dotati di particolare offensività.

Il rischio che si rimanga silenti a livello europeo sul punto è che tale questione sia affrontata in modo frammentato dai diversi ordinamenti nazionali. In questa prospettiva, alcuni spunti possono essere ricavati dalle discipline nazionali che regolano il ricorso ai captatori informatici[48]. Anche nell'ordinamento italiano, infatti, l'utilizzo delle forme investigative tecnologicamente più invasive è generalmente subordinato alla presenza di specifiche categorie di reati considerate particolarmente gravi dal legislatore. Pur trattandosi di contesti normativi differenti, tale modello evidenzia come la delimitazione sostanziale delle finalità investigative costituisca uno strumento essenziale per garantire il rispetto del principio di proporzionalità.

Le vicende relative alle comunicazioni cifrate mostrano dunque un quadro per molti aspetti ancora incompleto. Se la giurisprudenza europea ha sviluppato una teoria relativamente articolata della proporzionalità nell'ambito della *data retention*, analoga elaborazione non sembra essersi ancora consolidata con riguardo alle tecniche di accesso a comunicazioni protette da sistemi di cifratura[49]. Il dibattito continua a concentrarsi prevalentemente sulle garanzie procedurali e sull'utilizzabilità delle prove raccolte, mentre rimane in larga misura aperta la questione relativa alle condizioni sostanziali che possono giustificare il ricorso a forme di acquisizione massiva delle comunicazioni digitali.

Il confronto tra i due *case studies* evidenzia così una significativa asimmetria. È proprio questa asimmetria che conduce alla questione conclusiva del presente contributo: quale funzione debba assumere la nozione di "criminalità grave" all'interno del test di proporzionalità nelle investigazioni digitali e quali criteri possano orientarne una definizione sufficientemente determinata e compatibile con le esigenze di tutela dei diritti fondamentali.

4. Proporzionalità e "criminalità grave"

Le considerazioni svolte nei paragrafi precedenti mostrano come il principio di proporzionalità rappresenti oggi il principale criterio di legittimazione delle investigazioni digitali. La crescente capacità delle tecnologie investigative di incidere sulla sfera privata degli individui rende infatti insufficiente una prospettiva fondata esclusivamente sul principio di legalità formale, imponendo una valutazione ulteriore relativa alla giustificazione sostanziale dell'ingerenza.

Sebbene il codice di procedura penale non contenga una disciplina generale del principio di proporzionalità in materia probatoria, tale criterio ha progressivamente assunto una fisionomia autonoma all'interno del sistema[50], anche grazie all'influenza esercitata dal diritto europeo e dalla giurisprudenza sovranazionale. Tanto la Convenzione europea dei diritti dell'uomo quanto la Carta dei diritti fondamentali dell'Unione europea subordinano infatti la legittimità delle limitazioni ai diritti fondamentali a tale principio, costruito attorno alla presenza di una base legale adeguata, al perseguimento di un obiettivo legittimo di interesse generale e al rispetto del principio di necessità[51].

Nel contesto delle investigazioni digitali, tuttavia, il test di proporzionalità non può essere ricostruito esclusivamente a partire dalle categorie del

48. Flor–Marcolini 2022.

49. Lassalle–Lannier 2025. Come evidenziano gli autori, anche se "undoubtedly being the most intrusive [steps] in the process (…), At the European level, neither the ECJ nor the ECtHR has yet addressed the substance of the proportionality of the legal hacking carried out in France. They also have not dealt with the implications of these measures for criminal proceedings abroad. Several applications are pending before the ECtHR, which will likely offer the opportunity to revisit the matter. However, as these applications are not directed against France as the 'collecting country', the Court in Strasbourg is not going to discuss the proportionality of legal hacking".

50. Caianello 2025.

51. Espressamente previsto dall'art. 52 par. 1 della Carta di Nizza, ma rinvenibile anche nel sistema CEDU anche se non espressamente richiamato. Su questo cfr. Galetta 1999.

diritto processuale penale. La particolare natura dell'oggetto dell'attività investigativa, costituito da dati personali, comunicazioni elettroniche e informazioni digitali, impone infatti di integrare tale prospettiva con ulteriori coordinate.

Una prima integrazione deriva dal diritto della protezione dei dati personali. Tanto il Regolamento (UE) 2016/679 (GDPR), quanto la direttiva (UE) 2016/680 (Law Enforcement Directive), pur operando in contesti differenti, richiedono che ogni trattamento di dati personali sia necessario e proporzionato rispetto alle finalità perseguite[52]. La proporzionalità assume quindi una dimensione specificamente informazionale, imponendo di considerare non soltanto le modalità di acquisizione dei dati, ma anche la loro qualità, quantità, durata della conservazione, possibilità di riutilizzo e circolazione tra soggetti pubblici e privati[53]. Si tratta di una prospettiva che appare particolarmente rilevante nelle investigazioni digitali. Una lettura esclusivamente processualistica rischia infatti di concentrarsi prevalentemente sul "contenitore" dell'attività investigativa (il *device*, ad esempio), senza considerare adeguatamente il "contenuto" rappresentato dai dati concretamente accessibili attraverso tali strumenti.

In letteratura[54], seppur in un contesto diverso da quello delle indagini digitali, ci si è già confrontati con l'integrazione di questi due livelli, da cui deriva un test di proporzionalità che si articola in scanditi passaggi, ossia quelli della disciplina positiva della misura, della finalità legittima perseguita, della necessità della misura in una società democratica. Il terzo step poi racchiude a sua volta diversi sotto-criteri, ossia che la misura sia: genuinamente effettiva, la minor intrusiva possibile, che vi sia un equo bilanciamento tra diritti contrapposti, che vi siano adeguate salvaguardie.

Accanto alla dimensione processuale e a quella della protezione dei dati personali deve poi essere valorizzata una terza prospettiva, rappresentata dal diritto penale sostanziale. È infatti proprio sul terreno della proporzionalità in senso stretto che emerge la necessità di considerare non soltanto l'intensità dell'ingerenza investigativa, ma anche il valore degli interessi pubblici perseguiti attraverso tale ingerenza. In altri termini, il giudizio di proporzionalità non può limitarsi a verificare se una determinata misura sia astrattamente idonea e necessaria all'accertamento dei fatti, ma deve altresì interrogarsi sulla gravità del fenomeno criminale che ne giustifica l'utilizzo.

Da questo punto di vista, il tradizionale test tripartito elaborato nella cultura giuridica tedesca, articolato nei criteri della idoneità (ossia capacità della misura in astratto a perseguire l'obiettivo prefissato, in questo caso le esigenze probatorie), necessità (ossia assenza di alternative meno intrusive) e proporzionalità in senso stretto (ossia adeguatezza nel bilanciamento tra esigenze contrapposte, in questo caso in relazione al fine perseguito, e quindi alla gravità del reato perseguito), e progressivamente valorizzato anche nel sistema domestico[55] appare perfettamente compatibile con la struttura del controllo di proporzionalità elaborata dalla giurisprudenza europea e ricavabile dalla disciplina della protezione dei dati personali. I modelli, più che alternativi, risultano complementari.

È proprio all'interno dei diversi livelli che compongono il test di proporzionalità che assume rilievo la nozione di "criminalità grave". Come mostrano le vicende della *data retention* sopra esaminate, la gravità del reato non costituisce un elemento esterno al giudizio di proporzionalità, bensì uno dei suoi fattori costitutivi. Quanto maggiore è la capacità intrusiva dello strumento investigativo, tanto più elevato deve essere il livello di offensività del fenomeno criminale che ne giustifica l'impiego.

La nozione di criminalità grave assume pertanto una duplice funzione. In primo luogo, essa opera sul piano legislativo, orientando le scelte di politica criminale relative alla delimitazione dei presupposti applicativi dei mezzi investigativi maggiormente invasivi. In secondo luogo, essa rileva sul piano applicativo, consentendo al giudice di verificare in concreto se il sacrificio imposto ai

52. Cfr. artt. 6 par. 4, 23, 9, 10, 22 GDPR e art. 4 LED.

53. Cfr. de Jonge–de Vries 2024.

54. Bertrand–Maxwell–Vamparys 2020.

55. Si veda la ricostruzione del principio fatta da Caianello 2014, compresi i riferimenti relativi alla dottrina tedesca sul punto.

diritti fondamentali risulti giustificato rispetto alle caratteristiche del caso sottoposto al suo esame.

Questa duplice dimensione emerge chiaramente anche dalla recente giurisprudenza della Corte di giustizia relativa alla disciplina italiana della *data retention*. La sentenza della Procura di Bolzano mostra infatti come il rispetto del principio di proporzionalità non possa essere assicurato esclusivamente attraverso criteri legislativi astratti fondati sui limiti edittali di pena, ma richieda altresì una verifica concreta della gravità del fatto oggetto di accertamento. Al tempo stesso, tuttavia, una valutazione interamente rimessa alla discrezionalità giudiziale rischierebbe di compromettere le esigenze di prevedibilità e certezza del diritto.

La soluzione sembra dunque risiedere in un modello integrato, nel quale il legislatore individui *ex ante* le categorie di reati sufficientemente gravi da giustificare il ricorso a determinati strumenti investigativi, lasciando al giudice il compito di verificare, nel caso concreto, se l'ingerenza richiesta risulti effettivamente proporzionata rispetto alle caratteristiche della fattispecie. Occorre, in altri termini, considerare, da un lato, la tipologia del reato (seguendo, ad esempio, le aree di criminalità grave individuate dallo stesso diritto penale europeo) [56], e, dall'altro, la gravità del fatto.

Anche la giurisprudenza della CGUE sembra muoversi nella medesima direzione. In materia di *data retention*, la Corte ha progressivamente elaborato una vera e propria gerarchia degli interessi pubblici suscettibili di giustificare limitazioni ai diritti fondamentali[57]. Al vertice si colloca la tutela della sicurezza nazionale[58], seguita dalla prevenzione delle minacce gravi alla sicurezza pubblica e dalla lotta contro forme gravi di criminalità. Solo in posizione subordinata si collocano, invece, la lotta contro la criminalità ordinaria e gli obiettivi generali di prevenzione.

Le indagini digitali rappresentano, dunque, un terreno particolarmente fertile per sviluppare un dialogo interdisciplinare tra diritto processuale penale, protezione dei dati personali e diritto penale sostanziale. Proprio la crescente centralità del dato quale oggetto dell'attività investigativa impone infatti di superare una visione frammentata delle garanzie, favorendo una lettura integrata delle diverse dimensioni coinvolte.

Anche se rimane il piano applicativo, in ultima istanza, il contesto in cui la proporzionalità assume concretezza e in cui devono quindi raccogliersi in modo equilibrato l'esercizio di un margine di discrezionalità e la sua applicazione rigorosa, attraverso un'adeguata "proceduralità argomentativa"[59] orientata ai criteri derivanti dal quadro (normativo e giurisprudenziale) europeo, tale impostazione conferma come la proporzionalità non possa essere ridotta a un mero criterio applicativo rimesso alla valutazione del giudice, ma debba essere considerata anche quale salvaguardia metodologica nelle scelte di politica legislativa (eventualmente sindacabile dalla sola Corte Costituzionale). La selezione delle forme di criminalità che giustificano il ricorso agli strumenti investigativi più invasivi costituisce infatti una scelta normativa preliminare, destinata a incidere profondamente sull'equilibrio tra sicurezza e libertà all'interno dell'ordinamento. Ed è proprio la crescente diffusione delle investigazioni digitali a rendere sempre più urgente la costruzione di una disciplina sistematica che assuma il principio di proporzionalità e la nozione di criminalità grave quali parametri centrali nella regolazione dei poteri investigativi tecnologicamente avanzati.

Riferimenti bibliografici

D. Albanese (2024), *Dalla Corte di Giustizia dell'Unione europea un'altra svolta garantista in materia di acquisizione dei tabulati telefonici*, in "Sistema penale", 2024, n. 5

56. Ci si riferisce alle aree di cui all'art. 83 par. 1 TFUE. Evidenzia il problema di lasciare una discrezionalità troppo ampia agli Stati membri Marino 2024.
57. Cfr. C. giust. UE, 5 aprile 2022, *Commissioner of An Garda Síochána*, C-140/ 20, par. 56.
58. Cfr. C-511/18, C-512/18, C-520/18, cit.
59. Caianiello 2025.

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

V. Bajović, V. Ćorić (2025), *Encrochat and SkyECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision*, in "European Journal of Crime, Criminal Law and Criminal Justice", vol. 33, 2025

A. Bertrand, W. Maxwell, X. Vamparys (2020), *Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?*, in SSRN, 2020

E. Billis, N. Knust, J.P. Rui (Eds.) (2021), *Proportionality in Crime Control and Criminal Justice*, Bloomsbury, 2021

S. Bonetti (2026), *La data retention: alcune riflessioni nella prospettiva del diritto privato della protezione dei dati personali*, in "Rivista italiana di informatica e diritto", 2026, n. 1

M. Caianiello (2025), *Il principio di proporzionalità nel diritto penale*, in "Rivista italiana di diritto e procedura penale", 2025, n. 3

M. Caianiello (2019), *Criminal Process Faced with the Challenges of Scientific and Technological Development*, in "European Journal of Crime, Criminal Law and Criminal Justice", vol. 27, 2019

M. Caianiello (2014), *Il principio di proporzionalità nel procedimento penale*, in "Diritto Penale Contemporaneo", 2014, n. 3-4

S. Cognetti (2011), *Principio di proporzionalità. Profili di teoria generale e di analisi sistematica*, Giappichelli, 2011

J. Dalla Torre (2024), *Proporzionalità va cercandosi: la Corte di giustizia sul concetto di criminalità grave nella data retention*, in "Rivista italiana di diritto e procedura penale", 2024, n. 2

B. de Jonge, B. de Vries (2024), *Data-Driven Investigations in a Cross-Border Setting*, in "eucrim", vol. 19, 2024, n. 3

G. Di Paolo (2024), *La circolazione transfrontaliera delle prove elettroniche*, in "Penale. Diritto e Procedura", 2024, n. 2

G. Di Paolo, L. Pressacco (a cura di) (2025), *Indagini e prove nella società digitale. Questioni attuali e prospettive future*, Editoriale Scientifica, 2025

F. Fabbrini (2015), *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, in "Harvard Human Rights Journal", 2015

R. Flor (2014), *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in "Diritto Penale Contemporaneo", 2014, n. 2

R. Flor, S. Marcolini (2022), *Dalla data retention alle indagini ad alto contenuto tecnologico*, Giappichelli, 2022

G. Formici (2021), *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Giappichelli, 2021

D.U. Galetta (1999), *Il principio di proporzionalità nella Convenzione europea dei diritti dell'uomo, fra principio di necessarietà e dottrina del margine di apprezzamento statale: riflessioni generali su contenuti e rilevanza effettiva del principio*, in "Rivista italiana di diritto pubblico comunitario", vol. 9, 1999, n. 3-4

M. Galič, L. Stevens, B.-J. Koops (2023), *Editorial: A Trialogue on Regulating Data-Driven Criminal Procedure,* in "New Journal of European Criminal Law", vol. 14, 2023, n. 4

H. Goldstein (1990), *Problem-Oriented Policing*, McGraw-Hill, 1990

E. Grisonich (2024), *Al vaglio della Corte di giustizia la riforma italiana in materia di acquisizione dei tabulati telefonici*, in "Processo Penale e Giustizia", 2024

T. Hickman (2008), *The Substance and Structure of Proportionality,* in "Public Law", 2008

D. Kaye (2015), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/29/32, 22 maggio 2015

O. Kerr (2024), *The Digital Fourth Amendment*, Oxford University Press, 2024

E. Kosta, I. Kamara (Eds.) (2025), *Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive*, Oxford University Press, 2025

N. Lacey (2016), *The Metaphor of Proportionality*, in "Journal of Law and Society", vol. 43, 2016

G. Lasagni (2018), *Tackling Phone Searches in Italy and in the US. Proposals for a Technological Re-Thinking of Procedural Rights and Freedoms*, in "New Journal of European Criminal Law", vol. 9, 2018

M. Lassalle, S. Lannier (2025), *EncroChat – A Judicial Chronology*, in "eucrim", vol. 20, 2025, n. 4

A. Lavorgna, P. Ugwudike (2021), *The Datafication Revolution in Criminal Justice: An Empirical Exploration of Frames Portraying Data-Driven Technologies for Crime Prevention and Control,* in "Big Data & Society", 2021

K. Ligeti (Ed.) (2026), *AI Evidence and Criminal Proceedings*, Hart Publishing, 2026

S. Marcolini (2019), *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "Cybercrime", Utet-WKI, 2019

F. Marino (2024), *Comunicazioni elettroniche, perseguimento di reati gravi e rispetto della vita privata*, in "Giurisprudenza Italiana", 2024

V. Mitsilegas (2025), *Data Retention and the Judicial Parameters of Mass Surveillance in EU Law*, in E. Kosta, I. Kamara (Eds.), "Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive", Oxford University Press, 2025

V. Mitsilegas, E. Guild, E. Kuskonmaz, N. Vavoula (2023), *Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks*, in "European Law Journal", vol. 29, 2023, n. 1-2

B.C. Newell, T. Timan, B-J. Koops (Eds.) (2018), *Surveillance, Privacy, and Public Space*, Routledge, 2018

F. Nicolicchia (2024), *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla querelle giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero*, in "Sistema penale", 2024, n. 2

J.-J. Oerlemans, S. Royer (2023), *The Future of Data Driven Investigations in Light of the Sky ECC Operation*, in "New Journal of European Criminal Law", vol. 14, 2023, n. 4

J.-J. Oerlemans, D.A.G. van Toor (2022), *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in "European Journal of Crime, Criminal Law and Criminal Justice", vol. 30, 2022, n. 3-4

M. Panzavolta, E. Maes (2022), *Exclusion of Evidence in Times of Mass Surveillance. In Search of a Principled Approach to Exclusion of Illegally Obtained Evidence in Criminal Cases in the European Union,* in "The International Journal of Evidence & Proof", vol. 26, 2022

L. Parodi (2025), *La "gravità dell'ingerenza" nel prisma della proporzionalità: nuovi equilibri in tema di data retention*, in "Sistema penale", 2025

A. Sachoulidou (2026), *A Typology of Automated Law Enforcement Systems Under EU Law: What Standards for Defence Rights?*, in N. Vavoula (Ed.), "The Future of Digitalisation in EU Law Enforcement", in "European Papers – A Journal on Law and Integration," vol. 11, 2026, n. 1

I. Škorvánek, B.-J. Koops, B.C. Newell, A. Roberts (2019), *"My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking*, in "Brigham Young University law review", 2019, n. 4

G. Todaro (2024), *L'evoluzione delle fonti del diritto nella «società algoritmica»: data retention e diritti fondamentali della persona*, in "Cassazione Penale", 2024, n. 6

N. Vavoula (Ed.) (2026), *The Future of Digitalisation in EU Law Enforcement*, in "European Papers – A Journal on Law and Integration", vol. 11, 2026, n. 1

M. Washington, N. Richards (2019), *Digital Civil Liberties and the Translation Problem*, in D.K. Brown, J.I. Turner., B. Weisser (Eds.), "The Oxford Handbook of Criminal Process", Oxford University Press, 2019