A PROPOSITO DI ACQUISIZIONE DELLE IMMAGINI ESTRAPOLATE DALLE TELECAMERE DI VIDEOSORVEGLIANZA

Wanda Nocerino

Cass., Sez. I, 5 dicembre 2023 (dep. 12 marzo 2024), n. 10378

Pres. Di Nicola – Rel. Monaco – P.M. Mignolo (Conf.)

Sommario: 1. Il pensiero della Corte. – 2. Il contesto di riferimento. – 3. Una conclusione da ripensare.

ABSTRACT

Confermando un principio consolidato sia in dottrina che in giurisprudenza, i giudici di legittimità ribadiscono la natura documentale delle immagini estrapolate dalle telecamere di videosorveglianza. In quest'ottica, ai fini dell'utilizzabilità processuale delle videoregistrazioni, non è necessario rispettare la c.d. "catena di custodia", ossia la procedura atta a preservare la genuinità dei dati digitali, non assumendo alcun rilievo la natura supporto su cui la rappresentazione è incorporata. Una simile impostazione – che, di fatto, è volta a estendere a dismisura il perimetro operativo della prova documentale nell'ottica di semplificare le procedure di acquisizione delle videoregistrazioni – rischia di essere alquanto pericolosa visto il crescente uso di questo strumento di prova.

Confirming a consolidated principle in doctrine and jurisprudence, the judges of legitimacy reaffirm the documentary nature of the images extracted from video surveillance cameras. From this point of view, for the purposes of the procedural usability of video recordings, it is not necessary to comply with the so-called 'chain of custody', i.e. the procedure aimed at preserving the genuineness of digital data, since the nature of the support on which the representation is embedded is not relevant. Such an approach – which, in fact, is aimed at disproportionately extending the operational perimeter of the document and, therefore, aimed at simplifying the procedures for the acquisition of video recordings – risks being rather dangerous given the growing use of this instrument of evidence.

1. Il pensiero della Corte.

Non è facile per la Corte di Cassazione prendere posizione su una materia tecnicamente complessa come quella inerente alle modalità di acquisizione dei filmati delle telecamere di videosorveglianza e al relativo regime di impiego processuale. Non a caso, infatti, la giurisprudenza di legittimità si è a sempre concentrata sulla qualificazione giuridica da attribuire alle videoriprese investigative e alle videoregistrazioni[1] senza entrare nel merito delle questioni attinenti ai profili più "specialistici" della materia, nella piena consapevolezza del delicato equilibrio che regola i rapporti tra innovazioni tecnico-scientifiche e processo penale.

In questo campo – più di qualunque altro – il pericolo è che nel soppesare i diversi interessi in gioco, il diritto di difesa, da un lato, e l'esigenza di accertamento del fatto, dall'altro, si tende o a fare del primo un "super diritto costituzionale", in grado di travolgere ogni altro precetto fondamentale, o ad enfatizzare il secondo

quale unico e primario scopo del processo[2].

Nel caso di specie, i giudici preferiscono salvaguardare l'autonomia investigativa della p.g. e blindare il risultato probatorio che ne deriva: a parere della Corte, infatti, i *file* contenenti videoriprese effettuate da privati – al pari dei dati relativi al tracciamento GPS – rientrano nel *genus* della prova documentale e ne seguono il relativo regime acquisitivo di cui all'art. 234 c.p.p., non assumendo alcun rilievo la peculiare natura del supporto su cui i dati sono immagazzinati.

Così ragionando, la Corte arriva a ritenere che non occorre rispettare la catena di custodia per garantire l'impiego probatorio dei filmati estrapolati dalle telecamere di videosorveglianza, posto che «la copia estratta da un documento informatico ha la medesima valenza probatoria del dato originariamente acquisito, salvo che se ne deduca e dimostri la manipolazione [...]»[3].

Senza anticipare quanto verrà approfondito nel prosieguo, si può dire che una simile impostazione non è del tutto convincente, e piuttosto acutizza quelle criticità procedurali e teleologiche che la dottrina ha tentato di arginare tutte le volte in cui il sistema ha dovuto fare i conti con la prova tecnico-scientifica[4]. Si è indotti a pensare che una simile impostazione rischia di delegittimare il complesso di regole procedurali per l'assunzione delle *digital evidences* che sono – o, almeno, dovrebbero essere – sedimentate nel sistema processuale quali garanzie ineludibili per assicurare la genuinità degli elementi probatori di stampo digitale[5].

Tali considerazioni appaiono ancora più preoccupanti in ragione del crescente uso di questo strumento di prova che, in prospettiva, è destinato ad aumentare ancora il suo "peso"[6]. Ci si riferisce, in particolare, all'*AI Act*[7] che concorre ad accrescere a dismisura le potenzialità informativo-investigative delle immagini videoregistrate. Il Regolamento, infatti, autorizzando (a specifiche condizioni)[8] l'impiego di sistemi di identificazione remota *real time* per la prevenzione e il contrasto di gravi minacce alla sicurezza nazionale, sembra di fatto incoraggiare il ricorso a sistemi di sorveglianza "intelligenti" per procedere al riconoscimento biometrico di «sospettati" di reati».

2. Il contesto di riferimento.

Prima ancora di soffermarsi sulle implicazioni giuridico-dogmatiche che derivano dalla pronuncia in commento, conviene considerare il contesto nel quale si insinua il fenomeno dei "*video surveillance systems*".

Da oltre un decennio, si è diffusa la convinzione che la videosorveglianza porti grandi contributi alla sicurezza pubblica, sia in chiave preventiva, come strumento di deterrenza, sia in chiave repressiva, quale mezzo di individuazione e identificazione dei responsabili di reati già commessi[9].

I più recenti sviluppi della tecnologia digitale – e, in particolare, dell'intelligenza artificiale – hanno raggiunto e potenziato il congegno, schiudendo scenari inimmaginabili in passato. Con l'ausilio delle telecamere di videosorveglianza, infatti, è diventato possibile non solo ascoltare i dialoghi intercorrenti tra i soggetti monitorati[10], ma anche riconoscere un individuo filmato incrociando le immagini con altri dati personali[11] e rilevare automaticamente comportamenti sospetti, registrandoli e segnalandoli.

Alla serrata regolamentazione relativa all'uso degli impianti di videosorveglianza per fini di pubblica sicurezza[12] non corrisponde un adeguato regime processuale per favorire l'impiego probatorio delle immagini nel circuito processuale[13]: si tratta di «un difetto grave, perché le riprese visive pongono problemi di qualificazione giuridica piuttosto intricati»[14].

Di fronte all'assenza di norme volte a regolare il regime di utilizzabilità probatoria delle immagini provenienti dalle telecamere di sorveglianza, è la giurisprudenza a delineare il perimetro entro cui l'acquisizione delle registrazioni può considerarsi legittima.

La Corte è granitica nel discernere le condizioni di impiego dibattimentale delle videoriprese investigative, ossia quelle esperite dalla p.g., anche di iniziativa, nel corso del procedimento e per finalità di indagine, e delle videoregistrazioni, ovvero i filmati estratti dagli impianti di sicurezza confezionati di privati in un contesto stragiudiziale.

Nel primo caso i giudici sono fermi nel seguire i dettami delle Sezioni Unite c.d. "Prisco"[15]; nel secondo, la Corte – altrettanto fermamente – ritiene che l'utilizzo processuale delle immagini provenienti dalle

telecamere di sorveglianza è condizionato alla disciplina di cui all'art. 234 c.p.p., trattandosi di prove documentali di natura informatica[16].

Di qui, si è detto che «la copia estratta da un documento informatico ha la medesima valenza probatoria del dato originariamente acquisito, salvo che se ne deduca o dimostri la manipolazione»[17]; per tale ragione, secondo la Corte, non occorre rispettare la catena di custodia per garantire l'impiego processuale delle immagini videoregistrate, vigendo una presunzione di "genuinità" dell'informazione ottenuta, proprio come avverrebbe se fosse acquisito un documento analogico[18].

Altrettanto inconfutabile per la giurisprudenza è la natura ripetibile del rilievo consistente nell'estrazione dei filmati dalle telecamere di videosorveglianza[19].

Se è vero che «la tecnica consente di acquisire un dato informatico attraverso operazioni meramente esecutive e materiali, il cui unico scopo è quello di assicurare alla fase processuale quanto di rilevante è contenuto all'interno dello stesso in formato digitale»[20], è evidente l'impossibilità di ricorrere allo statuto dell'accertamento tecnico irripetibile di cui all'art. 360 c.p.p.[21], poiché «l'apprensione non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale»[22].

3. Una conclusione da ripensare.

La decisione – in linea con l'impostazione seguita dalla giurisprudenza maggioritaria – non è del tutto convincente.

Intanto, va rilevato l'errore di fondo sotteso alla pronuncia in commento: i giudici, infatti, sembrano partire da un presupposto errato, sovrapponendo i dati relativi al tracciamento GPS alle videoregistrazioni.

Il segnale video è dato da un insieme di immagini o, più correttamente, da una sequenza di fotogrammi che

vengono visualizzati in successione, prendendo il nome di *frame*. Si tratta, dunque di dati digitali che contengono informazioni espresse in un codice binario – ossia in sequenze di numeri, zero e uno, definite *bit* – e contenute nelle memorie di computer o di altri dispositivi informatici, oppure circolanti in Rete[23].

Le informazioni relative alla localizzazione satellitare, invece, non rientrano nel concetto di *digital evidences,* trattandosi di immagini "statiche" e dati alfanumerici che delineano le coordinate spazio-territoriali entro cui il bersaglio si muove[24].

Di conseguenza, pur essendo entrambi dotati di un'autonoma efficacia rappresentativa, per l'impiego processuale delle videoregistrazioni occorre assicurare "a monte" l'affidabilità dell'elemento di prova digitale; viceversa, nel caso di dati di geolocalizzazione «mentre *ex ante* non pare discutibile l'attendibilità della tecnica GPS, [solo] *ex post* occorrerà verificare se l'oggettività della rilevazione sia stata o no compromessa tramite strumentazioni esterne»[25].

Da questo punto di vista, risulta indispensabile distinguere le modalità con cui si procede all'apprensione materiale delle due *species* di informazioni perché, se nell'ipotesi di dati relativi al tracciamento GPS non è richiesto *a priori* alcun nessun adempimento specifico in sede di acquisizione, nel caso di videoregistrazioni è doveroso ricorrere al complesso di regole valevoli per la raccolta degli elementi di prova digitali così da contenere gli ontologici rischi di alterazione[26].

Come è noto, le prescrizioni in materia di *digital forensics* impongono il rispetto della c.d. catena di custodia, ossia «l'insieme di passaggi, formalizzati con un sistema di tracciamento (manuale o elettronico), attraverso i quali il reperto, o meglio i plichi ed i confezionamenti in cui è conservato, transita dalla scena del crimine al tutte le altre fasi del procedimento penale»[27], al fine di consentire al dato digitale di trovare impiego nel processo al riparo da eventuali eccezioni di inutilizzabilità fondate proprio sul mancato rispetto delle cautele di ordine tecnico[28].

Peraltro, va considerato che l'acquisizione "genuina" del materiale probatorio da riversare in sede processuale rappresenta un dogma imposto dalle stesse norme del codice di rito.

Considerato che i filmati provenienti dalle telecamere di sorveglianza sono documenti informatici[29] –

peraltro dotati di caratteristiche proprie e univoche che li rendono ancora più "fragili" rispetto ai modelli tradizionali[30] –, il punto di riferimento per delineare il relativo regime acquisitivo è l'art. 234 c.p.p., secondo cui l'atto rappresentativo deve essere intromesso nel circuito processuale in originale e, solo «[Q]uando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia».

Ciò significa che la regola che sottende l'apprensione di documenti è l'acquisizione fedele dell'informazione; il ricorso alle copie è riservato ad ipotesi eccezionali[31].

Segue il corollario: allorquando ci si accinge ad acquisire un documento informatico, risulta imprescindibile procedere alla duplicazione dello stesso per assicurare al processo una "copia clone" (c.d. "copia forense")[32] quale condizione ineludibile per riconoscere al materiale appreso una "dignità" probatoria.

Di conseguenza, appare assolutamente discutibile la scelta della Corte di semplificare la procedura di estrapolazione e conservazione delle immagini, ritenendo superfluo il ricorso alla copia forense e alla catena di custodia: in questo caso, la volontà di "liberalizzare" le forme rappresenta un forte limite all'affidabilità dell'atto, acuendo il rischio di far entrare al processo informazioni parziali o, addirittura, errate[33].

A ragionare diversamente, si rischia di compromettere il diritto di difesa dell'imputato[34], inteso quale diritto ad un corretto accertamento giudiziale[35] fondato sulla base di indagini complete (e corrette) in tutti gli aspetti, considerato che durante il processo «è in gioco un'opzione di civiltà, di tutela della libertà, che segna un primato dei mezzi sui fini»[36].

Perché ciò avvenga non sembra sufficiente che in sede investigativa si sia proceduto ad acquisire il maggior numero possibile di elementi di prova a disposizione, apparendo anche indispensabile garantire anche che l'acquisizione di tali elementi sia avvenuta correttamente, dal momento che «ad una valutazione formale della completezza, deve quindi corrisponderne una sostanziale, pena lo svuotamento del principio stesso della completezza delle indagini»[37].

[1] Ci si riferisce, in particolare, alla ben nota distinzione introdotta dalla pronuncia delle Sezioni Unite "Prisco" che, da un lato, ha definito la natura documentale dei filmati acquisiti dalle telecamere di videosorveglianza effettuate da privati in luoghi pubblici, aperti o esposti al pubblico; dall'altra ha chiarito che le videoriprese esperite dalla p.g. a fini investigativi rientrano nella magmatica categoria delle prove atipiche. Cfr. Cass., Sez. un., 28 marzo 2006, n. 26795, in *Cass. pen.,* 2006, 3739, con nota di RUGGIERI, *Riprese visive e inammissibilità della prova.* Sulla pronuncia in esame, *ex multis,* CAMON, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi,* in *Riv. it. dir. proc. pen.,* 2006, 1550; CONTI, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati,* in *Dir. pen. proc.,* 2006, 1347.Sull'inquadramento giuridico delle videoregistrazioni, tra gli altri, si vedano IASEVOLI, *La nomofilachia "creatrice" in materia di videoriprese,* in Aa. Vv., *L'intercettazione di comunicazioni*, a cura di Bene, Bari, 2018, 285. Da ultimo, SAPONARO, *L'impatto processuale delle immagini: fotografie e videoriprese,* Padova, 2021.

[2] In questo senso, CURTOTTI, *Rilievi e accertamenti tecnici,* Padova, 2013, 3.

[3] Così Cass., Sez. I, 5 dicembre 2023, n. 10378, non massimata, 4.

[4] Sul tema, per tutti, CURTOTTI, FISHER, HOUCK, SPANGHER, *Diritto e scienza: un rapporto in continua evoluzione,* in Aa. Vv., *Manuale delle investigazioni sulla scena del crimine,* a cura di Curtotti-Saravo, Torino, II ed., 2022, 1.

[5] Ci si riferisce alla legge 18 marzo 2008, n. 48, recante "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*", che delinea la normativa per procedere all'acquisizione delle prove digitali. Sul punto, per tutti, Aa. Vv., *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul* cybercrime, a cura di Luparia, Milano, 2009.

[6] Secondo uno studio condotto da CURTOTTI-BATTIATO, *L'uso delle telecamere di sorveglianza a scopi di indagine,* 2018, su commissione della Direzione Centrale della Polizia di Stato, il 96% degli intervistati (ossia

agenti e ufficiali di p.g. appartenenti alla Polizia di Stato) ricorre alle immagini provenienti dalle telecamere di videosorveglianza a fini investigativi.

[7] È in via di definitiva adozione da parte del Parlamento europeo e del Consiglio, secondo la procedura legislativa ordinaria, la proposta di regolamento, presentata dalla Commissione europea il 21 aprile 2021, recante un quadro giuridico in materia di intelligenza artificiale (esplicitamente denominato "legge sull'intelligenza artificiale", ovvero *"AI Act"*).

[8] In particolare, l'art. 5 dell'*AI Act,* prevede che non è consentito «l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico, a fini di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi: 1) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; 2) la prevenzione di una minaccia specifica sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; 3) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'Allegato 2, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni [...]».

[9] Sottolineano il crescente uso dei sistemi di videosorveglianza a fini securitari, CALIFANO-FIORILLO, voce *Videosorveglianza,* in *Dig. pubbl.,* Agg., Torino, 2015, 504.

[10] Si veda, sul punto, Sez. I, 8 aprile 2009, n. 18174, in *Arch. nuova proc. pen.,* 2009, 467, in materia di intercettazione dei colloqui in ambiente carcerario mediante l'utilizzo di strumentazione audiovisiva.

[11] Si pensi che il Regolamento 2024/982/UE, "*Sulla consultazione e lo scambio automatizzati di dati per la cooperazione di polizia e che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 del Parlamento europeo e del Consiglio"* (c.d. Regolamento "Prüm II"), adottato il 13 marzo 2024, delinea la procedura di consultazione automatizzata delle immagini del volto e degli estratti del casellario giudiziale.

[12] Si pensi al decreto in materia di pubblica sicurezza del 2009 (d.l. 23 febbraio 2009, n. 11) che, in combinato disposto con le regole segnate dal Regolamento europeo 2016/679, pur consentendo agli enti statuali di installare impianti per la tutela della sicurezza urbana in luoghi pubblici o aperti al pubblico, introduce una serie di limiti al trattamento dei dati personali immagazzinati dai sistemi di videosorveglianza a carico dei Titolari (ossia la Pubblica Amministrazione che installa il dispositivo) e a favore degli interessati (ovvero i cittadini), con riguardo ai tempi di conservazione, alle finalità del trattamento e ai requisiti tecnici dei sistemi, in ossequio al principio di *accountability* e di *privacy by design.* Si pensi, ancora al d.lgs. 18 maggio 2018, n. 51, di recepimento della Direttiva UE 2016/680, che consente ai Titolari del trattamento, ossia i Comuni in persona dei sindaci *pro tempore*, di stipulare appositi "patti per la sicurezza" per legittimare gli organi di polizia di sicurezza ad utilizzare gli impianti di telecontrollo per esigenze di prevenzione o repressione dei fenomeni criminali, sempre nel rispetto delle regole generali imposte dal GDPR.

[13] Esistono, tutt'al più delle circolari interne diffuse dalle procure più virtuose. Cfr, per tutte, Procura della Repubblica presso il Tribunale di Tivoli, *Direttiva n. 1/2022. Prime indicazioni operative sull'applicazione del d.lgs. n. 150/2022,* disponibile *online* su *www.procura.tivoli.giustizia.it.*

[14] Così CAMON, voce *Captazione di immagini (diritto processuale penale),* in *Enc. dir.,* VI, Milano, 2013, 135.

[15] Cass., Sez. un., 28 luglio 2006, n. 26795, cit.

[16] Così Cass., Sez. VI, 20 dicembre 2018, n. 15838, in *C.E.D. Cass.,* n. 275541. In senso analogo, Cass., Sez. V, 6 maggio 2020, n. 13779, in *Proc. pen. giust.,* 2020, n. 4, 919. Da ultimo, Cass., Sez. II, 21 marzo 2024, n. 11837, non massimata.

[17] Cass., Sez. VI, 6 febbraio 2020, n. 12975, in *C.E.D. Cass.,* n. 278808; Cass., Sez. VI, 20 dicembre 2018, n. 15838, cit.

[18] Così Cass., Sez. I, 5 dicembre 2023, n. 10378, cit., 4.

[19] Cass., Sez. VI, 14 luglio 2016, n. 41695, in *C.E.D. Cass.,* n. 268932; Cass., Sez. II, 10 novembre 1992, n. 4523,

ivi, n. 192570.

[20] Cass., Sez. VI, 20 dicembre 2018, n. 15838, cit., 6.

[21] Cass., Sez. I, 2 novembre 2023, n. 4895, in *C.E.D. Cass.,* n. 285716; Cass., Sez. I, 27 novembre 2018, n. 19299, non massimata; Cass., Sez. VI, 14 luglio 2016, n. 41695, in *C.E.D. Cass.,* n. 268326.

[22] Cass., Sez. I, 5 marzo 2019, n. 14511, in *Cass. pen.,* 2010, 1520. Analogamente, Sez. I, 9 marzo 2011, *ivi,* 440, con nota di DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche.*

[23] Il segnale video è dato da un insieme di immagini o, più correttamente, da una sequenza di fotogrammi che vengono visualizzati in successione, prendendo il nome di *frame*. Questi ultimi sono dati digitali che contengono informazioni espresse in un codice binario – ossia in sequenze di numeri, zero e uno, definite *bit* – e contenute nelle memorie di computer o di altri dispositivi informatici, oppure circolanti in Rete. Sul punto, si veda. CRICRI', voce *Videoregistrazioni,* in *Enc. giur.,* XXXII, Roma, 2006, 1

[24] Secondo la giurisprudenza, i dati relativi alla localizzazione degli spostamenti tramite sistema di rilevamento satellitare rappresentanouna prova documentale (Cass., Sez. II, 21 gennaio 2021, n. 5415, in *C.E.D. Cass.,* n. 280647), ovvero un'attività atipica se esperita da soggetti del procedimento per fini strettamente investigativi (Cass., Sez. VI, 9 marzo 2023, n. 15422, *ivi,* n. 284582). Per approfondimenti sul tema, si veda BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali*, *Le indagini atipiche,* a cura di Scalfati, Torino, II ed., 2019, 443.

[25] Così FILIPPI, *La disciplina italiana dei tabulati telefonici e telematici contrasta con il diritto U.E.,* in *Dir. difesa*, 2021, n. 2, 423. In effetti, come chiarisce la giurisprudenza di legittimità, «poiché l'attività di p.g. consiste nella semplice trasposizione di un dato oggettivo (cioè, nella specie, quello costituito dalle coordinate ottenute dal GPS) nelle annotazioni della stessa p.g. o nelle sue relazioni di servizio, si dovrebbe escludere che la mancanza del supporto informatico contenente gli originali dei tracciati possa in alcun modo inficiare l'attendibilità e la oggettiva valenza probatoria dei medesimi dati, concernenti le suddette coordinate». Cass., Sez. IV, 27 novembre 2012, n. 48279, in *Giust. pen.,* 2013, III, 434; Cass., Sez. I, 7 gennaio 2010, n. 9416, in *Cass. pen*., 2012, 1062.

[26] Sul punto, da ultimo, MURRO, *Lo* smartphone c*ome fonte di prova. Dal sequestro del dispositivo all'analisi dei dati,* Padova, 2024, 111.

[27] Testualmente, GENNARI-SARAVO, *Le tracce,* in Aa. Vv., *Manuale delle investigazioni sulla scena del crimine,* cit., 546. Secondo ZICCARDI, *La procedura di analisi della fonte di prova digitale,* in Aa. Vv., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, a cura di Luparia-Ziccardi, Milano, 2007, 65, la catena di custodia va intesa come «la garanzia di aver mantenuto inalterati tutti i dati e lo stato del supporto fisico che li contiene durante le varie fasi del repertamento e dell'analisi».

[28] Secondo una parte della dottrina (BRAGHÒ, *L'ispezione e la perquisizione di dati*, in Aa. Vv., *profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul* cybercrime, a cura di Luparia, Milano, 2009, 191; ZACCHÈ, *La prova documentale*, Milano, 2012, 33), l'inosservanza delle regole sulle modalità operative sarebbe estranea all'area di operatività dell'inutilizzabilità, di talché potrebbe avere rilevanza soltanto nel momento della valutazione della prova. Secondo altri (CONTI, *Il volto attuale dell'inutilizzabilità: derive sostanzialistiche e bussola della legalità*, in *Dir. pen. proc.,* 2010, 790; LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, 1522), la violazione delle regole tecniche dovrebbe determinare l'inutilizzabilità delle evidenze elettroniche raccolte. Questa opzione ermeneutica potrebbe poggiare «sulla individuazione di un divieto probatorio espresso in maniera implicita proprio per il tramite degli innesti del 2008», oppure, nonostante la tipizzazione della materia realizzata dalla legge del 2008, «sulla valorizzazione della portata dogmatica dell'art. 189 in punto di vaglio giudiziale di idoneità dei nuovi strumenti ad assicurare un accertamento attendibile», oppure, ancora, sulla estensione dei canoni, già contenuti *in nuce* nel sistema, di estromissione dal processo d'ogni materiale inquinato capace di adulterare la ricostruzione penale». Così LUPARIA, Computer crimes *e procedimento penale*, in Aa. Vv., *Modelli differenziati di accertamento,* a cura di Garuti, in *Trattato di procedura penale,* diretto da Spangher, Torino, 2011, 463.

[29] Ossia rappresentazioni incorporate su base materiale con metodo digitale In questo senso, TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico*, in Aa. Vv., Cybercrime, a cura di Cadoppi, Canestrari, Manna, Papa, Torino, 2023, 1506. Più in generale, sull'inquadramento giuridico della categoria della prova documentale, *ex multis,* I. CALAMANDREI, *La prova documentale,* Padova, 1995; CANTONE, *La prova documentale,* Giuffrè, 2004; KALB, *Il documento nel sistema probatorio,* Giappichelli, 2000; LARONGA, *La*

prova documentale nel processo penale, Torino, 2004; PERCHINUNNO, voce *Prova documentale (dir. proc. pen.),* in *Enc. dir.,* XXXVII, 1998, Milano, 721; ZACCHE', *La prova documentale,* cit. Da ultimo VELE, *La prova documentale nel processo penale,* Bari, 2022.

[30] Sulle caratteristiche del dato digitale, *ex multis,* ATERNO, voce Digital forensics (*investigazioni digitali),* in *Dig. dig. pen.,* VIII, Torino, 2014, 217; DI PAOLO, voce *Prova informatica,* in *Enc. dir.,* VI, Milano, 2013, 738; PITTIRUTI, Digital evidence *e procedimento penale,* Torino, 2018, 10;SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* Torino, 2018, 121.

[31] Sul punto, approfonditamente, KALB, *Il documento nel sistema probatorio,* cit., 125;ZACCHE', *La prova documentale,* cit., 34. In questo senso anche la giurisprudenza di legittimità. *Ex multis,* Cass.,Sez. III, 1 dicembre 2021, n. 8557, in *C.E.D. Cass.,* n. 282917; Cass., Sez. V, 16 gennaio 2018, n. 8736, *ivi,* 272417; Sez. II, 21 novembre 2014, n. 52017, *ivi,* n. 261627.

[32] Da un punto di vista strettamente tecnico, le più accreditate pratiche di *digital forensics* consentono di realizzare una copia-clone dell'originale. Ciò avviene grazie ad un sistema di acquisizione e di analisi che è in grado di effettuare una c.d. *bit-stream image*, cioè una immagine "*bit per bit*" del contenuto del supporto originario. Tale operazione deve essere accompagnata da un blocco di scrittura che impedisce ogni modifica, cancellazione e compromissione (anche colposa) dei dati grazie alla funzione *hash*, ossia uno strumento che imprime la traccia dell'analisi forense e permette l'aderenza assoluta della copia all'originale. Sul punto, ATERNO, voce Digital forensics, cit., 220; DANIELE, *La prova digitale nel processo penale,* in *Riv. dir. proc*., 2011, 292; PADUA, *Videosorveglianza e prova: una questione di attendibilità*, in *Proc. pen. giust.,* 2020, n. 4, 927; SIGNORATO, *Le indagini digitali*, cit., 223.

[33] Secondo CASEY, *Error, uncertainty and loss in digital evidence,* in *International journal dig. evid.,* n. 1-2, 2002, 10, il margine di errore nell'acquisizione delle prove digitale è molto elevato, potendo recare pregiudizio alla genuinità del dato virtuale già nel momento in cui si procede a estrapolare l'immagine. In questo modo, potrebbero entrare al processo prove errate sotto il profilo rappresentativo.

[34] Sul tema, *ex multis,* CIMADOMO-DALIA, voce *Difensore,* in *Enc. dir.,* III, Milano, 1999, 501; FERRUA, voce *Difesa (Diritto di)*, in *Dig. disc. pen*., III, Torino, 1989, 66; RANDAZZO, *Difesa e difensore*, in Aa. Vv., *Protagonisti e comprimari del processo penale*, coordinato da Chiavario, Torino, 1995, 277.

[35] Per la contrapposizione tra la difesa come diritto dell'imputato e la difesa come garanzia oggettiva per un corretto svolgimento del giudizio, cfr. DENTI, *La difesa come diritto e come garanzia,* in Aa. Vv., *Il problema dell'autodifesa nel processo penale,* a cura di Grevi, Bologna, 1977, 48; GIARDA, *La difesa tecnica dell'imputato: diritto inviolabile e canone oggettivo di regolarità della giurisdizione, ivi,* 69; GREVI, *Rifiuto del difensore e inviolabilità della difesa, ivi,* 9.

[36] FERRUA, voce *Difesa,* cit., 69.

[37] Così SIGNORATO, *Le indagini digitali*, cit., 129.