SEQUESTRO DEI DISPOSITIVI INFORMATICI: VERSO L'ART. 254 TER C.P.P.? BREVI NOTE A MARGINE DEL D.D.L. A.S. N. 806

Ottavia Murro

1. Una premessa necessaria.

La disinvolta disciplina codicistica con la quale – sinora – si sono legittimate le operazioni investigative condotte nei dispositivi informatici (*smartphone*, *computer*, *tablet*, etc.) è apparsa non solo inadeguata, ma anche inidonea a limitare le attività di indagine che impattano sui diritti fondamentali, nonché su quelli c.d. di seconda e terza generazione[1].

Si è notato, infatti, che tali dispositivi dischiudono al loro interno un vero e proprio mondo virtuale[2], idoneo a descrivere «l'intera esistenza digitale delle persone»[3]. Più precisamente, in riferimento allo *smartphone*, non è apparso peregrino sostenere come esso, mediato dalla connessione alla Rete[4], diventi una vera e propria «proiezione informatica dell'individuo»[5] che abbraccia l'intera esistenza dell'uomo[6]. Questi, infatti, attraverso il dispositivo elettronico svolge la sua vita digitale (lavora, effettua ricerche, comunica, socializza, etc.), esercitando così i suoi diritti fondamentali[7].

Si è così sostenuto che, anche nel luogo virtuale, assumono rilievo sia l'art. 13 Cost., presupposto di tutti gli altri diritti di libertà[8], sia i successivi segmenti, indicati negli artt. 14 e 15 Cost., che ne ampliano, rafforzano e perfezionano la portata[9].

Tuttavia, nonostante l'impatto sui volari tutelati dalla Costituzione sia ormai evidente, all'interprete è stata consegnata una disciplina frammentata tra gli artt. 244, 247, 253, 254 e 354 c.p.p. che, però, non precisa limiti e divieti[10], né presuppone un controllo giurisdizionale preventivo o effettivo a posteriori[11]. E sullo sfondo delle questioni si è adombrato il rischio della prova illecita[12].

L'attualità del tema ha visto talaltro accendersi un faro, dopo la sentenza della Corte Costituzionale del 27 luglio 2023, n. 170[13], in riferimento al sequestro di *e-mail* e *chat* presenti nello *smartphone*. Non solo. In tale contesto, già dal mese di maggio 2023[14] è iniziato un vivido dibattito sulla disciplina del sequestro dei dispositivi elettronici che prosegue, proprio in queste settimane, con la presentazione degli emendamenti alla proposta di legge che anima i lavori della Commissione Giustizia del Senato[15].

Opportuno appare, allora, delineare gli snodi principali della proposta di legge, con riguardo all'emendamento 1.100 che sostituisce l'integrale testo del d.d.l. A.S. 806, mirando ad introdurre l'art. 254 *ter* c.p.p. (*Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute*).

2. L'emendamento 1.100: profili generali

Gli insegnamenti della più recente sentenza della Corte Costituzionale[16] – in riferimento ai dati comunicativi presenti in *smartphone* e *computer* – uniti ai Protocolli[17] che hanno provato a procedimentalizzare per fasi il sequestro dei dispositivi elettronici, trovano connotazione nell'emendamento in questione[18].

Esso propone una articolata procedimentalizzazione che suddivide in tre distinte fasi le operazioni investigative condotte sui dispositivi informatici: a) sequestro del dispositivo; b) copia ed analisi dei dati; c) acquisizione di quelli di rilievo investigativo; individuando per gli snodi principiali lo strumento di controllo della riserva di giurisdizione. Emerge, in primissima approssimazione, la consapevolezza che la sequenza operativa che conduce al sequestro dei dati (sequestro del dispositivo elettronico; copia forense del suo contenuto; perquisizione, *ex* art. 274, comma 1 *bis*, c.p.p.; sequestro dei *files* rilevanti), sia un «atto investigativo complesso, che necessita di adeguati presupposti giustificativi in ogni suo snodo»[19]. In tale contesto, poiché il sequestro dei dispositivi elettronici,oltre a determinare lo spossessamento del cellulare, incide anche sui dati digitali in esso custoditi[20], si cerca di disciplinare il sequestro nella duplice dimensione (sia in riferimento al contenitore, ovvero il dispositivo; sia in riferimento al contenuto, ovvero i dati digitali)[21].

Appare allora necessario analizzare separatamente i diversi snodi della procedura che la proposta di legge mira ad inserire.

2.1 *Segue*: il sequestro del dispositivo

L'emendamento, al punto n. 1, prevede che il sequestro di dispositivi, sistemi informatici o telematici, o di memorie digitali, sia disposto con decreto motivato dal giudice per le indagini preliminari, su richiesta del pubblico ministero, quando esso è necessario alla «prosecuzione delle indagini in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del criterio di proporzione».

Una vera e propria riserva di giurisdizione, in rima con la disciplina prevista per le intercettazioni e l'acquisizione di tabulati di traffico telefonico e telematico. Ovviamente, vi è la deroga per ragioni di urgenza, con la successiva convalida, entro quarantotto ore, da parte del giudice e l'emissione del relativo decreto (punto n. 4 dell'emendamento).

Introdurre per tali atti investigativi il controllo giurisdizionale, significa aprire il testo costituzionale alla possibile emersione di nuovi strumenti, quali quelli digitali, che dischiudo luoghi virtuali, nei quali si deve comunque garantire il rispetto dei valori tutelati dalla Carta[22]. Tale interpretazione sembra essere coerente anche con l'esigenza di modernità della Costituzione[23].

Di contro, l'assenza di un limite espressamente previsto dal legislatore e di una specificazione dei casi e dei modi legittimanti la lesione del diritto, rende difficilmente superabile il *test* di costituzionalità della proposta di legge in esame[24]. Infatti, si nota l'assenza della riserva di legge, atteso che l'unico parametro con cui corredare il decreto di sequestro è il generico richiamo alla necessità, unita al criterio di proporzione.

Tuttavia, se il dispositivo elettronico può – quantomeno in potenza – custodire un'enorme mole di dati[25], le riflessioni si devono spostare sulla portata più ampia dell'art. 13 Cost. che consente di ricomprendere al suo interno il vasto spettro delle libertà morali[26] e della dignità stessa della persona[27]. In siffatto contesto, si è estesa la libertà sino a ricomprendere, ad esempio, gli oggetti che «abitualmente sono portati sulla persona (come portafogli, portamonete etc.) o ad immediato contatto con essa (come borse, borselli e borsette)»[28]. Ed è innegabile che il rapporto di continuità spaziale – tra individuo ed oggetto – rilevi anche per i dispositivi informatici e, soprattutto, per lo *smartphone*[29]che, più di ogni altro bene materiale, rappresenta l'estensione del corpo umano[30].

Ed allora, se la massima espansione delle libertà e dei diritti fondamentali presuppone sempre un'interpretazione estensiva di tali diritti e restrittiva dei limiti, il sequestro dei dispositivi elettronici deve necessariamente essere presidiato da norme processuali atte anche a definire casi, tempi e modi dell'attività investigativa. Altrimenti, l'atto investigativo, impattando sui diritti fondamentali e violando il principio della riserva di legge, risulterebbe illegittimo[31].

2.2 *Segue*: la duplicazione del contenuto

La seconda fase, disciplinata dalla proposta qui in esame, è quella della duplicazione ed analisi del contenuto digitale, enucleata nei punti da 6 a 11 dell'emendamento.

In tale contesto, entro cinque giorni dal deposito del verbale di sequestro, il pubblico ministero avvisa le parti e i difensori del giorno, dell'ora e luogo fissati per il conferimento dell'incarico per la duplicazione del contenuto dei dispositivi informatici, nonché dei dati, delle informazioni o dei programmi accessibili da remoto dal dispositivo in sequestro. Le parti sono avvisate della facoltà di nominare consulenti tecnici, con espresso richiamo alla sola disposizione di cui all'art. 364, comma 2, c.p.p. Una volta effettuata la duplicazione si dispone senza ritardo la restituzione dei dispositivi e si procede all'analisi dei dati.

Sotto un primo profilo, si nota subito come il disegno di legge, nel richiamare la procedura di «duplicazione del contenuto dei dispositivi», faccia espresso riferimento all'art. 364, comma 2, c.p.p., serbando un roboante silenzio sul ricorso alla procedura garantita disciplinata dall'art. 360 c.p.p. Su tale specifica questione, invero, la dottrina ha precisato come i dati digitali sono dematerializzati[32], fragili e alterabili[33], circostanza che dovrebbe far propendere per una non ripetibilità[34] delle attività tecniche di natura digitale[35].

Diversamente detto, in vista di una modifica dell'assetto che disciplina l'intera normativa, bisognerebbe ragionare in termini di irripetibilità, piuttosto che di urgenza, dove quest'ultima dovrebbe costituire una eccezione, proprio in ragione dei cedimenti garantitici che la connotano.

2.3 *Segue*: analisi dei dati

Il disegno di legge prevede il sequestro del dispositivo (e dunque anche del suo integrale patrimonio digitale) quando sussiste il requisito della «necessità in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del criterio di proporzione». Nel contempo, ammette le operazioni di duplicazione del contenuto integrale dei dispositivi informatici, senza indicare alcun ulteriore criterio selettivo nelle successive operazioni di analisi dei dati, ammettendo finanche la copia di tutte le informazioni accessibili da remoto dal dispositivo in sequestro (ovvero dei dati contenuti nei *Cloud*, *App*, *Drive*, archivi multimediali, etc).

Così delineata la disciplina, sembra però confliggere con il generale divieto di sequestri indiscriminati e totalizzanti di massici dati informatici.

A ben vedere, poiché, ogni singola attività condotta nello *smartphone* è idonea ad interferire con le libertà della persona[36], sfiorando finanche i diritti di seconda e terza generazione[37], si impone un estremo rigore

nel valutare la proporzione tra contenuto del provvedimento ablativo ed esigenze di accertamento dei fatti[38]. Di contro, l'assenza di qualsivoglia limite previsto in tale specifico snodo procedurale, rischia di confliggere con i più recenti approdi della giurisprudenza interna che, proprio con riferimento allo *smartphone*, hanno decretato l'illegittimità di sequestri totalizzanti[39].

Per tale ragione, il punto di equilibrio tra attività investigativa e diritti coinvolti, dovrebbe essere quello di ammette ingerenze da parte della pubblica autorità solo nei casi previsti dalla legge, purché sia rispettato il principio di proporzionalità[40]. È infatti necessario specificare, nel provvedimento, un «"protocollo di ricerca" per la successiva perquisizione, che contenga l'indicazione di "parole chiave" specifiche rispetto all'oggetto di prova e collegate alla *res iudicanda*»[41].

La proposta in esame, invece, non limitando *ad origine* il perimetro delle operazioni di ricerca dei dati[42], rischia di configurare un'attività di indagine esplorativa[43], apparendo così in difformità con gli approdi della giurisprudenza sia interna, sia europea, che hanno decretato l'illegittimità di tali forme di acquisizione massiva ed indiscriminata.

2.4 *Segue*: i tempi del sequestro

Ulteriore profilo meritevole di essere analizzato è quello dei tempi del sequestro, con riferimento sia al dispositivo, sia alla copia dei dati. Per quanto attiene al dispositivo elettronico, la proposta prevede dei tempi stringenti per lo svolgimento delle operazioni tecniche[44] e, effettuata la duplicazione, il pubblico ministero deve disporre senza ritardo la restituzione dei dispositivi informatici, dei sistemi informatici o telematici, o delle memorie digitali all'avente diritto[45].

Diversamente, invece, non soddisfa la disciplina riservata ai tempi di restituzione della copia clone[46], atteso che si prevede una conservazione «fino alla sentenza o al decreto penale di condanna non più soggetti a impugnazione». A ben vedere, però, la restituzione dello *smartphone* non elimina il pregiudizio determinato dal mantenimento del vincolo sui dati informatici, sui quali non solo sussiste un vero e proprio diritto alla reintegrazione della *privacy*[47], ma tale diritto appare meritevole di una adeguata tutela, poiché tali informazioni costituiscono – come detto – la spina dorsale dell'essere digitale.

Non a caso, su tale specifico aspetto si sono strutturati alcuni Protocolli[48] finalizzati a garantire l'immediata restituzione sia del dispositivo, sia (e soprattutto) della copia integrale e di ogni altra eventuale copia estratta (art. 262, comma 1, c.p.p.)[49].

Il rischio è che il sequestro integrale dei dati, unito alla possibilità di detenere tale patrimonio informatico sino alla sentenza definitiva, trasformi l'atto investigativo in un atto esplorativo, con il pericolo – quantomeno astratto – che tale vincolo sulla copia forense, prolungato per anni, si possa prestare anche ai pericoli del dossieraggio.

2.5 *Segue:* il sequestro dei dati comunicativi

Altro aspetto cristallizzato nella proposta di legge, è quello del sequestro dei dati che prevede due procedure distinte che si differenziano in base alla tipologia dell'elemento da acquisire: i dati inerenti a programmi, informazioni, etc., possono essere acquisiti con il solo decreto autorizzativo del pubblico ministero, purché essi siano strettamente pertinenti al reato, in relazione alle circostanze di tempo, di luogo e alle modalità della condotta, nonché nel rispetto dei criteri di necessità e proporzione. Invece, per i dati c.d. comunicativi si prevede una seconda finestra di giurisdizione e un secondo decreto autorizzativo del giudice, qualora sussistono i presupposti di cui agli artt. 266, comma 1, e 267, comma 1, c.p.p.

Sotto un primo profilo, laddove entrano in gioco i dati inerenti alle comunicazioni e conversazioni, appare necessario il ricorso all'autorizzazione del giudice, nonché a limiti ben determinati per legittimare ogni compressione[50].

In tale contesto, l'introduzione di una doppia riserva per tali dati, stante l'espresso richiamo agli artt. 266, comma 1, e 267, comma 1, c.p.p., sanerebbe le incongruenze che separano l'acquisizione di dati comunicativi archiviati nei dispositivi elettronici, dall'acquisizione dei medesimi dati attraverso le operazioni di intercettazione[51]; ovvero le disparità di trattamento che sinora hanno contraddistinto la disciplina dei tabulati di traffico telefonico e telematico e quella del sequestro dei dati comunicativi presento nello *smartphone*.

Ciò che, però, non convince è la scelta di legittimare un sequestro *ad origine* integrale, con una duplicazione

totalizzante dei dati comunicativi, in difetto di specifiche ragioni che possono legittimare tale massiccia acquisizione di informazioni. In tal caso, vengono così copiate tutte le conversazioni archiate nel dispositivo, anche quelle inerenti a posizioni di terze persone, del tutto avulse dall'attività di indagine. A ben vedere, però, se non sussistono i presupposti della riserva di legge, dovrebbe essere precluso non solo il sequestro, ma anche la copia di quei dati.

2.6 *Segue*: l'acquisizione dei dati "non comunicativi"

La proposta di legge prevede che per tutti i *dati*, *informazioni* e *programmi*, non aventi carattere comunicativo, si procede con decreto motivato del pubblico ministero, purché sia rispettato il criterio di pertinenza rispetto al reato e in relazione alle circostanze di tempo e di luogo del fatto.

Mancherebbe, quindi, sia il controllo del giudice terzo, sia l'indicazione della gravità del reato, con espresso richiamo a casi e modi entro cui perimetrare l'ingerenza su tali dati.

Tuttavia, si è già detto che i dispositivi elettronici (e lo *smartphone* in particolare) hanno assunto la dimensione di un "nuovo luogo", al cui interno si dischiude un ambiente del tutto inedito, nel quale si estrinseca l'*essere digitale*; per tale ragione essi devono essere considerati come una vera e propria proiezione dell'individuo nello spazio virtuale, all'interno del quale sono esercitate (tra le altre cose) anche le libertà fondamentali tutelate dalla Costituzione[52].

Più nel dettaglio, *dati*, *informazioni* e *programmi*, indicati nella proposta di legge, altro non sono che elementi che consentono di mappare le abitudini di vita di un soggetto, sino a delineare le caratteristiche descrittive della persona stessa. La vastissima mole di informazioni attiene, infatti, a dati di geolocalizzazione, idonei a svelare luoghi visitati e percorsi effettuati[53]; file multimediali, che ricostruiscono i momenti della vita quotidiana, intima, familiare, etc.; dati lavorativi, sui quali non si può escludere la sussistenza del segreto professionale; documenti bancari; cronologia internet e molto altro ancora. Informazioni che impattano sugli artt. 13 e 14 Cost., nonché 8 C.e.d.u., il cui nucleo essenziale andrebbe posto sul piedistallo dell'inviolabilità, salvo riserva di legge rinforzata e riserva di giurisdizione[54].

Per disciplinare un atto idoneo a comprimere i diritti fondamentali, diviene necessaria una disposizione

normativa che soddisfi nell'*an* e nel *quomodo* la riserva di legge e di giurisdizione[55]. Ed allora, è proprio il primo snodo investigativo, ovvero quello del sequestro del dispositivo disciplinato al punto n. 1 dell'emendamento, che andrebbe presidiato, *ex ante*,da precise garanzie che limitano l'atto investigativo (a prescindere dalla natura comunicativa o meno dei dati presenti nel dispositivo), prevedendo – analogamente a quanto accade per le intercettazioni – casi e modi, nonché presupposti stringenti e rigoroso rispetto dei criteri di proporzionalità.

3. Riflessioni conclusive

È arduo sostenere come l'attuale disciplina non sia obsoleta e inadeguata difronte ai nuovi ritrovati della scienza e della tecnica. Tuttavia, se da un lato i tempi delle riforme non possono coincidere con la velocità del progresso, sotto altro profilo, la rapidità con cui la tecnica si evolve e si innesta nel procedimento penale non può avere come contraltare un legislatore, inattivo sulla materia, ormai dal 2008[56]. Imprescindibile è, dunque, una riforma.

Ed infatti, all'alba di una nuova era tecnologica, che pone l'intelligenza artificiale[57] come una imminente sfida per il giurista contemporaneo[58], non ci si può più concedere di indugiare sull'aggiornamento del catalogo delle attività investigative digitali, tra le quali spicca – ormai da tempo – quella del sequestro di *smartphone*, *computer*, *tablet*, etc.

Ciò posto, per circoscrivere in un perimetro normativo siffatte attività investigative, «non si può prescindere dall'introduzione di una disciplina che contempli l'espressa definizione dei presupposti del sequestro nella cornice del principio di proporzionalità»[59].

Pertanto, l'intervento del legislatore, ormai inevitabile, dovrebbe *in primis* limitare il ricorso allo strumento di indagine in esame e ricondurre l'azione investigativa nel perimetro della riserva di legge postulata dalla Costituzione a tutela di ogni diritto inviolabile.

Sotto il profilo procedimentale, inoltre, è condivisibile l'innesto di un segmento dedicato alla verifica del rispetto di queste condizioni, attraverso la valorizzazione del ruolo del giudice per le indagini preliminari, potenziando l'effettività del suo controllo ed ampliando il suo orizzonte conoscitivo.

Ed ancora, per la delicatezza strettamente connessa alle operazioni sui dati digitali, appare necessario il ricorso allo schema degli accertamenti tecnici irripetibili, meccanismo funzionale anche alla selezione dei soli dati rilevanti e all'insaturazione immediata del contraddittorio.

Infine, anche la previsione – di tempi stringenti, entro cui effettuare le operazioni tecniche e restituire sia il dispositivo, sia le copie dei dati digitali, diviene funzionale al rispetto del principio di proporzionalità. In tale ottica, è sicuramente auspicabile una scansione temporale prevista a pena di inammissibilità.

In attesa che il disegno di legge approdi alla Camera, l'auspicio è che il legislatore riesca ad individuare il punto di equilibrio tra accertamento del fatto e tutela dei diritti fondamentali, partendo da una constatazione: la tecnica è chiamata, alla stregua di ogni altra prova, a piegarsi alle regole e ai valori a cui si ispira il procedimento penale.

---

[1] Così, K. LA REGINA, *Il sequestro dei dispositivi di archiviazione digitale*, in *Penale DP*,Rivista, 2023, p. 429. Sul tema anche G. VICIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, 2012, p. 58. Sul più ampio tema delle garanzie da accordare alle prove digitali, A. CAMON, *Le riprese visive come mezzo di indagine*: *spunti per una riflessione sulle prove «incostituzionali»*, in *Cass. pen.*, 1999, p. 1211; L. FILIPPI, *L'*home watching*: documento, prova atipica o prova incostituzionale*, in *Dir. pen. proc.*, 2001, p. 97. Sui dati di geolocalizzazione, C. FANUELE, *La localizzazione satellitare nelle investigazioni penali*, Wolters Kluwer - Cedam, 2019; A. LARONGA, *Il pedinamento satellitare: un atto atipico lesivo dei diritti inviolabili?* in *Quest. Giust*., 2002, p. 1161; volendo, O. MURRO, *La geolocalizzazione tramite celle telefoniche. Soluzioni percorribili, in un mondo digitale in trasformazione*, in *Dir. pen. proc.*, 2023, p. 1079; sui dati presenti in bacheche *social*, C. CONTI, M. TORRE, *Spionaggio digitale nell'ambito dei* social network, in AA.VV., *Le indagini atipiche*, a cura di A. Scalfati, Giappichelli, II ed., 2019, p. 536.

[2] Approfondisce il rapporto tra diritto e tecnica, N. IRTI, E. SEVERINO, *Dialogo su diritto e tecnica*, Laterza, 2001, *passim*.; R. ORLANDI, *Una giustizia penale a misura di nemici?*, in *Riv. it. dir. proc. pen.*, 2020, p. 718. L'A. analizza l'incidenza degli strumenti di indagine digitale sul nucleo più intimo e inviolabile del diritto alla riservatezza.

[3] Cfr., M. DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen.*

giust., 2018, f. 5, p. 834. Parla di "intera nuda vita" dell'uomo contenuta nello *smartphone,* M. OLIVETTI, *Diritti fondamentali e nuove tecnologie*. *Una mappa nel dibattito italiano*, in *Rev. Estudos inst.*, 2020, p. 400.

[4] M. OROFINO, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, Giuffrè, 2008, p. 4.

[5] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. bras. dir. proc. pen.*, 2017, f. 2, p. 491.

[6] E. BASSOLI, *La disciplina giuridica della seconda vita in Internet: l'esperienza* Second Life, in *Inform. dir.*, 2009, n. 1, p. 165.

[7] Così, A. BARBERA, *I principi costituzionali della libertà personale*, Giuffrè, 1967, p. 52; F. MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Giappichelli, 1995, p. 12; C. MORTATI, *Istituzioni di diritto pubblico*, Tomo II, Cedam, 1976, p. 1040; R. NANIA, *La libertà individuale nella esperienza costituzionale italiana*, Giappichelli, 1989, p. 69.

[8] V. GREVI, *Libertà personale dell'imputato e costituzione*, Giuffrè, 1976, p. 1; ID., voce *Libertà personale dell'imputato*, in *Enc. dir*., XXIV, Giuffrè, 1974, p. 333.

[9] M.L. FERRANTE, *A proposito del principio di inviolabilità della libertà personale*, in *Arch. pen.*, 2012, f. 3, p. 588.

[10] Corte e.d.u.**, 27 settembre 2018, *Brazzi c. Italia*, ric. 57278/11, in** *Arch. pen*., 2019, f. 2, p. 52, con nota di F. FALATO, *(il)Legittimità sistemica delle perquisizioni. Tra normazione nazionale e giurisdizione europea.*

[11] L. COMOGLIO, *L'inutilizzabilità 'assoluta' delle prove incostituzionali,* in *Riv. dir. proc.,* 2011, p. 30.

[12] V. GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.* 1973, p. 341; P. GROSSI, *Introduzione ad uno studio dei diritti inviolabili nella Costituzione italiana*, Cedam, 1972. Riprende tale concetto anche C. CONTI, *Accertamenti del fatto e inutilizzabilità nel processo penale*, Giuffrè, 2007, p. 151.

[13] Commenta la sentenza, L. FILIPPI, *Il cellulare "contenitore" di corrispondenza anche se già letta dal destinatario*, in *questa Rivista* (web), 6 settembre 2023..

[14] Il riferimento è al d.d.l. n. 690, presentato dall'On. R.M.F. Scarpinato il 9 maggio 2023; nonché al d.d.l. 806, presentato dagli On. P. Zanetti e G. Bongiorno il 19 luglio 2023. I disegni di legge sono stati riuniti e il testo che è stato prescelto è quello del d.d.l. 806. www.senato.it/leg/19/BGT/Schede/Ddliter/57327.htm. Per un commento, A. CHELO, *Tanto tuonò che piovve: il nuovo sequestro dei dispositivi informatici*, in *questa* Rivista (web) 29 febbraio 2024; K. LA REGINA, *Il sequestro dei dispositivi*, cit.

[15] Per una analisi si rinvia https://www.senato.it/leg/19/BGT/Schede/Ddliter/57327.htm.

[16] Cfr., C. Cost., 27 luglio 2023, n. 170, cit.

[17] Il riferimento è al Protocollo della Procura Generale della Repubblica di Trento, del 22.10.2021, in *Penale DP*,(web), 19 novembre 2021, con nota di L. FILIPPI, *Sequestro dei dispositivi elettronici: nota della Procura Generale di Trento*.

[18] L'emendamento prevede che dopo l'articolo 254 *bis* del codice di procedura penale è inserito il seguente: «Art. 254-ter. (Sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate e ricevute) – (1). Nel corso delle indagini preliminari, il giudice per le indagini preliminari, a richiesta del pubblico ministero, dispone con decreto motivato il sequestro di dispositivi e sistemi informatici o telematici, o di memorie digitali, necessari per la prosecuzione delle indagini in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del criterio di proporzione. Il decreto che dispone il sequestro è immediatamente trasmesso, a cura della cancelleria, al pubblico ministero, che ne cura l'esecuzione. (2). Il pubblico ministero può procedere all'esecuzione personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria. Il sequestro è eseguito con modalità tecniche idonee ad evitare l'alterazione o la perdita dei dati e, a tal fine, il pubblico ministero adotta le misure tecniche necessarie o impartisce specifiche prescrizioni. Copia del decreto di sequestro è consegnata all'interessato, se presente. (3). Il sequestro è immediatamente revocato dal pubblico ministero con decreto motivato, quando risultano mancanti, anche per fatti sopravvenuti, le condizioni di applicabilità previste dal comma 1. Il decreto è notificato a coloro che hanno diritto di proporre impugnazione. Se vi è richiesta di revoca dell'interessato, il pubblico ministero, quando ritiene che essa vada anche soltanto in parte respinta, la trasmette al giudice, cui presenta richieste

specifiche nonché gli elementi sui quali fonda le sue valutazioni. La richiesta di revoca è trasmessa non oltre il giorno successivo a quello del deposito nella segreteria. (4). Quando non è possibile, per la situazione di urgenza, attendere il provvedimento del giudice, il sequestro è disposto con decreto motivato dal pubblico ministero. Negli stessi casi, prima dell'intervento del pubblico ministero, al sequestro procedono ufficiali di polizia giudiziaria, i quali, nelle quarantotto ore successive, trasmettono il verbale al pubblico ministero del luogo in cui il sequestro è stato eseguito. Questi, se non dispone la restituzione delle cose sequestrate, richiede al giudice la convalida e l'emissione del decreto previsto dal comma 1 entro quarantotto ore dal sequestro, se disposto dallo stesso pubblico ministero, o dalla ricezione del verbale, se il sequestro è stato eseguito di iniziativa dalla polizia giudiziaria. (5). Il sequestro perde efficacia se non sono osservati i termini previsti dal comma 4 ovvero se il giudice non emette l'ordinanza di convalida entro dieci giorni dalla ricezione della richiesta. Copia dell'ordinanza è immediatamente notificata alla persona alla quale le cose sono state sequestrate. (6). Entro cinque giorni dal deposito del verbale di sequestro, il pubblico ministero avvisa la persona sottoposta alle indagini, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione, la persona offesa dal reato e i relativi difensori, del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico per la duplicazione del contenuto dei dispositivi informatici, dei sistemi informatici o telematici, o delle memorie digitali in sequestro, e della facoltà di nominare consulenti tecnici. Il pubblico ministero può disporre che sia effettuata la duplicazione anche dei dati, delle informazioni o dei programmi accessibili da remoto dal dispositivo in sequestro. Tra l'avviso e la data fissata per il conferimento dell'incarico non può intercorrere un termine superiore a dieci giorni. Si applicano le disposizioni dell'articolo 364, comma 2. 6. (7). Il pubblico ministero può autorizzare la persona sottoposta alle indagini, la persona offesa dal reato, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione, i difensori e i consulenti tecnici eventualmente nominati, che ne facciano richiesta, a partecipare a distanza al conferimento dell'incarico. (8). Fermo il diritto dei soggetti indicati al comma 6 di assistere al conferimento dell'incarico, i difensori nonché i consulenti tecnici eventualmente nominati hanno diritto, altresì, di partecipare allo svolgimento delle operazioni di duplicazione e di formulare osservazioni e riserve. (9). La duplicazione avviene su adeguati supporti informatici mediante una procedura che assicuri la conformità del duplicato all'originale e la sua immodificabilità. (10). Nei procedimenti di cui agli articoli 406, comma 5-bis e 371-bis, comma 4-bis, nonché quando sussiste un pericolo per la vita o l'incolumità di una persona o la sicurezza dello Stato, ovvero un pericolo di concreto pregiudizio per le indagini in corso, o un pericolo attuale di cancellazione o dispersione dei dati, delle informazioni o dei programmi, la duplicazione può avvenire in deroga al disposto dei commi 6, 7 e 8, con modalità tecniche idonee ad assicurare la conformità del duplicato all'originale e la sua immodificabilità. (11). Fermo quanto stabilito dal comma 3, il pubblico ministero, effettuata la duplicazione, dispone senza ritardo la restituzione dei dispositivi informatici, dei sistemi informatici o telematici, o delle

memorie digitali all'avente diritto. Non si fa luogo alla restituzione e il sequestro è mantenuto ai fini preventivi quando il giudice provvede a norma dell'articolo 321. (12). Effettuata l'analisi del duplicato informatico, il pubblico ministero procede con decreto motivato al sequestro dei dati, delle informazioni e dei programmi strettamente pertinenti al reato in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione. Qualora il pubblico ministero intenda procedere al sequestro dei dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute, lo richiede al giudice per le indagini preliminari, che provvede con decreto motivato, disponendo il sequestro in presenza dei presupposti di cui al primo periodo e agli articoli 266, comma 1, e 267, comma 1. Nei procedimenti rispetto ai quali trova applicazione l'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito con modificazioni dalla legge 12 luglio 1991, n. 203, il giudice dispone il sequestro in presenza dei presupposti indicati nella stessa norma. Copia del decreto di sequestro è notificata all'avente diritto alla restituzione del dispositivo. (13). I dati, le informazioni e i programmi sottoposti a sequestro ai sensi del comma 12 sono riversati su idonei supporti con modalità tecniche idonee ad assicurare la loro conformità ai medesimi dati, informazioni e programmi contenuti nel duplicato e la loro immodificabilità. I supporti di cui al periodo precedente sono acquisiti al fascicolo. (14). In caso di sequestro di comunicazioni, di conversazioni o di corrispondenza informatica inviate e ricevute si applicano, in quanto compatibili, gli articoli 269, commi 2 e 3, 270, commi 1, 2 e 3, 270-bis e 271. (15). Salvi i casi di cui all'articolo 419, comma 3, dopo l'esercizio dell'azione penale il sequestro ai sensi dei commi 1 e 12 è disposto dal giudice che procede. In tal caso, alla duplicazione si procede con perizia. (16). La conservazione del duplicato informatico avviene presso la procura della Repubblica, in luogo protetto da specifiche misure di sicurezza, con modalità tali da assicurare l'assoluta riservatezza. (17). Il duplicato informatico è conservato fino alla sentenza o al decreto penale di condanna non più soggetti a impugnazione. Tuttavia gli interessati, quando i dati, le informazioni e i programmi contenuti nel duplicato non sono necessari per il procedimento, possono chiederne la distruzione, a tutela della riservatezza, al giudice che ha disposto o convalidato il sequestro di cui al comma 1. Il giudice decide in camera di consiglio a norma dell'articolo 127. In caso di archiviazione, il giudice dispone l'immediata distruzione del duplicato informatico, salvo che, anche su istanza di uno dei soggetti indicati dall'articolo 409, comma 2, ritenga sussistenti specifiche esigenze che ne impongono la conservazione. (18). La distruzione, nei casi in cui è prevista, viene eseguita sotto controllo del giudice. Dell'operato è redatto verbale. (19). Contro i provvedimenti emessi ai sensi dei commi 1, 4 e 12 è ammesso riesame ai sensi dell'articolo 257.».

[19] Così, A LOGLI, *Sequestro probatorio di un personal computer. Misure* ad explorandum *e tutela della corrispondenza elettronica* in *Cass. pen.*, 2007, p. 2595.

[20] Cass., sez. VI, 3 febbraio 2022, n. 17878 in *C.E.D. Cass.*,n. 283302. Sui rischi di un sequestro *omnibus*, M. PITTIRUTI, *Dalla Corte di Cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in *Sistema penale*, (web), 14 gennaio 2021. Sulla necessità di perimetrare l'attività di sequestro dei dati, A. DEL GIUDICE, *La Cassazione sul sequestro probatorio informatico: non si guardi al contenitore, ma al contenuto!*, in *Foro It.*, 2021, p. 416. Sul tema, anche, Cass., sez. un., 20 luglio 2017, n. 40963, in *Cass. pen.*, 2017, p. 4303, con nota di A. MARI, *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati*.

[21] C. FONTANI, *Il sequestro probatorio di un documento informatico: bilanciamento tra esigenze investigative e baluardi difensivi*, in *Dir. pen. proc.*, 2022, p. 239.

[22] Con specifico riferimento allo *smartphone*, si rimanda a C. cost., 12 gennaio 2023, n. 2, in *Giur. cost.*, 2023, p. 18, con nota di F. LOSURDO, *Nucleo essenziale della libertà di comunicazione e riserva di giurisdizione. Esiste un "diritto al mezzo"?*.

[23] M.R. FERRARESE, *Diritto sconfinato. Inventiva giuridica e spazi nel mondo globale*, Laterza, 2006; G. TEUBNER, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, Armando, 2005, che affronta il tema delle «Costituzioni infinite».

[24] D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, 2020, p. 3. Sul tema anche, L. FERRAJOLI, *Costituzionalismo principialista e costituzionalismo garantista*, in *Giur. cost.*, 2010, p. 2781; Si veda, G. LEO, *Politiche sanzionatorie e sindacato di proporzionalità*, *Dir. pen. cont.*,(web), 22 dicembre 2017, p. 7; D. ZOLO, *Teoria e critica dello Stato di diritto*, in AA.VV., *Lo Stato di diritto. Storia, teoria, critica*, a cura di O. Costa, E. Santoro, Feltrinelli, 2006, p. 45.

[25] Rappresenta una «sfera di esplicazione della libertà della persona di cui esso ne è la proiezione spaziale» per S. PISANI, *La tutela penale della "riservatezza": aspetti processuali,* in *Riv. it. dir. proc. pen.*, 1967, 785.

[26] C. cost., 31 maggio 1995, n. 210, in *Dir. pen. proc.*, 1996, p. 703 che riscontra la violazione dell'*habeas corpus* anche nei provvedimenti coercitivi che si traducono in una menomazione o mortificazione della dignità o del prestigio della persona. In dottrina, P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Il Mulino, 1984, p. 111; P.F. GROSSI, *Libertà personale, libertà di circolazione ed obbligo di residenza dell'imprenditore fallito*, in *Giur. cost.*, 1962, p. 205;

[27]Sul tema, C. Cost., 21 febbraio 1962, n. 30, in *Giur. cost.*, 1962, p. 242. In dottrina analizza in rapporto tra l'art. 13 Cost. e la "dignità umana", M. RUOTOLO, in *Art. 13*, in AA.VV., *Commentario alla Costituzione*, a cura di R. Bifulco, A. Celotto, M. Olivetti, Utet, 2006, p. 323.

[28] C., cost., 25 marzo 1987, n. 88, in *Il Foro it.*, 1988, p. 381.

[29] Sarebbe, invero, «grottesco» sostenere il contrario, così A. CAMON, *Cavalli di Troia in Cassazione*, in *Arch. nuova proc. pen.*, 2017, f. 1, p. 95.

[30] Sul tema, M. DANIELE, Habeas corpus. *Manipolazioni di una garanzia*, Giappichelli, 2017, p. 29; B. GALGANI, *Giudizio penale,* habeas data *e garanzie fondamentali*, in *Arch. pen*., (web), 8 febbraio 2019; S. SIGNORATO, *Le indagini digitali*. *Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 75. Per un approfondimento sui profili ampi delle libertà fondamentali nel nuovo millennio, S. RODOTA', *Libertà personale. Vecchi e nuovi nemici*, in *Quale libertà. Dizionario minimo contro i falsi liberali*, a cura di M. Bovero, Laterza, 2004, p. 52. Sul

[31] Sull'ampio tema dei vizi dell'atto investigativo e le eventuali ricadute sul successivo sequestro, P. FERRUA, *Perquisizioni illegittime e sequestro*, in *Giur. cost.*, 2019, p. 2581.

[32] P. TONINI, *Manuale di procedura penale*, Giuffrè, 2020, p. 358. Le argomentazioni sono riprese da M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale. La prova informatica nella legge 18 marzo 2008, n. 48*, in *Inf. diritto*, XLI annata, Vol. XXIV, 2015, n. 1-2, p. 71.

[33] M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, p. 442.

[34] M. MATTIUCCI, *Le indagini sui reperti invisibili*. High tech crime, in AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze*, a cura di D. Curtotti, L. Saravo, Giappichelli, 2013, p. 712.

[35] S. ATERNO, *Acquisizione ed analisi della prova informatica*, in *Dir. pen. proc.*, 2008, p. 61.

[36] In tema, L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei* social network*. Aspetti penali*, in *Giur. merito*, 2020, p. 2532.

[37] Analizza i diritti coinvolti nelle attività di indagine digitale, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, *passim*. Sui diritti emergenti in tema di captatore informatico, W. NOCERINO, *Le Sezioni Unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale*, in *Cass. pen*., 2016, p. 3566.

[38] Sul tema, L. NULLO, *Sequestro probatorio di materiale documentativo e principi di adeguatezza e proporzionalità*, in *Proc. pen. giust.*, 2020, f. 3, p. 660; M PITTIRUTI, *Adeguatezza e proporzionalità nel sequestro di un sistema informatico*, in *Dir. internet*, 24 luglio 2019, p. 777.

[39] Cass. VI, 22 settembre 2020, n. 35265, in *C.E.D. Cass.*, n. 279949.; Id., 9 dicembre 2020, n. 6623, in *C.E.D.* Cass., n. 280838; Id., 19 gennaio 2018, n. 9989, *ivi*, n. 272439; Id. Sez. VI, 15 aprile 2014, n. 31735, *ivi*, n., 260068. In tema, anche, S. CARNEVALE, Copia e restituzione dei documenti informatici sequestrati: il problema dell'interesse ad impugnare, in Dir. pen. e proc., 2009.

[40] Si veda, *ex multis*, Corte EDU, 16 febbraio 2000, *Amann c. Svizzera*.

[41] Corte EDU, sent., 28 gennaio 2003, *Peck c. Regno Unito*, par. 76. Sulla specifica questione, F.M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., 19.

[42] La giurisprudenza ha, da sempre, decretato l'illegittimità del decreto di acquisizione *omnibus* privo di ogni indicazione in ordine al tipo di dati da acquisire. Così, Cass., sez. II, 23 marzo 2023, n. 17604, in *C.E.D. Cass.*,n. 284393.

[43] In tema, G. COSTABILE, Scena criminis, *documento informatico e formazione della prova penale*, in *www.altalex.it*, 16 aprile 2004. Sul tema, L. NULLO, *Sequestro probatorio di materiale documentativo e principi di adeguatezza e proporzionalità*, in *Proc. pen. giust.*, 2020, f. 3, p. 660; M PITTIRUTI, *Adeguatezza e proporzionalità nel sequestro di un sistema informatico*, in *Dir. internet*, 24 luglio 2019, p. 777.

[44] Entro cinque giorni dal deposito del verbale di sequestro le parti devono essere avvisate della data per il conferimento dell'incarico per la duplicazione del contenuto dei dispositivi informatici e tra l'avviso e la data fissata per il conferimento dell'incarico non può intercorrere un termine superiore a dieci giorni.

[45] Se da un lato si apprezza l'introduzione di un termine (cinque giorni) previsto per l'inizio delle operazioni, sotto altro profilo, la scansione temporale potrebbe essere rafforzata non solo dall'introduzione di termini perentori, ma anche da un termine preciso per la restituzione della *res*, atteso che la locuzione *senza ritardo* può dar luogo a prassi difformi e a indebiti trattenimenti di dispositivi elettronici.

[46] È noto che «il documento informatico trasferisce il proprio valore anche sulla copia». Così, Cass., sez. un., 20 luglio 2017, n. 40963, in *Dir. pen. cont.*, Rivista, 2017, f. 11, p. 157, con nota di G. TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare*: revirement *delle Sezioni Unite*.

[47] Cass., sez. un., 20 luglio 2017, n. 40963, cit. In dottrina, S. CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc.*, 2009, p. 469.

[48] Il riferimento è al Protocollo della Procura Generale della Repubblica di Trento, del 22.10.2021, cit.

[49] Nel testo del Protocollo si legge espressamente che il fine *è quello di evitare una* «**inammissibile ed illecita diffusione di dati che attengono alla sfera personale**,**intima** *ed***inviolabile di ogni individuo**».

[50] I riferimenti all'ampia tematica delle tutele da accordare ai dati comunicativi sono molteplici, tra i tanti, D.N. CASCINI, *Messaggistica tra telefonia* Blackberry*: nuove prassi devianti al limite dell'abuso del processo*, in *Arch. pen.*, 2016, f. 2, p. 1; F. CERQUA, *Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica*, in *Dir. pen. cont.*, (web), 23 luglio 2015; G. PADUA, *L'accesso alla casella* e-mail *e l'acquisizione dei contenuti*, cit., p. 586; M. TORRE, WhatsApp *e l'acquisizione processuale della messagistica istantanea*, in *Dir. pen. proc.*, 2020, p. 1282; F. ZACCHE', *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 2013, f. 3, p. 108. Sul vasto tema delle intercettazioni e sui controlli sulla simultaneità tra controllo effettuato e trasmissione della *e-mail*, E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 535; A. CAPONE *Intercettazione e costituzione*, cit., p. 1263; W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*,Wolters Kluwer – Cedam, 2021.

[51] K. LA REGINA, *Il sequestro dei dispostivi di archiviazione digitale*, cit., p. 432

[52] C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. proc.*, 2018, p. 1210.

[53] Cass., sez. VI, 14 aprile 2023, n. 15836**,** in *Giur. it.*, 2023, p. 1676, con nota di, volendo, O. MURRO, *L'utilizzabilità dei dati di geolocalizzazione: le risposte della giurisprudenza* vs *il roboante silenzio normativo.*

[54] Sul tema, ampiamente, C. CONTI, *Accertamento del fatto*, cit., p. 230.

[55] C. CONTI, M. TORRE, *Spionaggio digitale*, cit., II ed., p. 536*;* L. FERRAJOLI, *Costituzionalismo principialista e costituzionalismo garantista*, in *Giur. cost.*, 2010, p. 2781; G. WEBBER, *On the Loss of Rights*, in *Proportionality and the Rule of Law. Rights, Justification, Reasoning*, a cura di G. Huscroft, B. Miller -G. Webber, Cambridge, 2014, p. 123; D. ZOLO, *Teoria e critica dello Stato di diritto*, in AA.VV., *Lo Stato di diritto. Storia, teoria, critica*, a cura di P. Costa, D. Zolo, Feltrinelli, 2006, p. 45.

[56] Il riferimento è alla L. n. 48 del 2008; per un commento, AA.VV., *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, a cura di G. Corasaniti, G. Corrias Lucente, Pacini, 2009.

[57] In tema, AA.VV., *Intelligenza artificiale e processo penale indagini, prove e giudizio*, a cura di G. Di Paolo, L. Pressacco, Editoriale Scientifica, 2022; L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Giuffrè, 2022, p. 40; M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2019; V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in AA.VV., *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di U. Ruffolo, Giuffrè, 2020, p. 547; P.P. PAULESU, *Intelligenza artificiale e giustizia penale. Una lettura attraverso i principi,* in *Arch. pen. web.*, 2022, p. 1; S. QUATTROCOLO, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *Legislazione pen.*, (web), 18 dicembre 2018; G. UBERTIS, *Intelligenza artificiale e diritto penale*, in *Dir. pen. cont., Riv. trim.*, 2020, n. 4, p. 75.

[58] AA.VV., *Diritto e intelligenza artificiale*, a cura di G. Alpa, Pacini, 2020; AA.VV., *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di S. Dorigo, Pacini, 2020.

[59] Così, K. LA REGINA, *Il sequestro dei dispositivi*, p. 432.