ANTONIO VELE

Documento informatico e tutela della riservatezza nel processo penale: aspetti problematici.

L'articolo tratta di alcuni profili critici relativi all'acquisizione del documento informatico, in particolare della tutela della privacy.

The article is about some critical profiles in regard to the acquisition of the informatic document, with particular focus on privacy protection.

1. Premessa

Il documento informatico è un documento non cartaceo formato dai programmi (*software*) di un calcolatore elettronico e, contemporaneamente alla sua formazione, registrati in un apposito spazio del calcolatore medesimo (*hardware*) o su strumenti di supporto elettronico o digitale, quali *pen-drives*, *dvd*, *cd-rom*, etc.[1]; possiamo, pertanto, definire il documento informatico come qualsiasi *file* avente un elemento rappresentativo espresso in linguaggio binario: un testo, un'immagine, un suono, quindi, anche una pagina *web* o una *e-mail*[2].

In quest'ambito ontologico, la concezione tradizionale del documento resta

[1] In riferimento a tale nozione di documento informatico cfr. L. P. COMOGLIO, *Le prove civili*, Torino, 2010, 529.

[2] Su questa definizione v. G. VACIAGO, *Profili processuali delle indagini informatiche*, in *Diritto dell'internet*, a cura di G. Cassano-G. Scorza-G. Vaciago, Padova, 2013, 640. In informatica e nella teoria dell'informazione, il *bit* (inteso come "cifra binaria", dall'inglese "*binary digit*") può essere definito come unità elementare dell'informazione trattata da un elaboratore. In questo contesto, il *bit* è dunque uno dei due simboli del sistema numerico binario, classicamente chiamati zero (0) e uno (1): il bit rappresenta quindi, in realtà, l'unità di definizione di uno stato logico, la cui rappresentazione è costituita dai soli valori 0 e 1. Ai fini della programmazione, è comune raggruppare sequenze di bit in entità più vaste che possano assumere valori in intervalli più ampi di quello consentito da un singolo bit; questi raggruppamenti contengono generalmente un numero di stringhe binarie pari a una potenza binaria, pari cioè a 2n; il più comune tra questi raggruppamenti è il *byte* (o "ottetto"), corrispondente a 8 *bit*, che costituisce l'unità di misura più utilizzata in campo informatico. Storicamente, un *byte* era il numero di bit utilizzati per codificare un "singolo carattere di testo" in un computer; il *byte* è anche la quantità minima d'informazione normalmente indirizzabile da parte di un microprocessore e utilizzabile nella programmazione ed è perciò divenuto l'elemento base come unità di misura delle capacità di memoria. Il *byte*, in quanto tipicamente formato da 8 *bit*, è in grado di assumere 28 = 256 possibili valori (da 0 a 255), cui corrispondono altrettante diverse possibili combinazioni di una sequenza di 8 bit (ovvero di 8 "0" e/o "1"). In prospettiva generale cfr. R. BORRUSO, voce «*Informatica giuridica*», in *Enc. dir.*, *Agg.*, I, Milano, 1997, abcd.

ancora valida[3]: il documento è uno strumento che fa conoscere un fatto e questa definizione può essere estesa anche al documento informatico.
Con il documento, infatti, l'effetto conoscitivo viene realizzato attraverso la tecnica della rappresentazione, ossia il soggetto non ha diretta percezione di un determinato fatto, ma si rappresenta (e conosce) quello stesso fatto attraverso le "sensazioni" che gli provengono dalla percezione del documento; tale ricostruzione concettuale è applicabile anche al documento informatico, sebbene quest'ultimo risulti "dematerializzato"[4], nel senso che sussiste a prescindere «dal supporto fisico sul quale è incorporato»[5]. Vi è quindi una necessaria base materiale che contiene la rappresentazione informatica di dati e fatti[6].

2. Acquisizione del documento informatico

Passando ad esaminare il profilo dell'acquisizione del documento informatico, diversi sono i nodi da sciogliere sul piano processuale.
Il documento informatico, infatti, implica l'adozione di tecniche peculiari volte a reperirlo, che devono necessariamente tener conto della sua fragilità,

---

[3] Resta attuale la concezione tradizionale, in quanto il documento è una cosa che ha in sé la virtù del far conoscere e quest'ultima è dovuta a ciò che si definisce il contenuto rappresentativo, sul punto, v. F. CARNELUTTI, Documento, in *Nss. Dig. It.*, VI, Torino, 1960, 86; più di recente in tema di prova documentale cfr. L. KALB, *Il documento nel sistema probatorio*, Torino, 2000, 95; A. LARONGA, *La prova documentale nel processo penale*, Torino, 2004, 10 ss.; volendo, A. VELE, *Art. 234 c.p.p.*, in *Commento codice di procedura penale*, a cura di Tranchina, Milano, 2008, I, 1765 ss.;

[4] L'aggettivo "dematerializzato" fa comprendere bene la caratteristica del documento informatico, vale a dire che il contenuto del documento informatico è autonomo dal supporto sul quale viene di volta in volta trasferito, così, F. ALCARO, *Riflessioni, vecchie e nuove in tema di beni immateriali. Il diritto d'autore nell'era digitale*, in *Rass. Dir. civ.*, 2006, 951.

[5] In tal senso, P. TONINI, *Manuale di procedura penale*, Milano, 2017, 365-366; l'Autore, alla luce del progresso tecnologico, osserva che «oggi i metodi di incorporamento sono due: quello analogico e quello digitale. *a*) attraverso il *metodo analogico* la rappresentazione è incorporata su di una base materiale mediante grandezze fisiche variabili con continuità. L'incorporamento è "materiale" nel senso che la rappresentazione esiste soltanto unitamente a quella base materiale su cui è incorporata; detto altrimenti, la rappresentazione non esiste senza quel supporto fisico sul quale è stata incorporata. Lo strumento che opera l'incorporamento può essere manuale (es. scrittura o disegno) o automatico (es. fotografia, fonografia o cinematografia);
b) attraverso il *metodo digitale* la rappresentazione è incorporata su di una base materiale mediante grandezze fisiche variabili con discontinuità: si tratta di numeri, zero e uno (presenza o assenza di segnale). Il dato che contiene l'informazione è denominato informatico ed è composto dalla sequenza di *bit*. Il documento informatico ha la caratteristica di essere "de materializzato", nel senso che il documento esiste indifferentemente dal supporto fisico sul quale è incorporato, anche se per la sua esistenza, richiede comunque l'incorporamento su di una base materiale: *hard disk*, *pen drive*, *CD* o altro strumento idoneo. La caratteristica del documento informatico, ed il suo pregio, è quella di essere trasferibile con rapidità da un supporto ad un altro, rimanendo identico».

[6] Cfr. nota 5; in argomento v. P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. e proc.*, 2009, 401 e ss.

essendo lo stesso suscettibile di alterazioni o danneggiamenti (anche involontari: si pensi ad una operazione messa in atto da un soggetto non adeguatamente preparato da un punto di vista tecnico).
Su queste basi, si tratta di individuare le modalità per acquisire i dati presenti in un supporto informatico, occorre cioè recuperare gli elementi di prova senza alterare il sistema informatico in cui essi si trovano[7].
In questa prospettiva, la legge n. 48 del 2008, di ratifica e di esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001, prevede alcune cautele; il legislatore ha modificato, infatti, alcune norme del III e del IV libro del codice di procedura penale, in ordine a strumenti d'indagine sui sistemi o programmi informatici e telematici (anche se salvaguardati da misure di sicurezza), al fine di assicurare la conservazione dei dati originali, impedirne l'alterazione nel corso delle operazioni di ricerca delle fonti di prova, garantire la conformità della copia all'originale e l'immodificabilità della stessa (quando si procede ad una duplicazione), dotare di sigilli informatici i documenti[8].

---

[7] P. PAULESU, *Art. 354, c.p.p.,* in *Codice di procedura penale commentato*, a cura di Giarda-Spangher, 2010, 4267 ss., sul punto si è osservato come «"le tracce digitali" costituiscono ormai elementi cognitivi di primaria importanza nell'ambito dell'investigazione criminale. Sennonché, si sa che il dato informatico, strutturalmente "immateriale", risulta fatalmente esposto ad un elevato rischio di dispersione ed alterazione. Labilità dell'elemento cognitivo, urgenza della sua captazione, non dispersione dello stesso sono tutti fenomeni suscettibili di incoraggiare prassi investigative disinvolte. Donde l'esigenza di predisporre alcuni protocolli operativi preordinati ad assicurare la genuinità e la conservazione della *digital evidence*».

[8] Con la legge del 18 marzo 2008 n. 48 il legislatore ha modificato alcune norme del codice di procedura penale, all'art. 244, comma 2, c.p.p. sono state aggiunte le parole: «anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»; all'art. 247 c.p.p., che concerne casi e forme delle perquisizioni, è stato inserito il comma 1-bis: «Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»; all'art. 254 c.p.p., riguardante il sequestro di corrispondenza, è stato sostituito il primo comma: «Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato»; all'art. 254 c.p.p. è stato sostituito il secondo comma:« Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli o alterarli e senza prendere altrimenti conoscenza del loro contenuto»; è stato aggiunto l'art. 254-bis c.p.p.: «L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è,

Tale legge, però, non ha regolamentato nello specifico le operazioni (il metodo) di acquisizione di notizie informatiche, in ragione dei diversi protocolli operanti in materia e della valutazione che questi risultano condizionati da una continua evoluzione tecnologica.
Analizzando le norme modificate con la legge n. 48 del 2008 (artt. 244, 247, 254, 254-bis, 256, 259, 260, 352, 353, 354 c.p.p.) risulta evidente come le attività di indagine degli elementi informatici rientrino nel novero dei mezzi tipici di ricerca, recependone la disciplina: di qui una serie di problemi interpretativi sul piano della tutela dei diritti fondamentali dell'individuo e della qualità del giudizio (affidabilità della prova). Problemi che derivano dalla difficoltà, come si è detto, di disciplinare per legge le procedure acquisitive dei documenti informatici.
Su questo terreno, occorre concentrare l'attenzione sulle modalità di recupero del documento informatico; una volta individuato, sul piano investigativo, il supporto digitale, è infatti necessario procedere preliminarmente all'acquisizione della *bit-stream image*[9], anche nel caso di

comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali»; all'art. 256 c.p.p. che riguarda il dovere delle persone indicate negli artt. 200 e 201 c.p.p. di consegnare immediatamente atti e documenti, sono state aggiunte le parole: «nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto»; all'art. 259, comma 2, c.p.p. riguardante l'obbligo del custode delle cose sequestrate, è stato aggiunto il periodo «Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria»; all'art. 260, comma 1, in relazione al sigillo delle cose sequestrate con appositi mezzi, sono state inserite le parole: «anche di carattere elettronico o informatico, idoneo a indicare il vincolo imposto a fini di giustizia»; nell'art. 352 c.p.p., che riguarda le perquisizioni a i iniziativa della polizia giudiziaria, è stato inserito il comma 1-bis: «Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi»; all'art. 353 c.p.p. che prevede che il pubblico ministero autorizzi la polizia giudiziaria a ricercare notizie utili all'assicurazione delle fonti di prova non solamente con l'immediata apertura dei plichi, ma anche (sono state inserite le parole) con «l'accertamento del contenuto» della corrispondenza informatica; all'art. 354 c.p.p., riguardo «accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro», è stato aggiunto: «In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

[9] V. S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. e proc.*, 2008, Dossier, *La prova scientifica nel processo penale*, 61, tale creazione viene resa non modificabile mediante determinati meccanismi ed in merito si osserva che «questa fase acquisitiva viene effettuata attraverso la *bit-stream image*, ovvero la realizzazione di una "immagine" *bit* a *bit* del contenuto del supporto posto

attivazione di accertamenti urgenti e/o ispezioni, sempreché non occorrano diverse ore per effettuare tale operazione, in modo da evitare problematiche sull'alterazione dei dati nella fase di analisi degli stessi[10].

La predetta acquisizione, ove effettuata in precedenza (ad esempio prima del sequestro), deve avvenire in modo tale da assicurare la massima corrispondenza fra l'originale e la copia[11].

Nella fase di acquisizione occorre redigere una "relazione tecnica", in modo da consentire alle parti e al giudice di verificare l'ammissibilità, l'utilizzabilità e l'attendibilità della prova. Ecco allora che, in una prospettiva de iure condendo, parrebbe necessario introdurre l'obbligo di redigere un verbale, a pena di inutilizzabilità della prova documentale informatica[12]. Tale verbale

---

sotto sequestro che consente di operare l'analisi forense su un hard disk praticamente identico all'originale: sia sotto il profilo logico sia sotto quello fisico». Tali cautele sono importanti al fine di evitare che un successivo accesso ad un *file* tramite dispositivo (tipo *personal computer*) possa essere modificato o alterato; gli aspetti problematici dell'analisi digitale si colgono prevalentemente nella fase di ricerca del documento informatico.

[10] Basti pensare che ad oggi i tempi di copia sono di circa 2 giga al minuto, per cui, ad esempio, per un *hard disk* di un *terabyte* saranno necessarie 8 ore circa per effettuare una *bitstream image* (cfr. G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., 648).

[11] G. VACIAGO, *Profili processuali delle indagini informatiche*, cit., 651, sul punto si è osservato come «è evidente che, nel momento stesso in cui venga rispettata la procedura di acquisizione *bitstream* dell'immagine del disco e sia verificata, attraverso il calcolo dell'algoritmo di *hash*, la perfetta identità della copia, non vi sono ragioni per ritenere irripetibile tale accertamento tecnico». In tale contesto è utile ricordare che secondo un orientamento del giudice di legittimità non possono essere invocate le garanzie previste per gli accertamenti tecnici irripetibili, visto che l'attività di estrazione di copia dei file da un computer non determina la irriproducibilità di informazioni identiche a quelle contenute nell'originale, Cass., Sez. III, 24 novembre 2010, Malfanti, in *Mass. Uff.,* n. 248767; Id., Sez. I, 26 febbraio 2009, Ammutinato, *ivi*, n. 243922; Id., Sez. I, 25 febbraio 2009, Dell'Aversano, *ivi*, n. 243495, secondo cui non dà luogo ad accertamento tecnico irripetibile la lettura dell'*hard disk* di un computer sequestrato che è attività di polizia giudiziaria volta, anche con urgenza all'assicurazione delle fonti di prova.

[12] Tale riflessione potrebbe far emergere il discorso sull'utilizzabilità della prova, in assenza della predetta regola (obbligo di redigere il verbale). In dottrina risultano orientamenti opposti in tema di prova incostituzionale (e prova illecita), da un lato c'è chi sostiene che la mancanza di regole probatorie implica l'utilizzabilità processuale del relativo dato probatorio anche in ragione del rapporto gerarchico tra norma costituzionale e norma ordinaria, F. CORDERO, *Tre studi sulle prove penali*, Milano, 1963, 63 e 149; ID., *Procedura penale*, Milano, 2003, 630 ss.; G. LOZZI, *Lezioni di procedura penale*, Torino, 2004, 226; N. GALANTINI, *Inutilizzabilità*, in *Enc. dir.*, I, Milano, 1997, 700; C. CONTI, *Inutilizzabilità*, in *Enc. giur.*, XVII, Roma, 2004, 9; dall'altro, *contra*, G. RICCIO, *Le perquisizioni nel codice di procedura penale*, Napoli, 1974, 181 ss.; G. PIERRO, *Una nuova specie di invalidità: l'inutilizzabilità degli atti processuali penali*, Napoli, 1992, 172; NOBILI, *Art. 191*, in *Commentario codice di procedura penale,* a cura di Chiavario, Torino, 1990, 409-413; D. SIRACUSANO, *Le prove*, in *Diritto processuale penale*, Milano, 2004, 343; G. ARICÒ, *Riflessioni in tema di inutilizzabilità delle prove nel nuovo processo penale*, in *Annali dell'istituto giuridico* dell'Università di Salerno, 1993, 28; in quest'ambito si osserva che la prova è inutilizzabile in virtù di un'interpretazione costituzionalmente orientata, A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, 1188; A. VELE, *La problematica utilizzabilità del documento formatosi nell'ambito della proce-*

dovrebbe dar conto di una serie di operazioni: recupero del supporto digitale e analisi del dato digitale, lo stato del dispositivo, l'annotazione del giorno e dell'ora di inizio e di cessazione dell'operazione, nonché i nominativi delle persone che hanno preso parte alle operazioni[13].
Un adempimento di questo tipo sarebbe, di fatto, necessario per garantire un efficace controllo *a posteriori* dell'operato degli inquirenti da parte della difesa e del giudice. In questa prospettiva, ad esempio, la difesa potrebbe affidare ad un proprio consulente tecnico o ad un perito (chiedendone l'ammissione) il compito di verificare se le tecniche di recupero e di analisi informatica abbiano alterato o danneggiato dati; non bisogna dimenticare, appunto, che eventuali alterazioni di dati potrebbero inficiare la fase valutativa del giudice, compromettendone la correttezza. Dal canto suo, lo stesso giudice può disporre una perizia *ex officio* ai sensi dell'art. 507 c.p.p.
In questo quadro, emerge il problema relativo all'affidabilità scientifica delle metodologie volte a recuperare il documento informatico; un'incertezza che presenta significative ricadute sull'inammissibilità dello stesso. A questo proposito vi è chi ritiene che la prova non autenticamente scientifica sia manifestamente irrilevante[14], nel senso che la stessa non può avere ingresso nel processo. Si è peraltro consapevoli delle difficoltà che il giudice incontra nel verificare *a posteriori* la violazione di regole tecniche; di qui la necessità di predisporre linee guida volte ad agevolare il vaglio giurisdizionale[15].

3. Dati informatici e tutela della riservatezza

Problematico è, poi, il rapporto tra analisi dei dati informatici e diritto alla riservatezza. Sappiamo che, con riferimento ai mezzi di ricerca della prova fondati sul fattore sorpresa, è impossibile predisporre congegni normativi a tutela della riservatezza prima dello svolgimento dell'attività di ricerca e questo valore può essere salvaguardato solo all'esito dell'operazione acquisitiva del documento informatico (successivamente alla ricerca

dura concorsuale in tema di dichiarazioni rese dal fallito al curatore fallimentare, in *Giust. pen.*, 2007, 520 ss.; ID., *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Padova, 2011, 97 ss.

[13] Il legislatore, peraltro, non può prevedere in maniera tassativa specifiche modalità tecniche, sia perché soggette a variazioni in forza della natura del dato ricercato e dello stato del dispositivo (spento, acceso, operativo *on line*), sia in forza del progresso tecnologico.

[14] F. CAPRIOLI, *La scienza "cattiva maestra": insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, 352.

[15] A. GRILLO-U. E. MOSCATO, *Riflessioni sulla prova informatica*, in *Cass. pen.*, 2010, 381, secondo cui la parte interessata dovrebbe segnalare e allegare protocolli, linee guida, regole tecniche comunemente accettate dagli ambienti scientifici, che ritiene siano stati violati nel corso della raccolta della prova e abbiano determinato una qualche distorsione della prova.

esplorativa di dati utili alle indagini) o al più tardi nella fase conclusiva delle indagini[16].

A questo proposito, può essere utile richiamare la disciplina delle intercettazioni anche in materia di documento informatico: prevedere, cioè, una fase di stralcio di dati estranei al processo (poiché appartenenti alla sfera personale dell'individuo) e sostanzialmente un divieto di pubblicazione degli stessi (fin quando non si è operato lo stralcio)[17].

Per quanto poi riguarda il profilo dei dati comunicativi presenti nella posta elettronica, dalle *chat line* private ai messaggi, occorre tracciare un distinguo tra la corrispondenza ordinaria in corso di spedizione e quella contenuta nella memoria di un *computer*[18].

Questa differenziazione è importante per separare l'area operativa del sequestro ordinario rispetto all'area operativa del sequestro di corrispondenza: le comunicazioni contenute nella memoria di un *computer*

---

[16] Per soluzioni costituzionalmente orientate cfr., Corte cost., 6 aprile 1973, n. 34, in *Giur. Cost.*, 1973, 316, con nota di GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche.* La Corte costituzionale, pur occupandosi specificamente del tema intercettazioni, rappresenta, infatti, un prezioso punto di riferimento della tutela di un diritto fondamentale, nel momento in cui afferma il principio secondo il quale violerebbe gravemente entrambe le norme costituzionali (artt. 2 e 15 Cost.) un sistema che, senza soddisfare gli interessi di giustizia, in funzione dei quali è consentita la limitazione della libertà e della segretezza delle comunicazioni, autorizzasse la divulgazione di comunicazioni telefoniche non pertinenti al processo.

[17] In dottrina si è critici sull'efficacia della disciplina delle intercettazioni in tema di riservatezza e, quindi, di pubblicazione delle conversazioni captate (le osservazioni si riferiscono alla disciplina previgente, visto il d.lgs. del 29 dicembre 2017, n. 216), A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, 206, ID., *Art. 268 c.p.p.*, in *Commento Codice di proc. pen.,* a cura di Conso-Grevi, Padova, 2015, 1041; L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, 141, secondo cui la disciplina vigente è in contrasto con gli artt. 2 e 15 Cost.; sul punto in ordine a delle diverse proposte di riforma, cfr. G. CONSO, *Intercettazioni telefoniche, troppe e troppo facilmente divulgabili*, *Dir. pen. e proc.*, 1996, 138; G. ILLUMINATI, *Come tutelare la riservatezza nelle intercettazioni telefoniche*, *GG*, 1996, 3; G. GIOSTRA, *Intercettazioni: troppo vago l'interesse da tutelare per allontanare i dubbi di legittimità della norma* in *Guid. Dir.*, 2009, 31, 207; V. GREVI, *Le intercettazioni come mero "mezzo di ricerca di riscontri probatori?*, in *Cass. pen.*, 2008, 848; ID., *Le intercettazioni al crocevia tra efficienza del processo e garanzie dei diritti*, in *Le intercettazioni di conversazioni e comunicazioni*, Atti del convegno di Milano, 5-7 ottobre 2007, Milano, 2009, 67; A. VELE, *Le intercettazioni*, *op. cit.*, 153, 179. In tema è utile evidenziare come il d.lgs. del 29 dicembre 2017, n. 216 ha introdotto l'art. 268-*quater* che prevede il venir meno del segreto sugli atti e i verbali delle conversazioni e comunicazioni oggetto di acquisizione con la pronuncia della relativa ordinanza.

[18] Cass., Sez. III, 25 novembre 2015, Giorgi, in *Mass. Uff.,* n. 265991; Cass., Sez. V, 21 novembre 2017, n. 1822, secondo cui non è applicabile la disciplina dettata dall'art. 254 c.p.p. con riferimento a messaggi *WhatsApp* e *SMS* rinvenuti in un telefono cellulare sottoposto a sequestro, in quanto questi testi non rientrano nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito; ancora non è configurabile neppure un'attività di intercettazione, che postula, per sua natura, la captazione di un flusso di comunicazioni in corso, mentre nel caso di specie ci si è limitati ad acquisire *ex post* il dato, conservato in memoria, che quei flussi documenta.

oppure in un programma di gestione di posta elettronica (non ancora spedite o giunte al destinatario ovvero aperte o meno), dovrebbero rientrare nel cono d'ombra del sequestro ordinario (art. 253 c.p.p.)[19]. La tutela della riservatezza non può essere affidata solo alla motivazione del decreto[20]; per una ragione molto semplice la motivazione in discorso non svolge alcuna funzione selettiva del materiale, ma contiene solo le ragioni giustificatrici del sequestro[21].

---

[19] Cass., Sez. un., 19 aprile 2012, Pasqua, in *Mass. Uff.*, n. 252893, le Sezioni unite hanno delineato il concetto giuridico di corrispondenza, osservando, infatti, che «la materia delle intrusioni investigative sulla "corrispondenza" è regolata dall'art. 254 c.p.p., che, rispetto alla normativa generale in tema di sequestri (art. 253 c.p.p.), si atteggia quale disciplina speciale, in quanto incidente su aspetti presidiati dall'art. 15 Cost. (nonché dall'art. 8 della C.E.D.U.), e che ha ad oggetto il sequestro della corrispondenza presso gestori (anche privati) di servizi postali (o, deve ritenersi, di quella che si trovi in luoghi accessori quali le cassette postali o che sia in via di recapito tramite il portalettere)» mentre hanno specificato che «nessuna speciale ragione di tutela - salve le peculiari esigenze attinenti ai rapporti tra imputato e difensore (art. 103 c.p.p. e art. 35 disp. att. c.p.p.) e le limitazioni imposte alla polizia giudiziaria nell'acquisizione di "plichi sigillati o altrimenti chiusi", distinti dalla "corrispondenza" (art. 353 1° co. c.p.p.) - interferisce con l'adozione di un ordinario provvedimento di sequestro da eseguire in qualsiasi luogo ove si trovino lettere o pieghi non ancora avviati dal mittente al destinatario o già da quest'ultimo ricevuti, in quanto simili cose non sono appunto "corrispondenza", implicando tale nozione un'attività di spedizione in corso o alla quale il mittente abbia dato comunque impulso consegnandola ad altri per il recapito»; Cass., sez. VI, 13 ottobre 2009, Giacalone, *ivi,* 245183. In tema cfr., altresì, Corte cost., 24 gennaio 2017, n. 20, in *www.cortecostituzionale.it* .

[20] R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. it. dir. e proc. pen.,* 2009, 136, riconosce particolare rilievo alla motivazione del decreto, che in caso di sequestro informatico il provvedimento dovrebbe delineare il fatto per cui si procede in modo tale da evidenziare il rapporto con lo strumento informatico, nonché recare l'indicazione dell'oggetto del sequestro, onde evitare che la selezione sia rimessa all'autorità giudiziaria; in tema, Cass., Sez. VI, 2 maggio 2013, M.R., in *Mass. Uff.*, n. 256327; Id., Sez. II, 20 novembre 2013, G.A.M., *ivi,* n. 258074, secondo tali sentenze la Corte di cassazione ha affermato che «non è possibile pretendere l'indicazione dettagliata delle cose da ricercare e sottoporre a sequestro, sia perché il più delle volte le stesse non possono essere specificate a priori, sia perché l'art. 248 c.p.p., nel prevedere la richiesta di consegna quando attraverso la perquisizione si cerca una cosa determinata, implica che oggetto di ricerca possano essere anche cose non determinate, che potranno essere individuate solo all'esito dell'eseguita perquisizione». Ancora ha specificato come «nel caso di ricerca di cose non determinate, secondo l'orientamento consolidato di questa corte, ai fini della legittimità del sequestro di cose ritenute corpo di reato o pertinenti al reato, effettuato dalla polizia giudiziaria all'esito di perquisizione disposta dal pubblico ministero, non è richiesto che le cose anzidette siano preventivamente individuate». Per completezza di ragionamento, inoltre, la Corte afferma che «quando invece la polizia giudiziaria abbia individuato e sequestrato cose non indicate nel decreto o il cui ordine di sequestro non sia desumibile dalle nozioni di corpo del reato o di cose pertinenti al reato, in relazione ai fatti per i quali si procede, l'Autorità giudiziaria dovrà procedere alla convalida del sequestro ovvero ordinare la restituzione delle cose non ritenute suscettibili di sequestro». Cfr., altresì, Cass., Sez. V, 25 novembre 1999, Cogni, in *Mass. Uff.*, n. 215566; Id., Sez. III, 2 marzo 2010, C.G., *ivi*, n. 246464.

[21] Occorre ricordare che secondo il giudice di legittimità l'oggetto "*computer*" è ritenuto come cosa pertinente al reato e non i dati contenuti nello stesso, Cass., sez. V, 21 agosto 2013, , D., in *Mass. Uff.*, n. 35269, secondo la quale, infatti, il *computer* è da ritenersi cosa pertinente al reato; in senso contrario, A. CHELO MANCHIA, *Sequestro probatorio di computers: un provvedimento superato dalla tecnologia?*

Un'efficace selezione in tal senso potrebbe essere rappresentata dalla previsione di un'apposita udienza stralcio, anche con riferimento al sequestro penale del documento informatico[22]; si impone, quindi, l'adozione di regole volte a tutelare la riservatezza del materiale processualmente irrilevante contenuto nel documento sequestrato[23].

Passando ad esaminare il profilo del "domicilio informatico"[24] occorre subito dire che la tutela della riservatezza non può essere affidata alla disciplina delle intercettazioni, perché non sussistono le caratteristiche tipiche dell'intercettazione, cioè la volontà dei captanti di escludere terzi dalla loro contestuale conversazione[25].

Più logico allora puntare sulla disciplina regolatrice degli altri mezzi di ricerca della prova[26]; una conferma, peraltro, è nell'applicazione della disciplina in

---

in *Cass. pen.*, 2005, 1635, sul punto si osserva che il nesso con il reato dovrebbe riferirsi esclusivamente ai dati e non al *computer* che ne costituisce il mero contenitore, ossia *res* neutra rispetto al *thema probandum.*

[22] L'oggetto informatico, peraltro, è complesso da valutare, anche sotto il profilo di dati utili all'accertamento; la prassi, appunto, ci conferma che l'apprensione dei dati informatici è così ampia che travolge tendenzialmente dati personali, molti dei quali risulteranno estranei all'imputazione. Per mero formalismo, inoltre, si specifica che la disciplina in tema di restituzione del materiale sequestrato, che può essere attivata d'ufficio o a richiesta dei soggetti titolari del bene, non è in grado naturalmente di salvaguardare la privacy; la valutazione dell'autorità giudiziaria, infatti, si incentra sul venir meno delle esigenze probatorie sottese al vincolo e sull'individuazione dell'avente diritto alla restituzione del bene.

[23] Questa soluzione, tra l'altro, è stata prospettata nel caso delle lecite registrazioni effettuate da privati, ove si è proposto di stralciare dalla conversazione la parte dichiarativa che non è in linea con l'interesse della giurisdizione, A. VELE, *Le intercettazioni*, *op. cit.*, 52 ss.

[24] Il computer è oggetto di interesse investigativo, non solo in relazione ai reati informatici, bensì con riferimento a qualsiasi tipologia delittuosa, contenendo dati utili alle indagini; accanto, però, a dati eventualmente utili alle indagini, vi sono ulteriori dati archiviati nel medesimo relativi alla vita privata del proprietario e/o dell'utilizzatore. A tal proposito, Cass., Sez. V, 8 maggio 2012, P.L., n. 42021, in *Dir. informaz. e informatica*, 2013, 88, secondo cui il legislatore, con la previsione dell'art. 615-ter c.p., ha assicurato la protezione del domicilio informatico, come spazio ideale e fisico di pertinenza della persona; spazio cui è estesa la tutela della riservatezza della sfera individuale, quale bene costituzionalmente protetto.

[25] In senso contrario, M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 288 ss., secondo cui al fine di proteggere la riservatezza in ordine all'acceso al sistema informatico si potrebbero prevedere requisiti analoghi a quelli delle intercettazioni: autorizzazione di un giudice alle operazioni di apprensione, preesistenza di gravi indizi di uno dei reati previsti in un elenco legislativo, vaglio preventivo sulla indispensabilità del mezzo.

[26] A tal proposito non si esclude che si possa migliorare la disciplina dei mezzi di ricerca della prova – nei suoi presupposti e modalità – ispezioni, perquisizioni e sequestro in ambito informatico. In argomento cfr. A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. Internet*, 2008, 506 ss., c'è chi osserva, ad esempio, che si evince un *favor* per la previa individuazione, tramite ispezione o perquisizione informatica, dei dati da acquisire in quanto pertinenti al reato: il sequestro dell'*hardware* dovrebbe restare confinato ai soli casi in cui non fosse possibile, o consigliabile, esperire i due altri mezzi di ricerca della prova; G. COSTABILE, *Scena criminis, documento informatico* e *formazione della prova penale*, in *Dir. informazione e informatica*, 2005,

materia di perquisizioni, sequestri e accertamenti urgenti.

4. L'acquisizione dei documenti digitali con lo strumento del captatore informatico

Per quanto attiene l'acquisizione occulta dei documenti informatici ottenuta tramite "perquisizioni *on line"* in cui si fa uso dei *trojan* per monitorare le attività compiute in rete e per captare i contenuti di alcuni dispositivi informatici (dati rinvenibili nell'*hard disk*, informazioni visualizzate sullo schermo, password digitate tramite la tastiera), occorre sottolineare come questo tipo di attività possa risultare fortemente lesiva dei diritti fondamentali (*in primis* gli artt. 2 e 14, Cost.).

Il nodo centrale è rappresentato dall'esigenza di garantire un equilibrio tra interessi contrapposti: da un lato una legittima ed efficace attività di polizia giudiziaria (anche o soprattutto di natura preventiva) e dall'altro una compressione di diritti fondamentali dell'individuo, durante la fase delle indagini, a determinate condizioni e solo nei casi in cui vi sia prevalenza dell'interesse pubblico rispetto a quello soggettivo; interesse pubblico che andrebbe misurato non solo sotto il profilo di natura sostanziale (pericolosità sui valori prevalenti derivante da specifici fatti di reato), bensì anche da quello di natura processuale (ad esempio della difficoltà oggettiva di poter svolgere indagini con altri strumenti investigativi in ordine a fattispecie giuridiche che incidano su valori fondamentali prevalenti); stando, quindi, ai valori fondamentali preminenti, la "perquisizione" mediante captatori informatici potrebbe essere prevista in particolare per i reati con finalità di terrorismo e mafiose sul piano dell'attività preventiva e processuale.

A questo proposito *de iure condendo* potrebbe essere utile rammentare i risultati cui è pervenuta la Corte costituzionale tedesca, secondo cui i limiti all'installazione di *trojan horse* all'insaputa dell'utente dovrebbero essere volti a tutelare valori fondamentali prevalenti: la vita e l'integrità degli altri cittadini, i fondamenti dello Stato, i valori essenziali di umanità[27].

---

531 ss. Inoltre, non sono mancati dubbi in ordine alla scelta legislativa volta semplicemente ad interpolare l'art. 354 c.p.p, allo scopo di adattarne la disciplina ivi contenuta alle nuove esigenze poste dall'investigazione informatica: infatti, si osserva che le peculiarità che contraddistinguono quest'ultima avrebbe dovuto imporre un intervento mirato ad introdurre nel codice specifici strumenti di ricerca della prova, in aggiunta a quelli tradizionali, L. LUPÁRIA, *La ratifica della Convenzione CyberCrime del Consiglio d'Europa. I profili processuali*, in *Dir. pen. e proc.,* 2008, 696.

[27] La Germania nel 2006 ha introdotto, come emendamento al § 5 co. 2, n. 11 della legge sulla protezione della Costituzione nel Nord Reno-Westfalia, una normativa in materia di raccolta e trattamento dei dati degli utenti da parte di sistemi informatici o attraverso la Rete. L'emendamento rinforzava i servizi segreti nazionali, ossia "L'Ufficio Federale per la Protezione della Costituzione" (Bundesamt für

In sostanza la Corte costituzionale tedesca, dichiarando illegittima per violazione del principio di proporzionalità e di tassatività la normativa che autorizzava l'istituzione di un apposito organismo incaricato di effettuare due diverse tipologie di indagine – l'accesso segreto a sistemi informatici e il monitoraggio segreto della rete – lascia aperta la porta all'emanazione di una nuova normativa che, nel rispetto dei citati principi, consenta di svolgere un'attività di monitoraggio e di *remote forensics.*

Per quanto riguarda le intercettazioni effettuate mediante l'uso occulto di captatori informatici, le Sezioni unite hanno affermato il principio secondo cui, «limitatamente ai procedimenti di criminalità organizzata, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti – mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (ad esempio, *personal computer*, *tablet*, *smartphon*, etc.) – anche nei luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa»[28].

Verfassungsschutz) poiché autorizzava l'istituzione di un apposito organismo, incaricato di effettuare due diverse tipologie di indagine: l'accesso segreto a sistemi informatici e il monitoraggio segreto della Rete. L'accesso a sistemi informatici poteva avvenire sia attraverso l'installazione di strumenti hardware (sonda e intercettazioni parametriche su dorsali di comunicazione) sia attraverso sistemi "da remoto", ossia software (keylogger, sniffer) installati in forma di *trojan horse* ad insaputa dell'utente. La Corte Costituzionale tedesca, a distanza di due anni dall'applicazione della legge, ha dichiarato incostituzionale tale legge riconoscendo un nuovo "diritto alla riservatezza ed alla integrità dei sistemi informatici" che ha come presupposti il diritto allo sviluppo della personalità di ogni cittadino e il diritto alla dignità della persona e che tutela ogni cittadino dall'accesso, da parte dello Stato, ai sistemi informatici nel loro complesso. Avendo stabilito che i diritti esistenti non sono sufficienti per proteggere i cittadini dalla minacce contro i loro diritti della personalità, la Corte stabilì un nuovo diritto fondamentale alla riservatezza ed integrità dei sistemi tecnologici di informazione per colmare così la lacuna normativa. Così come il diritto all'autodeterminazione dell'informazione, questo nuovo diritto fondamentale si basa sull'articolo 2.1 GG in combinato disposto con l'articolo 1.1 GG ed è derivato da un generale diritto della personalità. L'articolo 1 GG, il quale dispone che "la dignità umana è inviolabile, e tutti gli organi dello stato hanno l'obiettivo finale di proteggerla" stabilisce un generale principio fondamentale nel sistema legale tedesco ed è stato progettato esplicitamente come soluzione per eliminare le lacune se le soluzioni legislative non rispettano il cambiamento sociale. Il nuovo diritto costituzionale alla segretezza ed integrità dei sistemi tecnologici di informazione, secondo la Corte, protegge la vita personale e privata dei titolari dei diritti dall'accesso statale a dispositivi tecnologici di informazione, in particolare dall'accesso da parte dello Stato ai sistemi tecnologici di informazione nel loro complesso, non solo dunque per eventi di comunicazione individuale o memorizzazione dei dati (Bundesverfassungsgericht, 27.2.08, BVerfGE, NJW 2008, 822).

[28] Cass. pen., Sez. un., 28 aprile 2016, Scurato, n. 26889, in *www.giurisprudenzapenale.com*; Cass. pen., sez. VI, 13 giugno 2017, Romeo, n. 36874, in *www.penalecontemporaneo.it*; in tema di commenti alle Sez. un. cfr. A. CAMON, *Cavalli di troia in Cassazione*, in *Arch. nuova proc. pen.,* 2017, 76 ss.; A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.,* 2016, 2274-2288; G. CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, in *Dir. informazione e informatica,* 2016, 88; P. FELICIONI, *L'acquisizione da remoto di dati digitali nel proce-*

Un'interpretazione di questo tipo, ancorché in linea con la logica del doppio binario (che prevede trattamenti differenziati tra soggetti in ragione della tipologia di reato), appare tuttavia discutibile, perché si inserisce in un contesto normativo mancante di qualsiasi indicazione specifica circa i presupposti e le modalità esecutive dello strumento investigativo, a tutela delle garanzie individuali[29]; presupposti, limiti e modalità esecutive che risultano invece espressamente indicati nel d.lgs. n. 216 del 29 dicembre 2017 recante disposizioni in materia di intercettazione di conversazioni o comunicazioni in attuazione della legge delega n. 103 del 23 giugno 2017[30].

---

dimento penale: evoluzione giurisprudenziale e prospettive di riforma, in *Proc. pen. e giust.,* 2016, 5, 21; A. GAITO –S. FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.*, 2016, 2, 309; A. CISTERNA, *Spazio ed intercettazioni, una liaison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite, ivi*, 2016, 2, 331; L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico), ivi*, 2016, 2, 348; L. PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, *ivi*, 2016, 2, 354; G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *www.penalecontemporaneo.it*, 2016; G. BARROCU, *Il captatore informatico: un virus per tutte le stagioni*, in *Dir. pen. e proc.*, 2017, 3, 379 ss.

[29] Sul terreno dell'ammissibilità delle intercettazioni tra presenti, tra l'altro, sarebbe opportuno intervenire sul requisito costituito al «fondato motivo di ritenere che ivi si stia svolgendo un'attività criminosa», poiché la sua applicazione risulterebbe discutibile nelle ipotesi ordinarie di intercettazione tra presenti, nei casi previsti dall'art. 266 c.p.p. Per procedere con tale mezzo investigativo nell'ambito del domicilio per determinati delitti (previsti dalla legislazione speciale ex art. 13 d.l. 13 maggio 1991 n. 152, convertito in legge 12 luglio 1991 n. 203 e successive modificazioni) non è richiesto il limite del «fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa», sebbene questa "deroga" dovrebbe riguardare tutte le ipotesi di reato previste dall'art. 266 c.p.p., dal momento che appare singolare autorizzare un'intercettazione soltanto allorquando sia in atto un'attività criminosa (flagranza). Secondo questo schema, nell'ipotesi ordinaria andrebbero però strutturati degli ulteriori limiti a tutela dell'inviolabilità del domicilio, nel senso che l'intercettazione in tale luogo potrebbe essere espletata a condizione che quelle telefoniche e ambientali al di fuori del domicilio stesso non fossero possibili sulla scorta di specifici elementi.

[30] Cfr. legge del 23 giugno 2017, n. 103, Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario, in *Gazz. Uff.* n. 154 del 04 luglio 2017. Sul punto si riporta il *d.lgs. n. 216 del 29 dicembre 2017 recante disposizioni in materia di intercettazione di conversazioni o comunicazioni, in attuazione della delega di cui all'art. 1, comma 82, 83 e 84, lettere a), b), c) ed e) della legge 23 giugno 2017, n. 103,* in *Gazz. Uff.* n. 8 del 11 gennaio 2018: art. 4 (*modifiche al codice di procedura penale in materia di intercettazioni mediante inserimento di captatore informatico*) 1 Al codice di procedura penale, approvato con d.p.r. del 22 settembre 1988, n. 447, sono apportate le seguenti modificazioni: a) all'articolo 266, al 2° co.: 1) al 2° co., primo periodo, sono aggiunte, in fine, le seguenti parole: «, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile»; 2) dopo il 2° co è aggiunto il seguente: «2-bis. L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater; b) all'articolo 267: 1) al 1° co., è aggiunto, in fine, il seguente periodo: «Il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini; non-

Quanto alla definizione di captatore informatico, la relazione illustrativa del d.lgs. in discorso precisa che si tratta di un *malware* occultamente installato dall'inquirente su un apparecchio elettronico dotato di connessione internet attiva, il quale consente al captante di venire a conoscenza del «traffico dati (sia in entrata che in uscita), di attivare da remoto il microfono e la telecamera registrandone le attività, di "perquisire" gli *hard disk* e di fare copia integrale del loro contenuto, di intercettare tutto quanto digitato sulla tastiera, di fotografare le immagini ed i documenti visualizzati»[31].

ché, se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3-bis e 3-quater, i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono.»; 2) dopo il 2° co., è inserito il seguente: «2-bis. Nei casi di cui al 2° co., il pubblico ministero può disporre, con decreto motivato, l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile soltanto nei procedimenti per i delitti di cui all'articolo 51, commi 3-bis e 3-quater. A tal fine indica, oltre a quanto previsto dal 1° co., secondo periodo, le ragioni di urgenza che rendono impossibile attendere il provvedimento del giudice. Il decreto è trasmesso al giudice che decide sulla convalida nei termini, con le modalità e gli effetti indicati al 2° co.»; c) all'art. 268, co. 3-bis, è aggiunto, in fine, il seguente periodo: «Per le operazioni di avvio e di cessazione delle registrazioni con captatore informatico su dispositivo elettronico portatile, riguardanti comunicazioni e conversazioni tra presenti, l'ufficiale di polizia giudiziaria può avvalersi di persone idonee di cui all'articolo 348, 4° co.»; d) all'articolo 270, dopo il 1° co., è aggiunto il seguente: «1-bis. I risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile non possono essere utilizzati per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza.»; e) all'articolo 271: dopo il 1° co., è inserito il seguente: «1-bis. Non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo.». All'art. 5 (*Modifiche alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale)* 1. Alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, sono apportate le seguenti modificazioni: a) all'articolo 89: 1) al 1° co. è aggiunto, in fine, il seguente periodo: «Quando si procede ad intercettazione delle comunicazioni e conversazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile, il verbale indica il tipo di programma impiegato e i luoghi in cui si svolgono le comunicazioni o conversazioni.»; 2) dopo il comma 2 sono aggiunti i seguenti: «2-bis. Ai fini dell'installazione e dell'intercettazione attraverso captatore informatico in dispositivi elettronici portatili possono essere impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia. 2-ter. Nei casi previsti dal co. 2-bis le comunicazioni intercettate sono trasferite, dopo l'acquisizione delle necessarie informazioni in merito alle condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione, esclusivamente verso gli impianti della procura della Repubblica. Durante il trasferimento dei dati sono operati controlli costanti di integrità, in modo da assicurare l'integrale corrispondenza tra quanto intercettato e quanto trasmesso e registrato. 2-quater. Quando è impossibile il contestuale trasferimento dei dati intercettati, il verbale di cui all'articolo 268 del codice dà atto delle ragioni tecniche impeditive e della successione cronologica degli accadimenti captati e delle conversazioni intercettate. 2-quinquies. Al termine delle operazioni si provvede, anche mediante persone idonee di cui all'articolo 348 del codice, alla disattivazione del captatore con modalità tali da renderlo inidoneo a successivi impieghi. Dell'operazione si dà atto nel verbale.».

[31] In tal senso, *Relazione illustrativa dello schema di decreto legislativo recante disposizioni in materia di intercettazione di conversazioni o comunicazioni, in attuazione della delega di cui all'art. 1, comma 82, 83 e 84, lettere a), b), c) ed e) della legge 23 giugno 2017, n. 103,* in *www.camera.it*

Considerato, quindi, che lo strumento *de quo* realizza di fatto una sorta di perquisizione *on line*, il decreto prevede in via prudenziale la sanzione di «inutilizzabilità dei dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile»[32].

Non mancano però profili di criticità sul piano delle tutele[33]. La scelta di aggiungere all'art. 267, comma 1, c.p.p. il seguente periodo «il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini»[34], non appare sufficientemente garantista, vuoi per la genericità delle ragioni che rendono necessaria la modalità operativa in questione, vuoi perché occorre uno specifico presupposto che dia la possibilità al giudice di riempire di contenuto la motivazione. Da questo punto di vista, sarebbe stata opportuna una maggiore cautela sui presupposti di applicazione dei *trojan*, limitandone l'uso ai casi in cui non risulti possibile proseguire le indagini con le intercettazioni tradizionali.

Non convince poi la previsione di due diverse fattispecie autorizzative in tema di urgenza. Nei casi di cui all'art. 267, co. 2, c.p.p. il pubblico ministero può disporre, con decreto motivato, l'intercettazione tra presenti mediante l'inserimento di captatore informatico su dispositivo elettronico portatile soltanto nei procedimenti per delitti di cui all'art. 51, co. 3-*bis* e 3-*quater* c.p.p.[35]; c'è il rischio di perdere risultati investigativi anche per le diverse fattispecie di reato che ammettono l'intercettazione, purché l'esercizio del potere del pubblico ministero sia confinato in rigorosi presupposti e vi sia convalida giurisdizionale in tempi brevi.

La disciplina vigente, tra l'altro, eleva l'urgenza di apprendere comunicazioni utili (richiesta dal caso concreto) a requisito che legittima il pubblico ministero a disporre il decreto motivato, purché vi sia il fondato motivo di ritenere che dal ritardo possa derivare un grave pregiudizio alle indagini. Solo il pubblico ministero, in quanto gestore delle indagini, è infatti in grado di valutare la situazione "emergenziale" entro tempi così ristretti.

---

[32] A questo proposito cfr. nota n. 30.

[33] Un mezzo di ricerca della prova così insidioso, sia pure proiettato a captare le sole conversazioni o comunicazioni, necessita di rigorose garanzie a tutela dei diritti fondamentali, in quanto tale strumento comporta occulte perquisizioni *on line* in conflitto con le regole previste per tale mezzo investigativo (perquisizioni).

[34] V. nota n. 30.

[35] In merito cfr. nota n. 30.