ARTICOLO SOTTOPOSTO A PEER REVIEW

LE C.D. PERQUISIZIONI *ONLINE* TRA NUOVI DIRITTI FONDAMENTALI ED ESIGENZE DI ACCERTAMENTO PENALE

Federica Iovene

Abstract

Le c.d. perquisizioni *online* rappresentano un istituto di natura ibrida e di difficile inquadramento giuridico, oggetto di crescente attenzione a livello europeo ed internazionale. Muovendo dalla preliminare individuazione dei diritti fondamentali della persona coinvolti, il presente contributo si propone di vagliare l'ammissibilità di tale strumento di indagine nell'ordinamento italiano.

Sommario

1. Premessa.

L'effettività di un'efficace lotta contro gravi forme di criminalità dipende sempre più frequentemente dall'uso di strumenti d'indagine ad alto contenuto tecnologico.

Tra questi, le c.d. perquisizioni *online* occupano uno spazio che impegna la riflessione del processualista per la peculiarità del diritto fondamentale che la loro pratica comprime e per il fatto di assommare le caratteristiche di diversi strumenti di indagine. L'espressione allude all'insieme di operazioni volte ad esplorare e monitorare un sistema informatico, rese possibili dall'infiltrazione segreta nello stesso, che consentono sia di acquisire dati salvati sul *computer*, e quindi precostituiti, sia di captare flussi di dati in tempo reale[1]. Attraverso l'installazione, in locale o in remoto, di uno specifico *software*[2] sul *computer* oggetto di osservazione è infatti possibile, ogniqualvolta l'utente si colleghi a *Internet*, "perquisire" l'*hard disk* ed ottenerne copia, rilevare e registrare i siti *web* che vengono visitati, decifrare quel che viene digitato sulla tastiera, "intercettare" le comunicazioni *VoIP*, acquisire *e-mail*, attivare le periferiche audio e video per sorvegliare il luogo in cui si trova il *computer*[3].

In questo contesto è quindi particolarmente avvertita la necessità di una sinergia tra informatica e diritto: solo un'adeguata comprensione del funzionamento dei sistemi informatici e degli strumenti di *computer forensics* permette infatti di apprestare idonee garanzie a tutela dei diritti fondamentali di chi è sottoposto a procedimento penale e di introdurre le misure opportune per preservare la genuinità della *digital evidence* e garantire la sua utilizzabilità.

2. Le *online searches* nel panorama europeo e internazionale.

Le perquisizioni *online* vengono condotte attraverso l'invio, generalmente tramite *e-mail*, di un c.d. *trojan* (di qui l'espressione ricorrente di *Trojan di Stato*), ossia di un programma – *backdoor* – con funzionalità note all'utente ma che cela al suo interno un codice "segreto" che viene eseguito sul *computer*, creando un particolare collegamento tra il *computer* su cui è installata la *backdoor* e un *computer* remoto, che fa sì che l'utente di quest'ultimo abbia il pieno controllo del primo sistema informatico[4].

Già questi primi cenni sono sufficienti a mettere in evidenza da un lato le enormi potenzialità per la repressione – e in ipotesi prevenzione – dei reati insite in tale poliedrico strumento di indagine, dall'altro la particolare invasività di simile mezzo di ricerca della prova, capace di minare le fondamenta dei "classici" diritti fondamentali.

Che non sia più possibile rinviare una seria riflessione su questi temi, emerge con chiarezza sol se si volge lo sguardo oltre i confini nazionali.

Rimanendo in Europa, la possibilità di utilizzare questo specifico *software* per condurre attività di *intelligence* è stata per la prima volta introdotta in Germania, in particolare nel *Land Nord Rhein Westfalen*, dove attraverso una modifica della Legge sulla protezione della Costituzione del *Land* si autorizzava un organismo di *intelligence* a "protezione della costituzione" (*Verfassungsschutzbehörde*) ad effettuare due tipi di indagine: il monitoraggio e la ricognizione segreti di *Internet* e l'accesso segreto a sistemi informatici (§ 5 Abs. 2, n. 11).

Già prima dell'introduzione di tale norma, la dottrina e la giurisprudenza tedesche si interrogavano sui delicati rapporti tra *Online Durchsuchung* e diritti costituzionalmente garantiti e su come in ipotesi armonizzare tale strumento con il dettato codicistico.

Come noto, sulla questione è intervenuta nel 2008 la Corte costituzionale tedesca che, pur dichiarando la suddetta normativa incostituzionale in quanto non rispettosa dei principi di proporzionalità e determinatezza, non ha escluso in assoluto l'ammissibilità di tale

[1] Si spiega così la scelta di utilizzare il plurale per riferirsi a tale particolare strumento di indagine.

[2] Il programma in questione è una *backdoor* che può essere installata in locale o in remoto sul *computer* che si intende perquisire. La *backdoor* è un particolare tipo di *malware* (dall'inglese *malicious software*, ovverosia "programma malvagio") che consente di prendere il controllo di un altro *computer*, sfruttando una connessione *Internet*, quando l'utente vi si colleghi (di qui il termine perquisizioni *online*).

[3] Anche se che con l'installazione di un unico *software* si possono porre in essere diverse attività di indagine, è bene comunque tenere ferma la distinzione tra modalità statiche e modalità dinamiche di apprensione dei dati digitali perché diversi sono nei due casi gli strumenti di *computer forensics* utilizzati, appartenendo la seconda ipotesi alla c.d. *Live Forensics Analysis*.

[4] Possono essere utilizzati altresì *keyloggers*, *spywares* o *sniffers*. La *backdoor* può essere inoltre installata fisicamente – in locale anziché in remoto – sul *computer*, in maniera del tutto simile all'installazione di microspie ai fini delle intercettazioni ambientali.

strumento di indagine[5]. Interessante l'argomento reputato decisivo per la citata declaratoria di illegittimità. Ritenendo insufficienti le garanzie offerte dalle norme costituzionali a tutela della segretezza delle telecomunicazioni (art. 10 *Grundgesetz,* d'innanzi *GG*) e dell'inviolabilità del domicilio (art. 13 *GG*) e, altresì, del diritto all'autodeterminazione informativa[6], il *Bundesverfassungsgericht* ha preso atto dell'esistenza di un nuovo diritto fondamentale "alla garanzia della segretezza e integrità dei sistemi informatici" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). Un diritto di rango costituzionale, ricavato da quella sorgente di diritti inviolabili che è la *Menschenwürde* (artt. 1, comma 1 e 2, comma 1 *GG*).

Consapevole delle peculiarità proprie dello strumento informatico rispetto ai tradizionali mezzi di comunicazione, la Corte Costituzionale tedesca ha quindi ritenuto opportuno predisporre una tutela ulteriore e sussidiaria rispetto a quella già vigente. Di fronte alle sfide lanciate dal progresso tecnologico, infatti, la semplice, quanto doverosa, interpretazione evolutiva del dettato costituzionale non basta, le tradizionali garanzie della segretezza delle telecomunicazioni e dell'autodeterminazione informativa non sono sufficienti.

Sulla base di queste premesse, la Corte ha stabilito che operazioni investigative suscettibili di comprimere tale nuovo diritto della personalità possono essere giustificate, non solo da finalità di repressione di reati, ma anche da finalità preventive[7], a condizione che siano rispettati il principio di proporzionalità – la Corte fa un elenco di beni giuridici per tutelare i quali è consentita l'intromissione in sistemi informatici o telematici[8] – e la riserva di giurisdizione – occorre un provvedimento autorizzativo del giudice, che poi sorvegli tale attività, come peraltro è normalmente previsto per le altre operazioni limitative della libertà personale –.

Non solo, ma il *Bundesverfassungsgericht*, rivolgendosi al legislatore tedesco che voglia disciplinare questo particolare strumento, ha auspicato l'adozione di un adeguato sistema di misure tecniche preventive idoneo ad impedire di avere accesso a dati personali, irrilevanti per le indagini o comunque la previsione di garanzie *ex post* consistenti nell'immediata cancellazione di tali dati e nella loro inutilizzabilità processuale.

In tempi più recenti, anche in Olanda è stata proposta l'introduzione del c.d. *Trojan* di Stato, che consentirebbe alla polizia, su autorizzazione del giudice, di monitorare l'uso del sistema informatico, copiare i dati in esso contenuti e addirittura distruggerli, se illegali. Tale possibilità sarebbe riconosciuta alla polizia olandese anche qualora non fosse possibile localizzare il *computer* oggetto di indagine, essendo quindi consentito un accesso transfrontaliero diretto a dati informatici, mentre qualora fosse nota la sede del sistema informatico, occorrerebbe servirsi dei tradizionali meccanismi di cooperazione giudiziaria[9].

Analoga proposta è stata avanzata dal Ministro della giustizia spagnolo nel febbraio dello scorso anno. Attraverso una modifica degli artt. 350, 351, 352 del *Codigo Procesal Penal* si prevede infatti la possibilità di installare da remoto uno specifico *software* di indagine che permetta di avere accesso ai dati contenuti in un sistema informatico, all'insaputa dell'utente, e di "perquisirlo" (*registros remotos sobre equipos informaticos*). Tale forma di monitoraggio dovrebbe essere autorizzata dal *Tribunal de Garantías*, per una durata massima di dieci giorni, qualora la misura appaia necessaria e proporzionata per l'accertamento di un reato di particolare gravità. La proposta si preoccupa altresì di specificare quale debba essere il contenuto del mandato, ossia, oltre alla motivazione in ordine alla idoneità, necessità e proporzionalità della misura, l'indicazione dello specifico dispositivo oggetto d'indagine, dei dati ricercati, dei soggetti autorizzati a condurre l'indagine e l'eventuale autorizzazione ad effettuare copia, con misure idonee a garantirne l'integrità, dei dati rilevanti. È presa altresì in considerazione l'eventualità

[5] *BVerfG*, 27 febbraio 2008, *BVerfGE* 120, 274 ss. Per un commento alla sentenza si veda R. Flor, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung. *La prospettiva delle investigazioni ad alto contenuto tecnologico e il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. trim. dir. pen. ec.*, 2009, p. 697 ss.

[6] *Informationelles Selbstbestimmungsrecht*, messo a punto nel 1983 con la nota sentenza sul censimento (*Volkszählungsurteil*). *BVerfG*, 15 dicembre 1983, *BVerfGE* 65, 1 ss.

[7] Il passaggio è molto delicato perché rimanda al pericolo che le perquisizioni si trasformino in mezzi di ricerca della *notitia criminis*, pericolo peraltro che nell'ordinamento tedesco è ridimensionato dall'esistenza di una norma specifica, il § 108 *StPO*, che disciplina il sequestro di cose, rinvenute nel corso della perquisizione, pertinenti ad un reato diverso da quello per cui si procede.

[8] La vita, l'incolumità fisica, la libertà dei singoli, e i beni della collettività la cui minaccia tocca il fondamento dello Stato, il suo mantenimento o la base dell'esistenza umana. Il rispetto del principio di proporzionalità richiede infatti che la compressione dei diritti fondamentali persegua uno scopo legittimo e sia idonea, necessaria ed opportuna quale mezzo per il raggiungimento di questo scopo.

[9] La proposta proviene dal Ministro della Giustizia olandese Ivo Opstelten e risale all'ottobre 2012.

che l'autorità procedente abbia ragione di ritenere che i dati e le informazioni ricercate siano contenute in un diverso sistema informatico. In tal caso, se quest'ultimo è comunque situato nel territorio spagnolo, si ammette l'estensione dell'indagine, sempre se autorizzata dal *Tribunal de Garantías*, altrimenti si pretende il ricorso ai meccanismi di cooperazione giudiziaria.

Spostando lo sguardo oltre i confini europei, da segnalare è il caso statunitense, dove già da alcuni anni è stato messo a punto uno specifico *software*, denominato "*Magic Lantern*" che consente di decriptare i *files* e renderli quindi leggibili. Si tratta di un c.d. *keylogger*, inviato tramite *e-mail* o installato in locale, in grado di memorizzare i tasti schiacciati dall'utilizzatore del *computer* e quindi di rivelare le *passwords* poste dall'utente a protezione di cartelle e documenti. Sulla base di questi dati, sarà poi possibile sequestrare il *computer* e avere accesso ai *files* che interessano.

L'ammissibilità di tali strumenti di indagine, e in particolare la necessità che essi siano autorizzati con mandato del giudice (*judicial warrant*), dipende dal riconoscimento dell'esistenza di una *reasonable expectation of privacy* rispetto ai dati e alle informazioni contenute in un *computer*[10]. Infatti, solo laddove l'attività investigativa interferisca con la ragionevole aspettativa di *privacy* del destinatario, essa potrà essere qualificata quale *search* con conseguente applicazione della c.d. *Fourth Amendment Doctrine*, e quindi necessità di un mandato, supportato da un fondato motivo (*probable cause*)[11].

È altresì noto il caso *Ivanov-Gorshkov* in cui agenti *FBI* di Seattle si sono "infiltrati" in *computers*, fisicamente localizzati in Russia e appartenenti a cittadini russi, per poi scaricare sul loro *computer*, negli Stati Uniti, *files* utili per le indagini in corso[12]. Questo esempio, oltre a dimostrare che tali *softwares* di indagine sono utilizzati nella pratica, ne mette in luce una delle caratteristiche fondamentali, ossia la dimensione ontologicamente transnazionale. Le c.d. *remote computer searches* consentono infatti di avere accesso a *computers* ovunque essi siano localizzati, quindi anche al di fuori dei naturali confini della giurisdizione di uno Stato. Di qui la necessità di un approccio globale al fenomeno.

L'importanza di strumenti d'indagine quali le *online searches* è avvertita anche a livello di Unione Europea, sia ai fini della cooperazione giudiziaria, sia nel contesto delle nuove competenze penali ad essa attribuite col Trattato di Lisbona, tra cui rientra la criminalità informatica (art. 83 TFUE).

Sotto il primo profilo si segnalano le conclusioni del Consiglio del 27 novembre 2008 relative ad una strategia di lavoro concertata e a misure pratiche di lotta alla criminalità informatica[13], che contengono un espresso invito agli Stati membri ad agevolare la perquisizione a distanza, se prevista dalla legislazione nazionale, in quanto essa consente ai servizi investigativi, con l'accordo del Paese ospite, di accedere rapidamente alle informazioni. Tale disposizione sembra infatti fare indiretto riferimento all'istituto delle perquisizioni *online* (*remote computer searches*).

Quanto al secondo profilo, va ricordata la direttiva sulla lotta alla pedopornografia[14], che al *considerandum* 27 auspica che gli Stati membri mettano a disposizione dell'autorità inquirente strumenti investigativi efficaci, tra cui «controlli a distanza anche con uso di strumenti

[10] Cfr. S. W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, in 81 *Miss. L. J.*, 1 (2011), che dà atto di come le Corti riconoscano generalmente una legittima aspettativa di *privacy* rispetto al contenuto dell'*hard disk* del *computer*.

[11] *Katz v. United States*, 389 U. S. 347 (1967). In tale precedente è stato elaborato il *reasonable expectation of privacy test*. Tale *test*, secondo la formulazione risultante dalla *concurring opinion* del giudice Harlan, esige una doppia valutazione: per stabilire se un'attività d'indagine sia qualificabile come *search*, occorre verificare innanzitutto se il soggetto che ne è destinatario abbia manifestato un'aspettativa soggettiva di *privacy*, e in secondo luogo, se si tratti di un'aspettativa che la società è disposta a riconoscere come ragionevole. In assenza di leggi processuali positive, il compito di stabilire quando un'attività d'indagine sia ragionevole e quando si debbano applicare le garanzie costituzionali è stato naturalmente assunto dalla Corte Suprema, il cui *case law* ha progressivamente delineato un sistema di regole volto a tracciare un equo bilanciamento tra esigenze investigative e tutela dei singoli, che passa attraverso la qualificazione di una determinata attività come perquisizione o sequestro.

[12] Il caso risale al 2001. *United States v. Gorshkov*, 23 May 2001, WL 1024026, U.S. Dist. Gli agenti *FBI* non erano in origine in possesso di un mandato di perquisizione, hanno però aspettato di ottenerlo prima di leggere e copiare i *files* scaricati. La *District Court* di Washington ha ritenuto non sussistente una violazione del IV Emendamento in quanto «esso non si applica a perquisizioni e sequestri di cose di proprietà di stranieri non residenti [negli Stati Uniti] e che avvengano al di fuori del territorio nazionale. Nel caso di specie, i *computers* a cui gli agenti hanno avuto accesso erano situati in Russia, così come i dati copiati. Fino quando i dati copiati non sono stati trasmessi negli Stati Uniti, essi si trovavano fuori dal territorio di questo Paese e quindi non erano soggetti alla tutela del IV Emendamento». Cfr. J. R. Herrera-Flanigan, *Cybercrime and Jurisdiction in the United States*, in B. J. Koops – S. W. Brenner (a cura di), *Cybercrime and Jurisdiction. A Global Survey*, TMC Asser Press, The Hague, 2006, p. 313 ss.

[13] G.U.U.E. 17 marzo 2009, C 62/16.

[14] Direttiva 2011/92/UE, che sostituisce la DQ 2004/68/GAI, G.U.U.E. 17 dicembre 2011, L 351/1.

elettronici di sorveglianza, […] tenuto conto del principio di proporzionalità e del carattere e della gravità dei reati oggetto di indagine» – anche in questo caso il riferimento sembra essere alle *online searches* –.

L'Unione Europea si sta muovendo nel senso di stimolare il rinnovamento e l'armonizzazione dei sistemi processuali nazionali per quanto riguarda gli strumenti di indagine[15]. Come emerso dai lavori preparatori delle *Model Rules* elaborate dall'Università del Lussemburgo per l'istituendo Pubblico Ministero Europeo[16], il livello di armonizzazione raggiunto a livello europeo varia in ragione del tipo di mezzo di ricerca della prova, e per quanto riguarda le misure di *surveillance* cui appartengono anche le *online searches*, «l'unico elemento che pare accomunare le legislazioni nazionali è l'assenza di una disciplina puntuale nelle legislazioni nazionali»[17]. In quest'ambito è infatti diversa la sensibilità degli ordinamenti: alcuni reagiscono prima, in via legislativa o giurisprudenziale, riconoscendo la peculiarità dei nuovi strumenti investigativi ed apprestando una disciplina *ad hoc*; altri ricorrono all'applicazione analogica di norme dettate per misure affini o alla categoria della prova atipica. Il fenomeno non è nuovo, ma sviluppa criticità nuove in un contesto in cui sempre più spesso vi sono occasioni di confronto tra sistemi giuridici diversi a causa della transnazionalità della criminalità e della natura digitale della prova[18].

È pertanto opportuna una riflessione di ampio respiro, che tenga conto dei due interessi in gioco, da bilanciare: da un lato l'esigenza di repressione e prevenzione dei reati (sempre più spesso a dimensione transnazionale), dall'altro quella di tutela e rispetto dei diritti fondamentali della persona[19]. Riflessione che deve essere condotta non solo a livello nazionale, ma anche a quello europeo ed internazionale. Ciò sia perché lo spazio informatico (e quindi sia la criminalità informatica che le indagini informatiche) è globale e refrattario a limitazioni territoriali, sia perché, in considerazione del valore che oggi la Carta di Nizza e la CEDU hanno nell'ordinamento interno, la tutela dei diritti fondamentali è garantita da un sistema integrato di protezione che si articola per l'appunto sui tre livelli nazionale, europeo ed internazionale.

All'interno di tale panorama, il presente articolo si propone di vagliare l'ammissibilità delle c.d. perquisizioni *online* nell'ordinamento italiano.

Poiché in una concezione liberale del rito penale il potere investigativo costituisce un'eccezione alla regola della libertà, occorre prendere le mosse dall'individuazione dei diritti fondamentali coinvolti. Ciò consentirà innanzitutto di verificare se sia possibile, e – in caso di risposta affermativa – in che termini, inquadrare codesto strumento di acquisizione probatoria nell'ambito di istituti tipici. In secondo luogo, nel caso di esito negativo, si potrà vagliare la possibilità di considerarlo un mezzo di ricerca della prova atipico, tenendo a mente che il primo limite di ammissibilità di una prova «non disciplinata dalla legge» (art. 189 c.p.p.) è

[15] In tal senso è apprezzabile la proposta di Regolamento per l'istituzione della Procura Europea che, all'art. 26, contiene un elenco degli strumenti di indagine che gli Stati membri devono mettere a disposizione del Pubblico Ministero Europeo, obbligandoli ad introdurli nell'ordinamento interno se non previsti. Cfr. S. Allegrezza, *Verso una Procura europea per tutelare gli interessi finanziari dell'Unione. Idee di ieri, chances di oggi, prospettive di domani*, in *Dir. Pen. Cont.*, 31 ottobre 2013. Lo scorso aprile è stata inoltre approvata la Direttiva relativa all'Ordine Europeo di Indagine Penale (2014/41/UE, in G.U.U.E. 1 maggio 2014, L 130/1). Tale strumento, basato sul principio del mutuo riconoscimento, consente all'autorità competente di uno Stato membro di ottenere che l'autorità competente di un altro Stato membro compia uno o più atti di indagine specifici e si presta a ricomprendere anche le misure di *electronic surveillance*. Apprezzabile è quindi la previsione della possibilità per lo Stato ricevente di ricorrere ad un diverso strumento di indagine qualora sia in grado di garantire lo stesso risultato, ma in maniera meno intrusiva (proporzionalità).

[16] Il progetto è stato coordinato dalla Professoressa Katalin Ligeti dell'Università del Lussemburgo. Le *Model Rules* e la Relazione introduttiva della Prof. Katalin Ligeti sono disponibili all'indirizzo http://www.eppo-project.eu/index.php/EU-model-rules e saranno pubblicate insieme al report finale in K. Ligeti (ed.), *Toward a Prosecutor for the European Union. Draft Rules of procedure, Volume 2*, Oxford, 2013 (in corso di pubblicazione).

[17] S. Allegrezza, *Le misure coercitive nelle* «Model Rules for the Procedure of the European Public Prosecutor's Office», in F. Ruggieri, T. Rafaraci, G. Di Paolo, S. Marcolini, R. Belfiore (a cura di), *Processo penale, lingua e Unione Europea*, Padova, 2013, p. 151 ss.

[18] S. Allegrezza, *Le misure coercitive*, cit.

[19] Come recentemente ribadito dalla Corte di Giustizia nella sentenza sulla c.d. *data retention*, la lotta contro gravi forme di criminalità rappresenta un interesse per il cui perseguimento sono ammissibili limitazioni dei diritti fondamentali, purché esse avvengano nel rispetto dei presupposti fissati dalla legge e del principio di proporzionalità. Cfr., Giustizia dell'Unione Europea, 8 aprile 2014, (C-293/12, C-594/15), *Digital Rights Ireland Ltd.*, par. 42-46, con nota di R. Flor, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d.* "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. Pen. Cont.*, 28 aprile 2014 e di E. Colombo, "Data retention" *e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 2014, p. 2705 ss.

proprio la sua legittimità costituzionale[20].

3. Verso il superamento della distinzione tra segretezza e riservatezza.

L'accesso "segreto" ad un sistema informatico è suscettibile di ledere a più livelli la sfera privata di ogni individuo. Vengono in rilievo delicati profili di garanzia della libertà e segretezza delle comunicazioni (art. 15 Cost.) e dell'inviolabilità del domicilio (art. 14 Cost.), di tutela della riservatezza (artt. 2 Cost., 8 CEDU, 7 Carta dei Diritti Fondamentali dell'Unione Europea – di seguito CDFUE) e dei dati personali (art. 8 CDFUE, art. 16 TFUE).

Infatti, come riconosciuto dalla Corte costituzionale tedesca nella sentenza sulla *Online Durchsuchung*, i dispositivi informatici hanno acquisito un'importanza fondamentale quali strumenti di sviluppo della personalità. E quindi, così come il domicilio è tutelato in quanto proiezione spaziale della persona, luogo in cui essa svolge la propria vita privata lontano da occhi indiscreti, anche i "luoghi" *informatici* o *virtuali* in cui sono salvati dati, meritano protezione costituzionale. A tal fine, tuttavia, i diritti fondamentali già esistenti si rivelano inadeguati.

Occorre infatti considerare che il sistema informatico è un sistema complesso, contenente una moltitudine diversificata di dati e che d'altro canto non è ancora possibile un accesso selettivo al dispositivo tecnologico. Il termine dati informatici è riassuntivo di una pluralità di informazioni, di diversa natura, in grado di circolare con grande facilità e rapidità, prive di una dimensione fisica, duplicabili su più supporti[21]. Nel contesto tecnologico odierno è quindi superata la distinzione tra dati intimi e dati sociali, tra informazioni segrete e informazioni riservate. Un dato apparentemente innocuo, collegato ad altri dati altrettanto apparentemente innocui può in realtà rivelare aspetti della vita di una persona che si desiderano sottrarre alla conoscenza altrui. La promiscuità dei dati e il tipo di intromissione da parte dell'autorità pubblica fanno quindi sì che il pericolo per il diritto della personalità in generale sia qualitativamente e quantitativamente diverso da quello di una *semplice* raccolta di dati, a cui fa da baluardo il diritto all'autodeterminazione informativa, quale filiazione del diritto alla *privacy*.

Si rende quindi necessario tutelare il sistema informatico in quanto spazio in cui il singolo manifesta la sua personalità, a prescindere dalla natura delle informazioni che vi si affidano.

Nel mondo del *Web* 2.0, delle comunicazioni globali e del *cloud computing*, non si può più distinguere tra sfera privata e sfera pubblica[22], e la stessa nozione di *privacy* muta e si arricchisce di contenuti nuovi. Da un lato, l'originario *right to be let alone*[23] perde ogni riferimento alla realtà fisica; dall'altro, il *right to control the information about oneself*, acquista il significato di un diritto di controllo sui pacchetti di dati che viaggiano nel *web*. Sebbene quindi una definizione di *privacy* come diritto di essere lasciato solo abbia da tempo perso valore generale,

[20] Non si dubita dell'applicabilità dell'art. 189 c.p.p anche alla fase delle indagini preliminari; come correttamente osservato in dottrina, le disposizioni generali collocate nel titolo I del libro III costituiscono un catalogo di principi guida in materia probatoria, come tali applicabili «all'intero arco del procedimento, anche in via analogica, fuorché nei casi in cui norme speciali dettate per le diverse fasi, o peculiari previsioni di legge, non le deroghino». Cfr. M. Nobili, sub *art. 189 c.p.p.*, in AA.VV., *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, tomo II, Torino, 1990, p. 387. Anche la giurisprudenza ammette che l'art. 189 c.p.p. sia applicabile alle indagini atipiche, in quanto «*il contraddittorio previsto dall'art. 189 c.p.p. non riguarda la ricerca della prova, ma la sua assunzione e interviene dunque* […] *quando il giudice è chiamato a decidere sull'ammissione della prova*». Così, in tema di riprese visive, Cass., Sez. un. 28 marzo 2006, n. 26795, Prisco, con nota di M. L. Di Bitonto, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, e di F. Ruggieri, *Riprese visive e inammissibilità della prova*, in *Cass. pen.* 2006, p. 3937 s.; e di A. Camon, *Le Sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento ed alcuni dubbi nuovi*, in *Riv. it. dir. e proc. pen.* 2006, p. 1550 ss.

[21] I dati digitali sono immateriali, si risolvono in informazioni espresse in codice binario (c.d. *bit*, sequenze di 0 e 1), ma per essere fruibili e intellegibili hanno bisogno di un supporto fisico, di una *res* in cui essere incorporati. Essi sono, tuttavia, indipendenti e scindibili dal supporto informatico che li contiene, possono essere duplicati un'infinità di volte su supporti diversi e rimangono sempre uguali a se stessi.

[22] Ben si comprende quindi come non si possa più fare ricorso alla nota teoria delle sfere (*Sphärentheorie*), elaborata dalla dottrina tedesca verso la metà del secolo scorso e secondo la quale in base al grado di intimità delle informazioni, l'*allgemeines Persönlichkeitsrecht*, il generale diritto della personalità, oppone una resistenza più o meno maggiore a forme di intromissione da parte dei pubblici poteri. Sarebbe quindi possibile distinguere tra *Privatsphäre*, che comprende le notizie private, ed è quella più ampia, *Vertrauensphäre*, al cui interno sono ricomprese le notizie confidenziali, e *Gehemnisphäre* o *Intimsphäre* che riguarda notizie segrete e che costituisce il nocciolo duro, il nucleo inviolabile del diritto della personalità. Tale teoria è stata elaborata da H. Hubmann, *Das Persönlichkeitsrecht*, Münster-Köln-Böhlau, 1953, p. 17, e ripresa da Bricola nel noto scritto *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. e proc. pen.*, 1967, p. 1083 ss.

[23] Elaborato da S. D. Warren, L. D. Brandeis, *The Right to Privacy*, in *Harv. L. Rev.*, 4 (1890), p. 193 ss.

essa continua a cogliere un aspetto essenziale del problema[24]. Si avverte infatti la necessità di riaffermare l'esistenza di quella sfera di riservatezza, i cui classici confini, legati agli spazi fisici e al tipo di informazioni che si vuole sottrarre alla conoscenza altrui, sfumano e si dissolvono[25].

Occorre pertanto prendere atto dell'esistenza di un nuovo bene giuridico, meritevole di protezione costituzionale.

A tal proposito illuminanti sono le riflessioni dei penalisti intorno al bene giuridico tutelato da alcune delle nuove norme in materia di criminalità informatica (artt. 615 *ter*, 615 *quater*, 617 *quater*, 617 *quinquies*, 617 *sexies* c.p.)[26]. Inizialmente, e in considerazione del tenore letterale della relazione alla legge 574 del 1993, secondo la quale il legislatore intendeva tutelare i sistemi informatici e telematici quali «espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti essenziali agli articoli 614 e 615 del codice penale»[27], si era individuato il bene giuridico protetto dagli artt. 615 *ter* e 615 *quater* nel c.d. domicilio informatico. Tuttavia, come evidenziato da acuta dottrina «il parallelismo con il domicilio, bene eminentemente privato e personale, coglie solo parzialmente il contenuto dell'interesse all'*esclusione di terzi* da determinate "sfere di disponibilità e rispetto", create e rese fruibili dalla tecnologia informatica»[28].

L'intuizione, che si condivide, consiste nel riconoscere che l'interesse dell'utilizzatore di sistemi informatici e telematici è quello alla tutela dei propri dati, a prescindere dal "luogo" in cui si trovino, o dal mezzo di comunicazione prescelto. Tale affermazione è ben esemplificata attraverso il ricorso alla teoria c.d. assiomatica, anziché concentrica, delle sfere di tutela della vita privata[29]. Secondo tale ricostruzione, all'interno di un sistema informatico o telematico non ha più senso distinguere tra sfera individuale e sfera privata, ma occorre prendere atto dell'esistenza di «spazi virtuali di manifestazione della personalità, che coincidono con l'interesse sostanziale alla protezione di informazioni "riservate" e al loro controllo nello svolgimento di rapporti giuridici e personali *online* o in altri spazi "informatici"»[30].

Il discorso si sposta quindi dal domicilio alla riservatezza, ma non per arrivare ad una distinzione, quanto a copertura costituzionale, circa limiti e presupposti di ingerenza da parte degli investigatori, come hanno fatto le Sezioni Unite in materia di videoriprese[31], bensì per teorizzare, assieme alla più attenta dottrina penalistica[32], l'esistenza di un diverso bene giuridico tutelato: la *riservatezza informatica*[33]. Tale diritto nasce come espansione del domicilio per

[24] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 104 ss.

[25] Sostiene S. Rodotà, *Il diritto di avere diritti*, Roma, 2012, p. 319, che «nella dimensione tecnologica l'identità personale sembra dilatarsi, […] disperder[si], […] sino a diventare inconoscibile da parte dello stesso interessato». Infatti, «le informazioni riguardanti la stessa persona sono contenute in banche dati diverse, ciascuna delle quali restituisce soltanto una parte o un frammento dell'identità complessiva». Talvolta addirittura lo stesso interessato non sa dove siano dislocati i propri dati personali. Si tratta quindi di apprestare idonee forme di tutela di questa «identità esterna, […] frutto di un'operazione nella quale sono gli altri a giocare un ruolo decisivo, con la presenza continua di elaborazione e controllo».

[26] Per la distinzione dei reati informatici in tre diverse categorie a seconda del bene giuridico tutelato (e delle modalità di aggressione) si rinvia a L. Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in Id. (a cura di), *Il diritto penale dell'informatica nell'epoca di* Internet, Padova, 2004, p. 53, 54.

[27] Così, la Relazione ministeriale al disegno di legge, p. 9.

[28] Testualmente, L. Picotti, *Sistematica dei reati informatici*, cit., p. 80.

[29] L'elaborazione di tale teoria si deve a R. Flor, Phishing, identity theft, *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, *Riv. it. dir. proc. pen.*, 2007, p. 899 ss.; Id., *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht, cit.; Id, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di* Internet, in *Dir. Pen. Cont.*, 22 settembre 2012.

[30] R. Flor, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht, cit., p. 705.

[31] Come noto, il "mero" carattere riservato di luoghi diversi dal domicilio giustifica presupposti meno stringenti per un'eventuale limitazione rispetto a quelli richiesti dall'art. 14 Cost. per intromissioni nel domicilio. E quindi, mentre le videoriprese in ambito domiciliare, in mancanza di una specifica disposizione di legge, sono illegittime, quelle in luoghi riservati, tutelati dall'art. 2 Cost., sarebbero possibili se autorizzate da un provvedimento del pubblico ministero, rientrando nell'ampia previsione dell'art. 189 c.p.p. Cfr. Cass., sez. un., 28 marzo 2006, Prisco, cit.

[32] L. Picotti, *Sistematica dei reati informatici*, cit., p. 87 ss.; Id., *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. merito*, 2012, p. 2532; R. Flor, *Lotta alla "criminalità informatica"*, cit.; Id., *Verso una rivalutazione dell'art. 615* ter *c.p.?,* in *Dir. pen. cont – Riv. trim.*, n. 2/2012, p. 126 ss.; Id., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo* jus excludendi alios, in *Dir. pen. proc.*, 2005, p. 81 ss.

[33] La riservatezza informatica è definita quale «interesse al godimento e controllo esclusivo sia di determinati dati e informazioni, che dei relativi mezzi e procedimenti informatici e telematici di trattamento, che pur configurandosi sempre quale «diritto di escludere» i terzi non legittimati dal corrispondente accesso e utilizzo, prescinde in tutto o in parte dai tradizionali limiti e presupposti dei concetti civilistici di proprietà o possesso, ovvero dalle condizioni che fondano la rilevanza giuridica del segreto o della riservatezza personale in genere». Così, L. Picotti, (voce) *Reati informatici*, in *Enc. giur. Treccani*, agg. VIII, Roma, 2000, p. 20 ss. Si veda anche R. Flor, Phishing, identity theft, cit., secondo cui «il bene giuridico "riservatezza informatica", protetto dall'art. 615-*ter* c.p., si può configurare come interesse esclusivo, giuridicamente riconosciuto, di godere, disporre e controllare le informazioni, i procedimenti, i sistemi e "spazi" informatizzati e le relative utilità».

acquistare autonomia in un ambito, quello digitale, in cui non ci sono confini, non ci sono luoghi *fisici* che possano riflettere il carattere privato o riservato delle attività che ivi si svolgano o di ciò che vi sia custodito[34].

Nell'ottica del processualpenalista si pone a questo punto il problema di individuare il fondamento costituzionale di tale diritto, al fine di stabilire i presupposti per una sua legittima limitazione da parte dell'autorità pubblica. Infatti, si tratta pur sempre di un diritto soggetto al bilanciamento con contrapposti interessi ed esigenze, tra cui vanno senz'altro annoverate quelle di repressione dei reati.

4. Il diritto fondamentale alla riservatezza informatica.

Tradizionalmente il diritto alla riservatezza viene ricondotto all'art. 2 Cost., quale fattispecie "aperta", fonte di nuovi diritti della personalità[35]. Tuttavia, quando si tratta di bilanciare tale diritto con le esigenze di repressione dei reati, il richiamo al solo art. 2 Cost. mostra i suoi limiti. Tale norma, infatti, contrariamente agli artt. 13, 14 e 15 Cost., non individua i presupposti di una limitazione da parte della pubblica autorità dei diritti inviolabili ivi sanciti[36].

L'impostazione tradizionale deve oggi essere integrata alla luce del valore che è riconosciuto nel nostro ordinamento all'art. 8 CEDU che tutela il diritto al rispetto della vita privata. Infatti, secondo l'insegnamento della Corte costituzionale[37], i diritti fondamentali riconosciuti dalla CEDU, così come interpretati dalla Corte di Strasburgo, integrano quali "norme interposte" il parametro costituzionale espresso dall'art. 117, comma 1 Cost., nella parte in cui impone la conformazione della legislazione interna ai vincoli derivanti dagli ordinamenti internazionali, e da questo ripetono il loro rango all'interno del sistema delle fonti[38].

Il valore aggiunto dell'ancoraggio del fondamento costituzionale del diritto alla riservatezza all'art. 8 CEDU deriva dal fatto che tale norma individua le condizioni che devono sussistere affinché un'intromissione da parte della pubblica autorità nell'esercizio del diritto stesso sia legittima. Si deve trattare di un'ingerenza prevista dalla legge, che costituisca «una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la sicurezza pubblica, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, per la protezione dei diritti e delle libertà degli altri» (art. 8, par. 2 CEDU)[39].

Affinché un'attività d'indagine sia considerata «prevista dalla legge», occorre, secondo la Corte di Strasburgo, che essa abbia una base nel diritto interno – di creazione legislativa o giurisprudenziale – sia conoscibile dall'interessato e, soprattutto, che questi sia in grado di prevedere le conseguenze derivanti dall'applicazione della misura nei suoi confronti.

[34] La matrice del nuovo diritto è quindi pur sempre l'esigenza di riservatezza del titolare dello *ius excludendi alios*, ma essa va oltre la dimensione originaria della *privacy* e della tutela del domicilio, pur nella sua accezione di domicilio informatico. Cfr. R. Flor, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht, cit., p. 705.

[35] Come noto, la discussione sulla natura "aperta" o "chiusa" di questa norma è stata al centro di un acceso dibattito tra i costituzionalisti. Da un lato vi era chi la considerava una clausola riassuntiva di diritti di libertà espressamente tutelati nelle altre norme costituzionali (P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, p. 54 ss.; A. Pace, *Diritti «fondamentali» al di là della Costituzione*, in *Pol. dir.* 1993, p. 3 ss.), dall'altro si attribuiva all'art. 2 Cost. la funzione di tutela ora di diritti naturali non presenti nel testo costituzionale, ora di quei valori di libertà emergenti a livello di costituzione materiale (A. Barbera, *Art. 2*, in A. Branca (a cura di), *Commentario della Costituzione. Principi fondamentali*, Bologna, 1975, p. 65 ss.).

[36] F. B. Morelli, *La giurisprudenza costituzionale italiana tra diritto alla riservatezza e potere di controllo sulle informazioni personali*, in D. Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 41.

[37] C. cost., 24 ottobre 2007, n. 348, in *Giur. cost.*, 2007, p. 3475 ss., con nota di C. Pinelli, *Sul trattamento giurisdizionale della CEDU e delle leggi con essa confliggenti*; C. cost., 24 ottobre 2007, n. 349, *ivi*, 2007, p. 3535 ss., con nota di M. Cartabia, *Le sentenze "gemelle": diritti fondamentali, fonti, giudici*. Precisano che norme costituzionali e norme convenzionali danno vita ad un sistema integrato di tutela dei diritti fondamentali, il quale mira alla massima espansione delle garanzie, C. cost., 26 novembre 2009, n. 311, *ivi*, 2009, p. 4657 ss., con nota di M. Massa, *La "sostanza" della giurisprudenza europea sulle leggi retroattive* e C. cost. 4 dicembre 2009, n. 317, *ivi*, 2009, p. 4747 ss., con nota di G. Ubertis, *Sistema multilivello dei diritti fondamentali e prospettiva abolizionista del processo contumaciale*.

[38] Diversamente da quanto accade per il diritto dell'Unione, cui è riconosciuto primato sul diritto interno, i diritti fondamentali riconosciuti dalla CEDU sono quindi privi di effetto diretto. Da ciò deriva che eventuali contrasti tra norme interne e diritti convenzionali debbano essere risolti dalla Corte costituzionale, adita dal giudice *a quo*, nel caso in cui non sia possibile un'interpretazione convenzionalmente conforme. Cfr. Così, M. Cartabia, *La convenzione europea dei diritti dell'uomo e l'ordinamento italiano*, in A. Balsamo, R. E. Kostoris (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, p. 54.

[39] L'ingerenza, per essere compatibile con la Convenzione deve rispondere a un «bisogno sociale imperativo» ed essere proporzionata al perseguimento di uno scopo legittimo. Corte europea dei diritti dell'uomo, *Leander v. Sweden*, 26 marzo 1987, ric. n. 9248/81.

La nozione di vita privata fatta propria dall'art. 8 CEDU e dalla giurisprudenza di Strasburgo «è ampia e non suscettibile di una definizione esaustiva»[40]. La stessa Corte infatti evita di dare una definizione di vita privata ma, seguendo un approccio "in negativo"[41] e casistico, si impegna a qualificare le possibili interferenze nel suddetto diritto, fornendone un'interpretazione aperta ed evolutiva. Tale norma si presta quindi a fungere da baluardo nei confronti di diverse attività di indagine: intercettazioni telefoniche[42], acquisizione dei tabulati[43], intercettazione di *e-mail* e di comunicazioni via *Internet*[44], sorveglianza via *GPS*[45] costituiscono altrettante ingerenze nell'art. 8 CEDU. A seconda, tuttavia, dell'intensità dell'ingerenza nel suddetto diritto, la Corte EDU tollera una maggiore discrezionalità del legislatore nazionale nel fissare i requisiti del singolo mezzo di ricerca della prova.

Quanto all'ordinamento italiano, la giurisprudenza della Cassazione considera interpretazione conforme alla Convenzione l'applicazione ad attività d'indagine non tipizzate dal legislatore, suscettibili di ledere la vita privata dell'individuo, di quel "livello minimo di garanzie", rappresentato da un provvedimento motivato dell'autorità giudiziaria[46]. Tale orientamento è stato seguito in materia di acquisizione dei tabulati telefonici[47], di videoriprese eseguite in luoghi riservati diversi dal domicilio[48], e infine di registrazioni fonografiche eseguite da uno degli interlocutori con strumenti di captazione forniti dalla polizia giudiziaria[49], e muove dall'assunto che in questi casi il grado di intrusione nella sfera privata sarebbe inferiore rispetto a quello causato dallo strumento tipico, ossia le intercettazioni, e giustificherebbe quindi un livello di garanzia minore, soddisfatto da un decreto motivato del pubblico ministero. Il presupposto è quindi che la riservatezza costituisca un *minus* rispetto alla segretezza delle comunicazioni o all'inviolabilità del domicilio.

Questo ragionamento, tuttavia, non può essere applicato alla c.d. riservatezza informatica, che pure si ritiene tutelata dall'art. 8 CEDU. Infatti, come si è visto, essa rappresenta un bene giuridico nuovo, tipico di un contesto, quello digitale e informatico, in cui non è possibile distinguere tra attività o informazioni riservate e segrete. Pertanto, se si segue l'impostazione della Corte di Strasburgo, secondo cui i presupposti di legittimità delle diverse attività di indagine variano in relazione al grado di intrusività della misura stessa, mezzi di ricerca della prova, quali le perquisizioni *online*, che limitano il diritto alla riservatezza informatica, devono essere disciplinati in maniera puntuale e rigorosa dal legislatore.

L'analisi non può tuttavia arrestarsi alla sola Convenzione Europea dei Diritti dell'Uomo. Infatti, i c.d. diritti di *privacy* sono tutelati anche dalla Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE), a cui il Trattato di Lisbona ha attribuito lo stesso valore giuridico dei Trattati, ossia efficacia giuridica vincolante per gli Stati membri, seppur nelle sole materie di competenza dell'Unione[50].

Le norme che vengono in rilievo, ai fini che qui interessano, sono gli articoli 7 e 8 della Carta che tutelano rispettivamente il diritto al rispetto della vita privata e familiare, del domicilio e delle comunicazioni, e il diritto alla protezione dei dati personali.

Ai sensi dell'art. 52, comma 3 CDFUE «laddove la […] Carta contenga diritti corrispon-

[40] Corte Europea dei Diritti dell'Uomo, *Pretty v. United Kingdom*, 29 aprile 2002, ric. n. 2346/02.

[41] Così, V. Zeno Zencovich, sub *Art. 8*, in S. Bartole, B. Conforti, G. Raimondi (a cura di), *Commentario alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2011, p. 309.

[42] Corte Europea dei Diritti dell'Uomo, *Klass v. Germany*, 6 settembre 1978, ric. n. 5029/71.

[43] Corte Europea dei Diritti dell'Uomo, *Malone v. United Kingdom*, 2 agosto 1984, ric. n. 8691/79.

[44] Corte Europea dei Diritti dell'Uomo, *Copland v. United Kingdom*, 3 aprile 2007, ric. n. 62617/00.

[45] Corte Europea dei Diritti dell'Uomo, *Uzun v. Germany*, 2 settembre 2010, ric. n. 35623/05.

[46] Esse vengono quindi ricondotte all'art. 189 c.p.p.

[47] Cass., sez. un., 23 febbraio 2000, D'Amuri, in *Giur. it.*, 2001, p. 1707 ss. La materia è oggi regolata dall'art. 132 codice *privacy* (d. lgs. 196/2003), da ultimo modificato dal d. lgs. 109/2008 di attuazione della direttiva c.d. *data retention* 2006/24/CE, oggetto della recente sentenza della Corte di Giustizia (*Digital Rights Ireland Ltd.*, cit.), che l'ha ritenuta incompatibile con gli artt. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea. Per una prima riflessione sulle possibili conseguenze di tale decisione sull'art. 132 codice *privacy*, si veda R. Flor, *La Corte di Giustizia considera la direttiva europea*, cit. In merito, sia consentito rinviare inoltre a F. Iovene, Data retention *tra passato e futuro. Ma quale presente?* in corso di pubblicazione in *Cass. pen.*, n. 12/2014.

[48] Cass., sez. un., 28 marzo 2006, Prisco, cit.

[49] Cass., sez. IV, 7 aprile 2010, Angelini, in *C.E.D. Cass.*, n. 247384. In tale pronuncia la Cassazione afferma espressamente che «*il provvedimento motivato dell'autorità giudiziaria, sia esso giudice o pubblico ministero, è altresì idoneo a garantire il rispetto dell'art. 8 della CEDU, nella interpretazione che ne è stata data dalla Corte Europea dei Diritti dell'Uomo, offrendo un'adeguata tutela contro le ingerenze arbitrarie dei pubblici poteri nella vita privata*». Cfr. il commento di P. Gaeta, *Per utilizzare registrazioni fra presenti fatte dalla Pg è sufficiente un decreto del pubblico ministero*, in *Guida dir.*, 2010, p. 75 ss.

[50] L'art. 51 della Carta precisa ulteriormente che essa si applica agli Stati membri «esclusivamente nell'attuazione del diritto dell'Unione».

denti a quelli garantiti dalla [CEDU], il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione» (c.d. clausola di equivalenza). E quindi, gli articoli 7 e 8 CDFUE vanno riempiti di significato alla luce dell'art. 8 CEDU e della relativa giurisprudenza della Corte di Strasburgo, soprattutto per quanto riguarda i presupposti di un'ingerenza legittima negli stessi da parte della pubblica autorità[51].

Tuttavia, la circostanza che gli articoli 7 e 8 CDFUE, in quanto filiazione dell'art. 8 CEDU, siano tra loro intimamente connessi tanto da integrare un «diritto alla vita privata con riguardo al trattamento dei dati personali»[52], non deve tradursi in una mancata valorizzazione delle differenze.

Infatti, proprio con riferimento alla tutela della riservatezza informatica, a venire in rilievo è l'art. 7 della Carta e non l'art. 8. Non si tratta tanto di garantire all'interessato il controllo sulle modalità di trattamento dei propri dati personali, quanto, prima ancora, di tutelare la persona in un contesto nel quale gli aspetti più variegati della propria vita si sono tradotti in dati, suscettibili di trattamento informatico[53]. In un ambito nel quale non è più possibile distinguere tra dati intimi, dati riservati e dati sociali, l'art. 8 CDFUE risulta inapplicabile e tornerà ad operare l'ampia protezione offerta dall'art. 7 a tutela della vita privata.

La riservatezza informatica può quindi essere ricondotta all'art. 7 CDFUE, con la conseguenza che eventuali limitazioni all'esercizio di tale diritto dovranno essere previste dalla legge, rispettarne il contenuto essenziale e, nel rispetto del principio di proporzionalità, potranno essere apportate solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui (art. 52, comma 1 CDFUE).

Si può in conclusione affermare che il diritto fondamentale alla riservatezza informatica è riconosciuto e tutelato dagli artt. 2 Cost., 117 Cost. e 8 CEDU, 7 e 52 CDFUE e che, al pari dei tradizionali diritti fondamentali (libertà personale, libertà domiciliare, libertà e segretezza delle comunicazioni), esso potrà essere limitato solo nel rispetto della riserva di legge e di giurisdizione, alla luce del principio di proporzionalità.

5. Le c.d. perquisizioni *online* nell'ordinamento italiano.

Le c.d. perquisizioni *online* rappresentano un istituto di natura ibrida e di difficile inquadramento giuridico.

Esse non sono disciplinate nell'ordinamento giuridico italiano, tuttavia è opportuno segnalare due casi affrontati dalla giurisprudenza di legittimità in cui si è fatto uso di tecniche di indagine in senso lato assimilabili alla *Online Durchsuchung*. Il primo riguarda l'utilizzo di un c.d. captatore informatico (*gotsh*), in grado di acquisire in remoto copia dei *files* esistenti sul *computer* e di registrare in tempo reale i *files* elaborandi[54]. Il secondo è il più noto *caso Ryanair*, avente ad oggetto la perquisizione *ex* art. 247 c.p.p. e successivo sequestro delle credenziali di accesso al sistema *online* di prenotazione dei voli della suddetta compagnia aerea[55].

In entrambe le ipotesi, attraverso l'utilizzo di strumenti tipici si realizzava in realtà un monitoraggio continuativo – ed occulto nel primo caso – del sistema informatico oggetto di indagine.

[51] Tale equivalenza è stata ribadita dalla stessa Corte di Giustizia in due recenti pronunce in materia di tutela di diritti d'autore in *Internet*. Corte di Giustizia dell'Unione Europea, 24 novembre 2011 (C-70/10) e Corte di Giustizia dell'Unione Europea, 16 febbraio 2012, C 360/10, caso "*SABAM v. Netlog*". In merito si rinvia a R. Flor, *Lotta alla "criminalità informatica"*, cit. Ciò tuttavia ancora non significa che il diritto CEDU trovi diretta applicazione negli Stati membri, come accade per le norme della CDFUE che hanno lo stesso valore giuridico dei Trattati. Infatti, la Carta rimane soggetta al sindacato della Corte di Giustizia, che potrà eventualmente operare un diverso bilanciamento degli interessi in gioco. Cfr. C. Sotis, *Convenzione europea dei diritti dell'uomo e diritto comunitario*, in V. Manes, V. Zagrebelsky, *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Milano, 2011, p. 144.

[52] Corte di Giustizia dell'Unione Europea, 9 novembre 2010, *Volker und Markus Schecke e Eifert*, C-92/09 e C-93/09.

[53] Nella recente sentenza sulla direttiva c.d. *data retention* (C-293/12, C-594/15, *Digital Rights Ireland Ltd*) la Corte di Giustizia ha riconosciuto che la conservazione dei dati di traffico telefonico e telematico costituisce un'interferenza con l'art. 7 della Carta. Infatti, affinché scatti la protezione offerta da tale norma si prescinde dalla natura sensibile o meno dei dati e dall'apprensione del contenuto della comunicazione. Cfr. R. Flor, *La Corte di Giustizia considera la direttiva europea*, cit.

[54] Cass., sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass.*, n. 246954. Cfr. S. Aterno, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss.

[55] Cass., sez. IV, 17 aprile 2012, n. 19618, in *Cass. pen.*, 2013, p. 1523 ss.

Per quanto riguarda il c.d. captatore informatico, infatti, l'acquisizione dei *files* era stata disposta con decreto del pubblico ministero ai sensi dell'art. 234 c.p.p.

La Suprema Corte ha respinto le eccezioni sollevate dal ricorrente, il quale sosteneva innanzitutto che si sarebbe dovuta applicare la disciplina delle intercettazioni informatiche, e che in ogni caso l'attività posta in essere violava gli artt. 14 e 15 Cost. e doveva pertanto considerarsi una prova incostituzionale, e i relativi risultati inutilizzabili ai sensi dell'art. 191 c.p.p.

Quanto alla prima eccezione, la Corte ha ritenuto che correttamente i giudici di merito avessero escluso l'applicazione della disciplina di cui agli artt. 266 ss. c.p.p., in quanto il decreto del pubblico ministero non aveva ad oggetto un flusso di comunicazioni, bensì «*una relazione operativa tra microprocessore e video del sistema elettronico, ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del* personal computer». Non trattandosi di comunicazione, non trovava quindi applicazione la tutela di cui all'art. 15 Cost. Né la Corte riscontra una violazione dell'art. 14 Cost. in quanto il *computer* monitorato non si trovava all'interno del domicilio – inteso come luogo di privata dimora – ma in un luogo aperto al pubblico.

Se si può convenire sull'esclusione della garanzia di cui all'art. 15 Cost., l'argomentazione con cui la Corte esclude l'applicabilità dell'art. 14 Cost. appare troppo frettolosa. In ogni caso poi, tali prescrizioni costituzionali non esauriscono il novero dei diritti fondamentali che simile attività di indagine comprime. Se anche, nelle parole della Corte, «*quanto riprodotto in copia non era un testo inoltrato e trasmesso col sistema informatico, ma soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario*», persistono comunque esigenze di tutela della riservatezza, *sub specie* di riservatezza informatica, bene giuridico di rango costituzionale, che avrebbero richiesto un esame più approfondito della vicenda.

Oltre alle riserve di carattere costituzionale, anche la riconduzione dell'attività in questione all'acquisizione della prova documentale lascia perplessi. Infatti, se è vero che l'art. 234 c.p.p., per il richiamo in esso contenuto a «qualsiasi altro mezzo», è una norma a struttura aperta, idonea a ricomprendere anche i documenti informatici[56], bisogna fare attenzione a non confondere il contenuto con il contenitore: i dati digitali non sono prove documentali e non seguono le regole di ammissione per questi dettate dagli artt. 495, co. 3 e 515 c.p.p., valgono per essi, in considerazione della loro natura volatile e modificabile, regole di raccolta e utilizzo dibattimentale diverse.

Ad ogni modo, anche a voler ammettere l'applicabilità dell'art. 234 c.p.p., tale norma non può che riferirsi a documenti, ancorché informatici, preesistenti al provvedimento acquisitivo stesso e non a quelli costituendi. Ora, è ben vero che il decreto del pubblico ministero prevedeva l'acquisizione dei *files* memorizzati sul *computer*, ma è altresì vero che tale generica formula, unitamente al fatto che il monitoraggio si è protratto per otto mesi, fanno ritenere del tutto verosimile l'apprensione di documenti formati dopo il provvedimento *de quo*.

Per quanto riguarda invece la vicenda *Ryanair*, molto opportunamente la Cassazione ha confermato l'annullamento da parte del Tribunale del riesame del decreto di perquisizione e sequestro. Infatti, la Suprema Corte ravvisa in simile provvedimento un inammissibile strumento a carattere esplorativo, «*che mirava non tanto ad acquisire elementi di conoscenza in ordine ad una o più* notitiae criminis *determinate, quanto a monitorare in modo illimitato, preventivo e permanente il contenuto di un sistema informatico onde pervenire per suo tramite all'accertamento di reati non ancora commessi, ma dei quali si ipotizzava la futura commissione da parte di soggetti ancora da individuarsi*». Pertanto, conclude la Corte, «*è da escludere un preventivo ed indefinito monitoraggio del sistema predetto in attesa dell'eventuale e futura comparsa del dato da acquisire a base delle indagini: si verrebbe altrimenti ad integrare un nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative, di mera investigazione (paragonabile alle intercettazioni), che nulla ha a che fare con la perquisizione*». Con ciò si coglie uno tra i tanti aspetti problematici del monitoraggio di un sistema informatico realizzato attraverso specifici *softwares* di indagine, ossia l'alto rischio che esso si trasformi in un mezzo di ricerca di notizie di reato. Ne è evidente quindi l'eterogeneità e non riconducibilità alla disciplina delle perquisizioni, che trovano il loro naturale campo di applicazione nella ricerca di prove relative ad una preesistente *notitia criminis*.

[56] In tal senso, F. Cordero, sub *art. 234*, in *Codice di procedura penale commentato*, 2ª ed., Torino, 1992.

6. (segue) Prova atipica o prova incostituzionale?

Con il termine perquisizioni *online* si fa riferimento ad un'attività di indagine che assomma le caratteristiche e le funzioni di diversi mezzi di ricerca della prova tipici, pur non essendo riconducibile ad alcuno di essi, e che presenta altresì caratteri di originalità. Esse infatti non sono riconducibili né alla disciplina delle perquisizioni, né a quella delle ispezioni, né infine a quella delle intercettazioni, configurando piuttosto un *tertium genus*.

Anche dopo le modifiche introdotte con la legge di ratifica della Convenzione *Cybercrime*, l'art. 247 c.p.p. non pare applicabile a questo innovativo strumento di indagine. Tale norma, infatti, si limita a rendere possibili le tradizionali perquisizioni, volte alla ricerca del corpo del reato o di cose pertinenti al reato anche in ambiente informatico, autorizzando la perquisizione di sistemi informatici o telematici «quando vi è motivo di ritenere che ivi si trovino dati, informazioni, programmi informatici o tracce comunque pertinenti al reato». Ma la relativa disciplina rimane quella classica di uno strumento di indagine a sorpresa, ma "palese", e che non può essere condotto a distanza[57].

Ma nemmeno pare potersi applicare la norma relativa alle ispezioni informatiche, novellata nel 2008. Infatti, esse servono a fotografare la realtà esistente, senza alcuna apprensione di dati[58].

Il carattere segreto della perquisizione *online* potrebbe allora indurre a ritenere tale attività assimilabile a quella di intercettazione informatica o telematica (art. 266 *bis* c.p.p.). Tale disciplina è *prima facie* sicuramente più adatta a soddisfare le esigenze di tutela della riservatezza del destinatario della perquisizione *online*. Essa prevede innanzitutto una delimitazione dei reati per la repressione dei quali tale strumento può essere utilizzato e rigidi presupposti di applicazione (gravi indizi di reato e indispensabilità dell'intercettazione ai fini della prosecuzione delle indagini). Inoltre, contempla una serie di disposizioni poste a vario titolo a tutela del destinatario della misura: da quelle che dispongono in merito al quando e al come questi è ammesso a conoscere prima dell'esistenza dell'intercettazione e poi del suo contenuto, a quelle che prevedono divieti di utilizzazione e conseguenti obblighi di distruzione dei risultati di intercettazioni eseguite in violazione delle disposizioni di legge. Tuttavia, le intercettazioni hanno ad oggetto l'apprensione occulta e in tempo reale di *comunicazioni*, laddove con riferimento alle intercettazioni informatiche per comunicazioni si intende non qualsiasi comunicazione intercorrente tra sistemi informatici, ma solo lo scambio di dati digitali determinato da un'attività umana, ossia un'attività di comunicazione o di altro genere riconducibile ad una persona[59]. Ne deriva che lo strumento in esame può essere utilizzato per l'apprensione di messaggi scritti come le *e-mail*, di conversazioni via *chat*, ovvero per la captazione di collegamenti con siti *web*.

Tuttavia, come si è già sottolineato, ciò non esaurisce il novero delle attività che possono essere compiute attraverso questo specifico *software* d'indagine.

Il fatto che le perquisizioni *online* non siano riconducibili ad alcuno dei mezzi di ricerca della prova specificamente disciplinati dal codice di rito non significa che si possa automaticamente concludere nel senso della loro ammissibilità alle condizioni stabilite dall'art. 189 c.p.p. quale prova atipica. Infatti, il primo presupposto di validità di una prova atipica è la sua legittimità costituzionale.

Occorre quindi verificare quali diritti fondamentali siano coinvolti in tale attività di indagine, al fine di delineare i presupposti e i confini entro cui iscrivere tale mezzo di ricerca della

[57] Stabilisce l'art. 250 c.p.p. che «nell'atto di iniziare le operazioni copia del decreto di perquisizione locale è consegnata all'imputato, se presente, e a chi abbia l'attuale disponibilità del luogo, con l'avviso della facoltà di farsi rappresentare o assistere da persona di fiducia purché questa sia prontamente reperibile e idonea». Inoltre, in base al disposto dell'art. 365 c.p.p., il destinatario della perquisizione viene invitato a nominare un difensore di fiducia – se ne è privo gliene viene assegnato uno d'ufficio – il quale ha diritto a partecipare al compimento dell'atto, pur senza preavviso. Tali disposizioni sono inapplicabili alle c.d. perquisizioni *online* che vengono condotte all'insaputa dell'interessato.

[58] S. Marcolini, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, p. 2855 ss. Così già, R. Flor, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht, cit., p. 695 ss.

[59] Infatti, le intercettazioni informatiche rientrano nel più ampio *genus* delle intercettazioni di comunicazioni, la cui essenza è ravvisata dalla giurisprudenza «*nella captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo, attuata da soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato*». Cfr. Cass., sez. un., 24 settembre 2003, n. 36747, Torcasio, in *Cass. pen.*, 2004, p. 21. Si veda anche G. Di Paolo, (voce) *Prova informatica (diritto processuale penale)*, in *Enc. dir.*, Annali VI, Milano, 2013, p. 736 ss.

prova.

Viene innanzitutto in rilievo il diritto alla libertà e segretezza delle comunicazioni (art. 15 Cost.) che, tuttavia, estende il suo ambito di tutela alle sole comunicazioni che avvengano tramite il *computer* (conversazioni *VoIP*, *e-mail*, *chat*), nonché sulla base della giurisprudenza della Corte costituzionale in materia di tabulati telefonici, anche ai dati esterni di tali comunicazioni, ossia ai dati di traffico telematico.

Quanto all'art. 14 Cost., se per domicilio si intende «uno spazio isolato dall'ambiente esterno, adibito allo svolgimento di atti della vita privata e dal quale il soggetto o i soggetti titolari abbiano inteso normalmente escludere la presenza di terzi»[60], difficilmente può negarsi la sua operatività nella fase di intromissione nel sistema informatico[61]. Infatti, in considerazione dell'importanza essenziale nella vita di tutti i giorni che il *computer* è venuto assumendo, al punto che la Corte costituzionale tedesca lo ha considerato uno strumento attraverso cui l'individuo sviluppa liberamente la propria personalità, esso può considerarsi un "domicilio informatico", soprattutto quando sia protetto da *password*.

L'analisi non si può tuttavia arrestare a questa prima e più immediata interpretazione estensiva della tutela del domicilio tradizionale. Come si è visto nella prima parte del presente lavoro, il sistema informatico viene in rilievo quale perimetro ideale di una serie di informazioni che si vogliono sottrarre alla conoscenza altrui. Oggetto di protezione è quindi lo spazio informatico o virtuale, cui queste ultime sono affidate. In quest'ottica, la tutela del domicilio si rivela inadeguata: pur tutelando «la persona riflessa in una certa sfera spaziale volta a preservare il carattere intimo, domestico, o quanto meno privato di determinati comportamenti soggettivi», essa rimane pur sempre legata ad un ambiente fisico, all'interno del quale si svolge la vita privata. A venire in rilievo è piuttosto l'esigenza di riservatezza, *sub specie* di riservatezza informatica, dell'utilizzatore di un sistema informatico.

Se si accoglie l'idea che tale diritto fondamentale è tutelato dagli artt. 2, 117, comma 1 Cost., 8 CEDU e 7 CDFUE, eventuali limitazioni dello stesso ad opera della pubblica autorità potranno avvenire solo se rispettose delle prescrizioni di cui agli articoli 8, comma 2 CEDU e 52, comma 1 CDFUE. Esse dovranno quindi essere previste dalla legge, perseguire uno scopo legittimo e rispettare il principio di proporzionalità, fatta salva l'intangibilità del nucleo essenziale di tale diritto fondamentale.

Attualmente, pertanto, nell'assenza di una specifica disciplina legislativa, le c.d. perquisizioni *online* darebbero vita ad una prova inutilizzabile in quanto incostituzionale (o inammissibile se si accoglie l'idea, fatta propria dalla Cassazione nella sentenza Prisco[62], che l'art. 189 c.p.p. presuppone la formazione lecita della prova e che quindi nel caso delle attività atipiche il vaglio di ammissibilità è attività preliminare e precede quello di inutilizzabilità)[63].

7. Conclusioni: quale disciplina?

L'affermare che le c.d. perquisizioni *online* sono attualmente un prova incostituzionale non rappresenta una conclusione, ma un punto di partenza. Infatti, l'obiettivo non è quello di negare cittadinanza a tale strumento nel nostro ordinamento, ma di stabilire a quali condizioni sia da considerarsi legittimo, tenuto conto dell'importanza che lo stesso va acquisendo ai fini di indagine e della crescente attenzione che a livello europeo e internazionale viene dedicata al tema.

È quindi compito del legislatore intervenire, dettando una disciplina *ad hoc*, che raggiunga

[60] Così, G. Borrelli, *Riprese filmate nel bagno di un pubblico esercizio e garanzie costituzionali*, in Cass. pen., 2001, p. 2453ss.

[61] Come precisato anche dalla Corte costituzionale nella sentenza 24 aprile 2002, n. 135, in *Giur. cost.*, 2002, p. 1062 ss., con osservazioni di F. Caprioli, *Riprese visive nel domicilio e intercettazioni «per immagini»*, l'elenco dei mezzi di ricerca della prova attraverso cui la pubblica autorità può interferire nella libertà domiciliare non è tassativo. Argomenti in tal senso non si possono desumere nemmeno dall'art. 8 CEDU o dagli artt. 7 e 52 CDFUE. Inoltre, l'art. 14 Cost. «*nell'ammettere intrusioni nel domicilio per finalità di giustizia non prende posizione sul carattere palese o occulto delle intrusioni stesse. La configurazione di queste, e in particolare delle ispezioni, come atto palese*», prosegue la Corte, «*emerge esclusivamente a livello di legislazione ordinaria*».

[62] Cass., sez. un., 28 marzo 2006, Prisco, cit.

[63] In tal senso già S. Marcolini, *Le cosiddette perquisizioni*, cit., p. 2861, secondo il quale se le perquisizioni *online* «fossero effettuate in un procedimento penale italiano, [esse] dovrebbero essere dichiarate inammissibili come prova perché, non previste dalla legge, verrebbero ad incidere su di un bene giuridico – la riservatezza della vita privata – la cui lesione, alla luce del nuovo combinato costituzionale-sovranazionale […] esige la previa determinazione, da parte del legislatore ordinario, dei casi e dei modi di aggressione di quel bene».

un equo bilanciamento, alla luce del principio di proporzionalità, tra diritti costituzionalmente protetti: quello alla riservatezza informatica da un lato e quello alla repressione dei reati dall'altro. Disciplina che dovrà innanzitutto individuare i casi e modi dell'intromissione in un sistema informatico: elenco di gravi reati presupposto[64], provvedimento motivato dell'autorità giudiziaria – del giudice su richiesta del pubblico ministero – modalità dell'intromissione e di svolgimento dell'attività di indagine. Dovranno in particolare essere introdotte specifiche garanzie a tutela dei dati personali irrilevanti per le indagini, e apposite sanzioni di inutilizzabilità del materiale probatorio acquisito illegittimamente o irrilevante. Inoltre, è opportuno stabilire se il ricorso a tale strumento sia consentito anche per finalità preventive.

Occorre infine considerare un ultimo, importantissimo aspetto, quello della formazione degli operatori che in concreto si troveranno a svolgere questo tipo di attività di indagine. La scarsa comprensione o la sottovalutazione delle potenzialità delle innovazioni tecnologiche può infatti tradursi in minori garanzie per chi è sottoposto a procedimento penale.

[64] Quanto all'individuazione di tali gravi forme di criminalità, anche in considerazione del possibile utilizzo di codesto strumento d'indagine nell'ambito di indagini a carattere transnazionale, si può senz'altro fare riferimento a quanto stabilisce l'art. 83 TFUE con riferimento all'ambito di intervento dell'Unione nel settore del diritto penale sostanziale, ossia: «terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata». La stessa Corte di Giustizia nella sentenza sulla c.d. *data retention* ha individuato nella lotta contro gravi forme di criminalità, tra cui il terrorismo e la criminalità organizzata, un obiettivo di carattere generale che può essere realizzato attraverso l'uso di strumenti di indagine ad alto contenuto tecnologico, purché nel rispetto dei diritti fondamentali riconosciuti dalla Carta (8 aprile 2014, C-293/12, C-594/15, *Digital Rights Ireland Ltd.*, cit., par. 51).