GIUSEPPE CORASANITI

PROVE DIGITALI E INTERVENTI GIUDIZIARI SULLA RETE NEL PERCORSO DELLA GIURISPRUDENZA DI LEGITTIMITÀ

SOMMARIO: 1. Un percorso uniforme, una rete multiforme. — 2. Misure cautelari reali aventi ad oggetto computers e server ed identificazione degli utenti on line. — 3. Nuove forme di condotte criminose, nuove condotte criminose.

1. Un percorso uniforme, una rete multiforme.

Può sembrare operazione apparentemente semplice ricostruire il percorso della giurisprudenza penale della Corte di Cassazione in materia di reti informatiche che si muove quasi in parallelo alla vicenda normativa, segnata dalla L. n. 547 del 1993[1] e conclusasi nel 2008, con la L. 18 marzo 2008, n. 48 « *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno* » che detta una nuova disciplina della prova digitale[2], intervenendo in più punti sulla disciplina sostanziale e processuale e definendo espressamente gli ambiti di intervento giudiziario proprio nella acquisizione dei dati di accesso e di intervento sui sistemi informatici.

In realtà dietro alla elaborazione di principi giurisprudenziali traspare una certa sensibilità ai temi posti insistentemente dalla

* Il testo riproduce la relazione al Convegno « Il diritto penale della rete » tenutosi l'8 aprile 2011 presso la Suprema Corte di Cassazione.

[1] Su cui cfr. Borruso R., Buonomo G., Corasaniti G., D'Aietti G., *Profili penali dell'informatica*, Milano 1994.

[2] Sui cui contenuti sia consentito il rinvio a G. Corasaniti, e G. Corrias Lucente, *Cybercrime, responsabilità degli enti, prova digitale, Commento alla legge 18 marzo 2008 n. 48*, Padova 2009; Novario F., *Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla L. 18 marzo 2008, n. 48 al codice di procedura penale*, in *Riv. Dir. processuale*, 2008, p. 1069; G. Morgante, S. Tovani, Degl'Innocenti L., Corbì L., Da Valle G., Manzione D., L. 18 marzo 2008 n. 48 - *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*, in *La legislazione penale*, 2008, p. 251; Luparia L., *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48)*, Milano 2009.

dottrina in tema di tecniche acquisitive e di valutazione della relativa congruità dal punto di vista tecnologico, secondo standards di «*forensic*»[3] volti non solo a garantire la inalterabilità delle tracce acquisibili o acquisite ma a tradurre in concreto la nuova disciplina della prova digitale entro un ambito quanto mai vasto e di incerta definizione, caratterizzato dalla «volatilità» delle memorie e dall'uso di supporti in continua evoluzione tecnologica, sia sotto il profilo quantitativo che qualitativo.

Una prima osservazione di massima porta allora a sottolineare come l'individuazione delle essenziali problematiche di *ripetibilità/irripetibilità* dell'esame dei dati e delle informazioni contenuti e acquisibili nel sistema interessato, della legittimità dell'azione giudiziaria in un contesto assai complesso sia intervenuta gradualmente, forse talora in modo prudente e talora senza una puntuale definizione del contesto tecnologico di riferimento. Così sembrano collocarsi ancora sullo sfondo i temi essenziali nel rapporto problematico tra diritto penale e tecnologie informatiche e dei limiti delle attività acquisitive poste in essere dalla Polizia giudiziaria e dal Pubblico Ministero e sembrano gradualmente elaborate e quindi poste precisamente alcune linee interpretative molto importanti in tema di sequestri sia a carattere probatorio che preventivo.

L'incertezza definitoria, che talora sembra trasparire dalle pronunce giurisprudenziali, risente in un certo qual senso anche della incertezza generale che caratterizza questioni e casistiche assai varie (rispetto alla quale la predetta Convenzione internazionale in tema di crimini informatici e, non si dimentichi, di acquisizione generale delle prove digitali non è che solo l'avvio di un parallelo percorso normativo penale di tipo transnazionale). Eppure, come si vedrà, proprio tali tematiche, appaiono centrali e qualificanti con riferimenti talora molto sfumati, talora indiretti, ma sempre corrispondenti a principi ormai visibili ed articolati.

La Corte sembra in un primo momento concentrarsi solo sugli aspetti «formali» di regolamentazione delle responsabilità dei processi comunicativi (in una prima fase che copre il decennio 1995/2005) per intervenire poi più decisamente negli ultimi cinque anni proprio sugli aspetti sostanziali, definendo meglio gli ambiti e le responsabilità degli interventi processuali e chiarendo il fondamento delle condotte incriminatrici in un contesto tecnologico certo multiforme e continuamente in evoluzione.

Va infatti precisato che il riferimento alla «*rete*» in senso generalizzato rischia anche di apparire insieme semplificativo e fuor-

[3] Cfr. CHIRIZZI L., *Computer forensics: brevi cenni tecnici e procedurali sulla ricerca della fonte di prova informatica*, in *Ciberspazio e diritto*, 2006, p. 463. Cfr. da ultimo LUPARIA L., *Computer crimes e procedimento penale*, in *Trattato di Procedura Penale*, vol. VII, Torino 2001, p. 370 e ss.

viante, poiché la compresenza di azione, informazione ed automazione in tutte le condotte criminose di carattere informatico rende insieme facile un metodo in un certo senso « assimilativo » a condotte preesistenti, proiettandone i medesimi meccanismi di imputazione e di responsabilità sotto il profilo penale. Altrettanto complessa appare perciò l'operazione interpretativa che, sul piano della legittimità, rischia continuamente di produrre effetti incoerenti sul piano definitorio, rendendo sempre più problematica l'operazione ricostruttiva di linee omogenee, tanto più se riferibili a tematiche differenti e solo apparentemente non comparabili.

Così appare difficoltoso ricondurre ad un concetto unitario sul piano interpretativo condotte e tipologie di attività tecnologicamente molto differenti e diversificate, sia dal punto di vista organizzativo che sociale prima ed economico poi. Individuare allora la « *Net economy* » e la « *Net society* » significa riferirsi solo ad un approccio di regolamentazione a carattere promozionale che, sul piano penale, appare non strettamente corrispondente alle rassicuranti categorie e metodologie di condotte e di tecniche di accertamento fino ad oggi articolate[4].

In alcuni casi sarà forse più semplice ragionare in tema di individuazione e protezione di beni giuridici e quindi di allargamento di condotte criminose già esistenti, ma in altrettanti casi tale attività interpretativa appare non priva di rischi, ampliando sul piano analogico la portata delle norme di riferimento anziché contestualizzando le condotte nell'ambito di una regolamentazione internazionale che, sia pure *in itinere*, si rivela integrativa ed essenziale per cogliere sempre quello che è un percorso evolutivo del sistema internazionale e che non può trasformarsi in percorso involutivo dell'ordinamento nazionale.

Un concetto « unitario » di rete è quindi frutto dell'apparenza piuttosto che dell'analisi accurata della realtà tecnologica, frutto del bisogno di una parametrazione certa a categorie già esistenti piuttosto che dello sforzo ricostruttivo di individuazione di priorità di garanzie entro uno scenario in evoluzione continua e di mutevole connotazione nel quale convivono aspetti di informazione individuale, esigenze di comunicazione e partecipazione collettiva e sociale, modalità differenti di espressione di contenuti comunicativi (portali, *siti*, *blog*, *post*, *chat*, *mail*, *bacheche* sia in forma testuale che in forma multimediale) oggi più che mai caratterizzabili in termini di condivisione, e quindi con responsabilità non solo non facilmente sempre immediatamente riconoscibili, ma addirittura anche formalmente diversificabili e diversificate[5].

[4] SIEBER U. (ed.), *Information Technology Crime. National Legislation and International Initiatives*, Köln-Berlin, 1994.

[5] MARTELLO S., *Sulla Partecipazione e sulla Comunicazione nella Rete: riflessioni operative e giuridiche*, in *Ciberspazio e diritto*, 2009, p. 25.

Neppure il tradizionale riferimento alla regolamentazione europea, e ci si riferisce alla categoria del « fornitore » di servizi e di contenuti on line (*provider*)[6] oggi in un certo senso, nel web 2.0 appare oggi così certo e qualificante, e difatti molto incerte appaiono le prospettive giurisprudenziali in assenza di principi « sensibili » progressivamente alla « *Net neutrality* »[7], cioè in buona sostanza alla valutazione della rete come infrastruttura (complessa) di comunicazione neutra e diversificata, in grado di fornire, su iniziativa dell'utente, contenuti di ogni genere enucleabili organizzabili ed organizzati secondo modalità molto diversificate e sempre più spesso con una ripartizione di funzioni organizzative in ambito transnazionale.

E nello scenario di fondo appaiono già ora questioni ancora più complesse quali il c.d. « *Cloud* » computer[8], l'universo in espansione dei « *social networks* »[9] (come *Facebook*, equivalente alla quarta nazione del Pianeta quanto a soggetti coinvolti) ma con prospettive di mutevolezza e di cambiamento continue ed in grado di suscitare movimenti di opinione come e forse più dei mezzi di comunicazione tradizionali in un ambito interpersonale diretto.

[6] De Natale D., *La responsabilità dei fornitori di informazioni in internet per i casi di diffamazione on line*, in *Riv. Trimestrale di diritto penale dell'economia*, 2009, p. 509.

[7] Il concetto di « *Net neutrality* » si basa sull'idea di precludere all'operatore di rete in funzione di garanzie sia economiche che tecnologiche quei comportamenti discriminatori o anticompetitivi relativamente a pacchetti IP associati a specifici servizi, applicazioni, origini, destinazioni o devices. La *Network Neutrality* è quindi solitamente associata ai concetti di non discriminazione e di prevenzione di abusi (tecnologici, destinati a ripercuotersi sul mercato) di posizione dominante sul mercato delle comunicazioni interattive e delle applicazioni, più in generale. Un concetto economico e tecnologico al quale, oggi, non corrisponde una precisa qualificazione delle responsabilità giuridiche, che sul terreno penale appaiono quanto mai complesse.

[8] Il c.d. *Cloud Computing* è un insieme di tecnologie che consentono l'accesso a risorse (CPU, reti, server, *storage*, applicazioni e servizi) in modo configurabile e « a misura » per l'utilizzo richiesto. Non esiste più « un server » come tradizionalmente lo si intende, ovvero una singola macchina, eventualmente protetta contro eventuali perdite d'informazioni e situata in una località ben definita ove le informazioni e i dati sono custoditi. Esiste, invece, un gruppo distribuito di server interconnessi (« la nuvola »), una disseminazione operativa di infrastrutture interagenti che gestiscono servizi, eseguono applicazioni ed archiviano documenti in modo totalmente trasparente all'utilizzatore. Con tale sistema le aziende (specie quelle più grandi) hanno la possibilità di ottenere grandi risparmi sui costi dovuti all'acquisto ed alla gestione di macchine ed infrastrutture e gli utenti possono fruire di sistemi molto complessi anche con risorse infrastrutturali minime. Quasi tutti « social networks » e le applicazioni di posta da remoto corrispondono oggi a tale architettura.

[9] Il termine, oggi ormai di uso comune, è in realtà corrispondente a due significati distinti: da una parte esso non è che la traduzione del termine « rete sociale » cioè un insieme di individui collegati spontaneamente tra loro da un particolare tipo di relazione (familiare, di lavoro, di interesse, di consumo), che condividono sul *web* sistematicamente interessi e che sono interessati a collaborare e a mettere in comune idee e informazioni. Dall'altra viene ad essere utilizzato per indicare i siti, o meglio le categorie dei siti, che rendono possibile la creazione e la organizzazione di una rete sociale virtuale, ovvero che semplificano, attraverso una serie di applicazioni e di funzioni di ricerca, la nascita e il mantenimento di *contatti e legami individuali* o l'aggregazione di temi potenzialmente di interesse collettivo.

L'impatto di tali nuovi temi e dei nuovi protagonisti della fase avanzata del *web* (il c.d. « *web* 2.0 ») è tale da coinvolgere insieme e direttamente, ed in qualche modo da sconvolgere, il tradizionale ambito applicativo del diritto penale in termini di valutazione degli elementi soggettivi ed oggettivi del reato, ma è di tale intensità da far riconsiderare circostanze e contesti, da imporre una revisione critica dello stesso concetto di « evento » che sul piano telematico viene a corrispondere ad una così ampia categoria di fatti umani e di ipotesi di reato corrispondenti da poter costituire un insieme omogeneo di figure criminose, sempre più qualificabili entro un livello definitorio di tipo internazionale, che ne descrive i tratti in termini di danno o di pericolo e ne prefigura, sia pure in modo molto ampio, le connotazioni essenziali.

Non si tratta solo di fare o meno professione di fede nelle tecnologie in espansione e nella loro implicita capacità di autoregolarsi, si tratta invece di cogliere sempre, in ogni fattispecie di rilievo penale ed in ogni accertamento processuale che la accompagna modi e forme di equilibrio e di coerenza rispetto ai beni giuridici di rilievo costituzionale che proprio nelle tecnologie innovative trovano occasione di rafforzarsi e di essere posti in discussione e addirittura di essere messi a rischio.

Ed è solo all'attenta interpretazione del giudice penale e alla sua capacità di coerente analisi tecnologica e di sensibilità sociale[10] che viene affidato il ruolo di definire limiti e confini di un'azione tecnologicamente vasta, complessa, multiforme e mutevole nella quale concorrono soggetti diversi e che si muove su spazi diversi, ma che ogni giorno di più caratterizza la nostra vita.

2. Misure cautelari reali aventi ad oggetto computers e server ed identificazione degli utenti on line.

Le prime posizioni della S.C. muovono dalla esigenza di piena acquisizione della prova informatica anche qualora la condotta del reato si sia, almeno parzialmente, concretizzata fuori dal territorio italiano.

In un primo momento si profila l'esigenza di acquisire la struttura coinvolta nella sua integrità senza prosi alcun problema relativamente alla destinazione concreta dell'« oggetto » informatico. Sul piano generale, in tema di sequestro probatorio di cose costituenti corpo di reato, osserva la S.C. non è necessario offrire la dimostrazione puntuale della necessità del sequestro in funzione dell'accertamento dei fatti, atteso che l'esigenza probatoria del

[10] Cfr. a riguardo Picotti L., *Il diritto penale dell'informatica nell'epoca di Internet*, Padova 2004; Sarzana di S. Ippolito C., *Informatica, internet, diritto penale*, Milano, 2003.

« *corpus delicti* » è « *in re ipsa* », onde il decreto di sequestro è sempre legittimo quando abbia ad oggetto cose qualificabili come corpo di reato, essendo necessario e sufficiente, a tal fine, che risulti giustificata detta qualificazione.

La fattispecie riguardava proprio il sequestro di un « *computer* », che, secondo la prospettazione accusatoria, viene a costituire essenzialmente un mezzo di raccolta di documentazione[11], indipendentemente dalla valutazione di pertinenzialità effettiva tra contenuti formali dell'imputazione e dati oggetto della ricerca estrattiva, funzionali al positivo riscontro della fondatezza della medesima.

Più complessa appare la valutazione del rapporto tra misura cautelare informatica e disponibilità dell'oggetto della cautela nel quadro di una attività professionale, ponendosi progressivamente in luce l'esigenza di una acquisizione probatoria sensibile ed adeguata[12]. Sembra emergere con decisione allora un principio di « proporzionalità » della misura del sequestro probatorio[13], principio tanto più persistente quanto più in relazione con la concreta destinazione dei sistemi informatici e delle memorie interessate.

[11] Legittimo, quindi, è il sequestro di documentazione integrale dei corrispettivi e delle operazioni alberghiere che l'imprenditore doveva per legge effettuare e sul quale era stata operata una cancellazione della memorizzazione di tali dati al fine di evasione fiscale (Sez. 6, Sentenza n. 337 del 29 gennaio 1998). È legittimo il sequestro probatorio di un *intero server* informatico (peraltro completamente sigillato) presso lo studio di un avvocato indagato di concorso in bancarotta fraudolenta, al fine di verificare, con le garanzie del contraddittorio anticipato, la natura effettivamente pertinenziale rispetto al reato ipotizzato di atti e documenti sequestrati, così escludendo indebite conseguenze sulle garanzie del difensore in violazione dell'art. 103 c.p.p. Nella fattispecie la Corte ha ritenuto che il sequestro era funzionale alla selezione dei dati informatici pertinenti attraverso l'incombente processuale della perizia da espletarsi con incidente probatorio (Sez. 5, Sentenza n. 2816 del 19 marzo 2002).

[12] Il sequestro probatorio della memoria del « personal computer » di un giornalista che abbia opposto il segreto professionale è consentito soltanto ove sia ritenuta l'infondatezza del segreto e la necessità dell'acquisizione per l'indagine, ma l'attività investigativa deve essere condotta in modo da non compromettere il diritto del giornalista alla riservatezza della corrispondenza e delle proprie fonti (Sez. 1, Sentenza n. 25755 del 16 febbraio 2007). Sul tema cfr. TROISI P., *Sequestro probatorio del computer e segreto giornalistico*, in *Diritto penale e processo*, 2008, p. 765; NUZZOLESE V., *In tema di sequestro di computer ai giornalisti*, in *Diritto penale e processo*, 2009, p. 369; GABRIELLI C., *Quando il sequestro probatorio ha per oggetto l'hard-disk del computer di un giornalista*, in *Giur. It.*, 2008, p. 731; MACRILLÒ A., *Segreto* ex *art. 200 c.p.p. e sequestro del computer in uso al giornalista*, in *Diritto penale e processo*, 2008, p. 1416; LOGLI A., *Sequestro probatorio di un personal computer. Misure ad explorandum e tutela della corrispondenza elettronica*, in *Cass. Pen.*, 2008, p. 2946.

[13] Ed ancora sempre in tema di sequestro probatorio disposto nei confronti di un giornalista professionista si è ritenuto che debba rispettare con particolare rigore il *criterio di proporzionalità* tra il contenuto del provvedimento ablativo di cui egli è destinatario e le esigenze di accertamento dei fatti oggetto delle indagini, evitando quanto più è possibile indiscriminati interventi invasivi nella sua sfera professionale. In tal caso è stato ritenuto illegittimo il sequestro del computer in uso ad una giornalista e dell'area del « server » dalla stessa gestita, con la conseguente acquisizione dell'intero contenuto dell'« hard disk » e di un'intera cartella personale presente nell'area del sistema operativo (Sez. 6, Sentenza n. 40380 del 31 maggio 2007).

Nella predefinizione degli « oggetti » informatici da ricercare sembra emergere una valutazione elastica, attenta alla contestualizzazione del provvedimento cautelare ed alle esigenze di immediata percezione di dati la cui puntuale ricostruzione deve necessariamente formare oggetto di accertamento successivo[14].

Le pronunce riguardanti il giudizio di riesame in tema di sequestri di materiale informatico offrono altresì lo specchio di una situazione complessa che vede insieme emergere con evidenza il contrastato rapporto tra prove digitali ed accertamenti e rilievi ad opera della polizia giudiziaria e della magistratura inquirente.

Il giudice del riesame di un sequestro probatorio deve (sempre) accertare l'esistenza del vincolo *di pertinenzialità tra il reato ipotizzato ed i diversi beni o le diverse categorie di beni oggetto del provvedimento* di sequestro. In tal caso è stato ritenuto illegittimo il sequestro di un intero « server » aziendale disposto in relazione al reato di turbata libertà dell'industria o del commercio (Sez. 3, Sentenza n. 12107 del 18 novembre 2008). Anche in questo caso il principio di proporzionalità trova un suo riconoscimento diretto ed espresso. Più articolata appare invece la ricostruzione dei limiti del giudizio di riesame in sede di sequestro di sistemi informatici, apparendo una ricostruzione delle informazioni e dei dati contenuti essenziale tanto alla dimostrazione dell'ipotesi accusatoria quanto al ristoro sostanziale della intervenuta indisponibilità informativa da parte dell'indagato[15]. Ne consegue che la copia dei

[14] È stato infine sempre ritenuto utilizzabile, in relazione al delitto di detenzione di materiale pedopornografico, il sequestro probatorio del computer contenente tale materiale, pur se effettuato a seguito di autorizzazione di perquisizione in relazione a diversa fattispecie criminosa trattandosi di atto dovuto espletato dalla polizia giudiziaria nell'ambito dei propri poteri e riguardando bene comunque pertinente al reato di detenzione (Sez. 3, Sentenza n. 19887 del 18 marzo 2009). Il principio è confermato in una pronuncia più recente che ha ribadito che il sequestro del personal computer in caso di accertamenti in tema di porno pedofilia minorile costituisce atto dovuto (Sez. 3, Sentenza n. 45571 del 24 novembre 2010). Non è soggetto a convalida il sequestro operato dalla polizia giudiziaria in esecuzione di un decreto di perquisizione del P.M., nel caso in cui l'oggetto del sequestro non sia rimesso alla valutazione discrezionale della P.G. ma risulti indicato con certezza dal pubblico ministero (« files aventi contenuto pedopornografico inseriti in personal computer o in qualsiasi altro supporto ») (Sez. 3, Sentenza n. 12390 del 2 marzo 2010).

[15] È inammissibile, per carenza di interesse, la richiesta di riesame di sequestro probatorio volta ad ottenere non già la restituzione del bene sequestrato, bensì una pronuncia sulla legittimità od utilizzabilità della prova acquisita essendo tale ultima valutazione riservata al solo giudice del processo ed essendo di contro la procedura di riesame destinata unicamente ad eliminare le conseguenze pregiudizievoli per la parte derivanti dal vincolo d'indisponibilità del bene. In applicazione di tale principio la Corte ha dichiarato inammissibile la richiesta di riesame avverso il sequestro di documentazione custodita nei computer in uso agli indagati ed eseguito mediante la sola estrazione di copia degli « hard disks » e, conseguentemente, senza l'asportazione di alcun bene materiale (Sez. 2, Sentenza n. 24958 del 14 giugno 2007). Una volta restituita la cosa sequestrata, la richiesta di riesame del sequestro, o l'eventuale ricorso per cassazione contro la decisione del tribunale del riesame è inammissibile per sopravvenuta carenza di interesse, che non è configurabile neanche qualora l'autorità giudiziaria disponga, all'atto della restituzione, l'estrazione di copia degli atti o do-

dati secondo procedure e *standards* ben definiti finisce per soddisfare entrambe le esigenze apparentemente contrapposte fino a porsi in concreto quale metodologia uniforme sia per assicurare un contenuto informativo dimostrativo dell'azione pregressa svolta dall'indagato e dei suoi intervenuti contatti con l'esterno, sia, potenzialmente, per assicurare l'esigenza ricostruttiva opposta che tenderà alla giustificazione dei contenuti esistenti ovvero alla contestazione della relativa imputabilità effettiva al soggetto perquisito.

Ampio e diversificato appare l'intervento giurisprudenziale in tema di sequestro preventivo, dominato ed in un certo senso pervaso, dalla tematica della natura essenzialmente informativa della rete e quindi dell'esigenza di individuare un punto di equilibrio tra misura cautelare inibitoria e libera espressione di idee e opinioni che, proprio attraverso la rete viene a estrinsecarsi. Sicché, pur nella giustificabile ammissione della possibilità di sequestro preventivo quale mezzo per impedire la prosecuzione della condotta criminosa in essere attraverso una attività comunicativa organizzata[16], si pone poi il problema, sempre più avvertito socialmente della proporzionalità della misura e della sua coerenza rispetto al panorama tecnologico, tanto più in rapporto a valori controversi o religiosi[17], e finalmente rivolto alla

cumenti sequestrati sul computer, dal momento che il relativo provvedimento è autonomo rispetto al decreto di sequestro, né è soggetto ad alcuna forma di gravame, stante il principio di tassatività delle impugnazioni (Sez. U, Sentenza n. 18253 del 24 aprile 2008). La restituzione da parte del P.M. della cosa sequestrata, previa estrazione di atti o di documenti in esecuzione di decisione del Tribunale del Riesame di annullamento del sequestro probatorio, non rende inammissibile per sopravvenuta carenza di interesse il ricorso per cassazione proposto dallo stesso P.M., qualora il ripristino del vincolo consentirebbe l'espletamento di indagini non effettuabili su semplici copie. In tal caso erano stati estratti dati informatici dal computer sequestrato prima della sua restituzione (Sez. 6, Sentenza n. 26699 del 26 giugno 2009).

[16] In tema di sequestro di giornali e altre pubblicazioni, è legittimo il sequestro preventivo di messaggi ed annunci di contenuto osceno pubblicati su siti internet in quanto gli stessi sono equiparabili alle pubblicazioni a stampa, costituzionalmente vietate in caso di contrarietà al buon costume. (In motivazione la Corte, nell'enunciare il predetto principio in un procedimento penale per sfruttamento e favoreggiamento della prostituzione, ha ulteriormente precisato che il sequestro preventivo rientra proprio tra quei « provvedimenti adeguati a prevenire... le violazioni », cui si riferisce l'art. 21, comma sesto, Cost.) (Sez. 3, Sentenza n. 39354 del 27 settembre 2007). È sempre ammissibile il sequestro preventivo in caso di diffamazione via web. La misura cautelare reale, che si concretizza nell'oscuramento del sito internet che ospita l'attacco denigratorio, è disposta infatti dal giudice per evitare l'aggravarsi delle conseguenze del reato di cui all'art. 595 del codice penale (sez. 5 Sent. n. 17041 del 15 gennaio 2008).

[17] La Corte, adita in fase cautelare in una fattispecie avente ad oggetto la revoca di un sequestro preventivo di alcune pagine web di un sito internet in cui comparivano messaggi ed espressioni offensive di una confessione religiosa, ha anzitutto affermato che, ai fini della configurabilità del reato di offesa a una confessione religiosa mediante vilipendio di persone (art. 403 c.p.), non occorre che le espressioni di vilipendio debbano essere rivolte a fedeli ben determinati, essendo sufficiente che le stesse siano genericamente riferite alla indistinta generalità dei fedeli, tutelando la norma il sentimento religioso e non la persona (fisica o giuridica) offesa in quanto apparte-

valutazione della coerenza dell'imputazione in rapporto alla misura invocata[18].

Una prospettiva ancora più recente si spinge fino ad analizzare le differenti motivazioni della tutela tra stampa ed altri mezzi interattivi di comunicazione fino ad enucleare la *ratio* di una tutela differenziata per i contenuti *on line* in rapporto alle tipiche responsabilità redazionali della stampa e della comunicazione « redazionale »[19]: ne consegue una approfondita analisi che, muovendo dal tema del sequestro preventivo degli stampati e della sua estensione alle pubblicazioni *on line* finisce per ripercorrere criticamente l'evoluzione giurisprudenziale seguendo il tratto della coerenza costituzionale e della giustificazione funzionale della misura cautelare reale in rapporto ai mezzi di comunicazione[20] ed alle relative specifiche esigenze di libertà, che vanno considerate e valutate appropriatamente proprio nella imposizione (e nella graduazione) della misura cautelare.

Sempre in tema di sequestro preventivo la giurisprudenza si spinge ad analizzare la particolare funzione dello strumento cautelare in rete giustificandone l'uso in ragione « protettiva » (nella specie della proprietà intellettuale violata) ma senza spingersi fino ad esaminare la specificità della « *res* » oggetto di intervento ed i molteplici profili di « effettività » della sanzione cautelare (specie nelle ipotesi di attuazione presso i server nei casi di reindirizzamento)[21].

nente ad una determinata confessione religiosa. Ha, poi, ulteriormente affermato, in merito all'aspetto cautelare, che i messaggi contenenti espressioni offensive della confessione religiosa e residenti sul « forum » ospitato dal sito web, non sono tutelati dalla legge n. 47 del 1948 non rientrando nella nozione di « stampa » e, conseguentemente, non trova applicazione ai messaggi su « forum » (come ad altre forme moderne di comunicazione del pensiero, quali newsletter, blog, newsgroup, mailing list, chat, messaggi istantanei, etc.) la tutela costituzionale in tema di sequestro di cui all'art. 21, comma terzo, Cost. (Sez. 3 Sentenza n. 10535 11 dicembre 2008).

[18] La configurabilità del reato di usurpazione di funzioni pubbliche è necessario che la condotta realizzi in concreto un indebito esercizio di funzioni pubbliche in assenza di una legittima investitura. In tal caso la S.C. ha ritenuto illegittimo il sequestro preventivo di un sito internet creato per sostenere i diritti dei detenuti, escludendo che un esposto presentato all'autorità giudiziaria da parte del suo titolare, ed avente ad oggetto presunti favoritismi all'interno di un istituto penitenziario, usurpasse le attribuzioni proprie dell'organo istituzionale del garante per i diritti delle persone private della libertà personale, appositamente istituito da un ente comunale (sez. 6 Sentenza n. 26178 del 17 marzo 2009).

[19] Cfr. in proposito Di Fabio P., *Il giornalismo telematico: profili giuridici, diritti degli autori e problemi aperti*, in *Il diritto d'autore*, 2006, p. 68; Felici E., *Internet ed autointegrazione del sistema penale*, in *Giurisprudenza di merito*, 2002, p. 765.

[20] È la sentenza della sez. 5 n. 7155 del 24 febbraio 2011 che espressamente afferma come per giustificare il sequestro preventivo di uno spazio internet occorre procedere in concreto ad una valutazione della *possibile riconducibilità del fatto all'area del penalmente rilevante e delle esigenze impeditive tanto serie quanto è vasta l'area della tolleranza costituzionalmente imposta alla libertà di parola.*

[21] È legittimo il provvedimento cautelare con cui il giudice penale, in relazione a condotta di diffusione abusiva in rete di opere dell'ingegno, contestualmente al sequestro preventivo del sito il cui gestore

Non appare estranea alla prospettiva giurisprudenziale anche la problematica della utilizzabilità del sequestro preventivo anche in una prospettiva di confisca delle attrezzature funzionalmente preposte alla organizzata commissione di frodi informatiche[22]. Più complessa appare la ricostruzione — specie sotto il profilo tecnologico — delle potenzialità acquisitive di flussi di comunicazioni e della relativa utilizzabilità processuale, da un lato riconoscendosi la natura di sostanziale intercettazione telematica[23] soggetta quindi a controllo giurisdizionale e a regolamentazione ristretta e dall'altro affermando significative eccezioni in tema di documentazione informatica acquisibile e della sua rilevanza o meno come corrispondenza[24]. Una prospettiva più recente appare orientata al riconoscimento di piena acquisibilità dei dati di flusso (mediante decreto motivato del Pubblico Ministero) nei casi di utilizzazione di terminali collocati in strutture pubbliche o comunque di uso collettivo utilizzati per la commissione organizzata di reati[25].

concorra nell'attività penalmente illecita, imponga ai fornitori di servizi internet operanti sul territorio dello Stato italiano di inibire l'accesso al sito al limitato fine di precludere l'attività di diffusione di dette opere. (In motivazione la Corte ha richiamato gli artt. 14-17 del D.Lgs. n. 70 del 2003 secondo cui l'autorità giudiziaria può esigere, anche in via d'urgenza, che il prestatore di un servizio della società dell'informazione impedisca o ponga fine alle violazioni commesse ovvero impedisca l'accesso al contenuto illecito) (Sez. 3, Sentenza n. 49437 del 29 settembre 2009).

[22] Il sequestro preventivo funzionale alla confisca, prevista dal combinato disposto degli artt. 322-*ter* e 640-*quater* c.p., è applicabile anche al reato di frode informatica aggravato per essere stato il fatto commesso con abuso della qualità di operatore del sistema, se tale aggravante concorre con quella prevista dal numero 1) del secondo comma dell'articolo 640 c.p. (Sez. 6, Sentenza n. 8755 del 5 febbraio 2009).

[23] L'intercettazione di flussi telematici riconducibili ad un determinato utente mediante la procedura di monitoraggio del percorso, disposta dal g.i.p., comporta la legittima captazione dei flussi informatici gestiti dal soggetto titolare di un determinato nome utente che contraddistingue sia l'account di posta elettronica che quello di connessione. Conseguentemente non è causa di invalidità o di inutilizzabilità dei provvedimenti autorizzativi l'improprio riferimento informatico al solo « account » di posta elettronica e non a quello di connessione, trattandosi di due aspetti della stessa realtà giuridica, indicativa della facoltà di accesso di un determinato utente alla trasmissione e alla ricezione dei flussi telematici (Sez. 1, Sentenza n. 12901 del 14 febbraio 2005)

[24] La documentazione bancaria, consistente in supporti cartacei che riproducono dati estratti dalla memoria informatica e relativi ai rapporti intercorsi con l'istituto bancario, non rientra nella nozione di corrispondenza se non risulta che sia stata oggetto di spedizione al soggetto interessato e se per il decorso del tempo le comunicazioni in essa contenute hanno perso il requisito dell'attualità, sicché il sequestro di detta documentazione non richiede, ove l'interessato sia un membro del Parlamento, la previa autorizzazione della Camera a cui questi appartiene. Di conseguenza la sanzione dell'inutilizzabilità, che segue all'acquisizione dei tabulati concernenti il traffico telefonico in assenza di un provvedimento motivato dell'autorità giudiziaria, colpisce non il fatto come rappresentazione della realtà in essi documentata, ma la metodologia di acquisizione di tali atti, sicché, accertata l'inutilizzabilità, può validamente intervenire nello stesso procedimento il decreto motivato di acquisizione dei relativi dati, in modo da legittimarne l'utilizzazione (Sez. 6, Sentenza n. 33435 del 4 maggio 2006).

[25] L'intercettazione di flussi telematici riconducibili ad un determinato utente mediante la procedura di monitoraggio del percorso, disposta dal g.i.p., comporta la legittima captazione dei flussi informatici gestiti dal soggetto titolare di un determinato nome utente che contraddistingue sia

Piena acquisibilità viene sempre riconosciuta ai dati esterni di comunicazione anche mediante i collegamenti IP (*Internet Protocol*) coinvolti nel processo comunicativo[26].

La questione dell'esame della memoria degli apparati informatici è, in buona sostanza, il problema centrale che viene posto in sede critica, poiché da un lato, si sostiene occorre preservare nel senso più stretto i dati nella loro originalità e consistenza secondo quella che è non solo una visione « tecnologica » ma la formale disposizione della norma processuale vigente dopo le integrazioni della L. 48/2008 attuativa della Convenzione di Budapest del 2001, dall'altro si inquadrano tali accertamenti in un contesto « logico » che sembra fondarsi su profili sostanziali e concreti, rispetto ai quali se non altro occorrerà verificare caso per caso le modalità tecniche di accesso e di estrazione dei dati sia in termini di rilevanza effettiva che in rapporto ad effettive (e precise) esigenze funzionali in termini di prova.

Sembra emergere con chiarezza un riconoscimento della ripetibilità delle operazioni di estrazione di dati in memoria operato

l'*account* di posta elettronica che quello di connessione. Conseguentemente non è causa di invalidità o di inutilizzabilità dei provvedimenti autorizzativi l'improprio riferimento informatico al solo « *account* » di posta elettronica e non a quello di connessione, trattandosi di due aspetti della stessa realtà giuridica, indicativa della facoltà di accesso di un determinato utente alla trasmissione e alla ricezione dei flussi telematici (Sez. 1 sent. 12901 del 14 febbraio 2005). È legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel « personal computer » in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del « personal computer » o che in futuro sarebbero stati memorizzati. Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'« hard disk » del computer in uso all'imputato, aveva avuto ad oggetto non un « flusso di comunicazioni », richiedente un dialogo con altri soggetti, ma « una relazione operativa tra microprocessore e video del sistema elettronico », ossia « un flusso unidirezionale di dati » confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. c.p.p. (Sez. 5, Sentenza n. 16556 del 14 ottobre 2009). Sono state anche ritenuti pienamente utilizzabili nel giudizio abbreviato i risultati della localizzazione mediante il sistema di rilevamento satellitare (cosiddetto GPS) degli spostamenti di una persona sul territorio, mediante l'acquisizione delle annotazioni e rilevazioni di servizio della polizia giudiziaria circa le coordinate segnalate dal sistema di rilevamento, in quanto costituiscono il prodotto di un'attività di investigazione atipica assimilabile al pedinamento e non alle operazioni di intercettazione (S Sez. 6, Sentenza n. 15396 del 11 dicembre 2007 e Sez. 1, Sentenza n. 9416 del 7 gennaio 2010). Persino l'assenza di documentazione informatica viene ad essere considerata ritenendosi configurabile il delitto di bancarotta semplice documentale nel caso di perdita, per comportamento negligente o imprudente, della « memoria » informatica del computer contenente le annotazioni delle indicazioni contabili (Sez. 5, Sentenza n. 35886 del 20 luglio 2009), il principio era peraltro già stato espresso (Sez. 5, Sentenza n. 20729 del 21 marzo 2003).

[26] In tema di ingiuria e diffamazione realizzate attraverso l'invio di messaggi di posta elettronica, sono sempre utilizzabili i dati esterni relativi ai collegamenti IP dell'utenza telefonica di trasmissione, acquisiti con decreto motivato del Pubblico Ministero (Sez. 5, Sentenza n. 19491 del 10 marzo 2010).

dalla Polizia giudiziaria[27], pur non mancando posizioni prudenti certamente più attente alla prospettiva di una valutazione tecnica aperta al contraddittorio processuale[28].

Maggiore cautela viene tuttavia — sia pure inizialmente — espressa in sede processuale in tema di validità della fissazione registrazione e trasmissione di richieste giudiziarie su documenti informatici[29]. Dieci anni dopo il principio viene ad essere superato, sembra, a vantaggio di un esame « funzionale » della organizzazione informatica[30].

Ed è proprio la Corte a definire con chiarezza la nozione di « *sistema informatico* » agli effetti penali, anticipando in un certo senso l'ampia definizione della Convenzione di Budapest[31] defi-

[27] Non dà luogo pertanto 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 (Sez. 1, Sentenza n. 11503 del 25 febbraio 2009). L'estrazione dei dati contenuti in un supporto informatico, se eseguita da personale esperto in grado di evitare la perdita dei medesimi dati, costituisce un accertamento tecnico ripetibile (Sez. 1, Sentenza n. 11863 del 26 febbraio 2009). Così non rientra nel novero degli atti irripetibili l'attività di estrazione di copia di « file » da un computer oggetto di sequestro, dal momento che essa non comporta alcuna attività di carattere valutativo su base tecnico-scientifica, né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità d'informazioni identiche a quelle contenute nell'originale (Sez. 1, Sentenza n. 14511 del 5 marzo 2009).

[28] L'esame dell'« hard disk » di un computer in sequestro e la conseguente estrazione di copia dei dati ivi contenuti non sono attività che le parti possono compiere durante il termine per comparire all'udienza dibattimentale senza contraddittorio e alla sola presenza del custode, in quanto implicano accertamenti ed interventi di persone qualificate e l'utilizzo di appositi strumenti, sì che devono essere necessariamente svolti in dibattimento, nel contraddittorio, e sotto la direzione del giudice (Sez. 3, Sentenza n. 28524 del 9 giugno 2009).

[29] La richiesta del P.M. di emissione dell'ordinanza di custodia cautelare in carcere al G.I.P. è — in tale prospettiva — atto che necessariamente deve essere trasmesso al giudice del riesame, essendo tale richiesta il presupposto della misura cautelare *ex* art. 291 c.p.p., in relazione alla quale la difesa è posta in grado di conoscere gli elementi su cui si fonda, nonché tutti gli elementi eventualmente a favore dell'imputato. Non adempirebbe perciò a tale obbligo il P.M. che trasmette la richiesta al Tribunale della libertà solo a mezzo di supporto informatico, e cioè registrata su « dischetto » inserito nel fascicolo. Ciò in quanto tale modalità di trasmissione non è equiparabile all'atto trascritto, per le difficoltà oggettive di procedere alla trascrizione e per i tempi tecnici che essa comporta, a fronte dei termini strettissimi entro cui il giudizio davanti al tribunale del riesame deve svolgersi — sempre che il supporto tecnico sia valido e di facile lettura da parte degli strumenti informatici (Sez. 6, Ordinanza n. 3409 del 30 ottobre 1998).

[30] Così in materia di intercettazioni si afferma come condizione necessaria per l'utilizzabilità delle stesse è che l'attività di registrazione — che, sulla base delle tecnologie attualmente in uso, consiste nella immissione dei dati captati in una memoria informatica centralizzata — avvenga nei locali della Procura della Repubblica mediante l'utilizzo di impianti ivi esistenti, mentre non rileva che negli stessi locali vengano successivamente svolte anche le ulteriori attività di ascolto, verbalizzazione ed eventuale riproduzione dei dati così registrati, che possono dunque essere eseguite « in remoto » presso gli uffici della polizia giudiziaria. In motivazione la Corte ha precisato, con riguardo all'attività di riproduzione — e cioè di trasferimento su supporti informatici di quanto registrato mediante gli impianti presenti nell'ufficio giudiziario —, che trattasi di operazione estranea alla nozione di « registrazione », la cui « remotizzazione » non pregiudica le garanzie della difesa, alla quale è sempre consentito l'accesso alle registrazioni originali) (Sez. U, Sentenza n. 36359 del 26 giugno 2008).

[31] Data dall'art. 1 lettera *a*) della

nendo quale sistema informatico « *un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate — per mezzo di un'attività di "codificazione" e "decodificazione" — dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente* »[32].

Il principio affermato assume una particolare valenza evolutiva proprio nel riservare al giudice ogni valutazione in ordine al profilo funzionale dei sistemi informatici (e telematici) interessati, ricomprendendone ogni aspetto che sia in qualche modo legato al trattamento informatico di dati o di informazioni, e legando il significato definitorio alla logica informatica della programmazione, all'uso di infrastrutture di qualsiasi genere, alla interfaccia uomo-macchina in relazione all'aggregazione dei dati immessi ed alle operazioni derivanti dal processo elaborativo, e ciò indipendentemente dalle caratteristiche oggettive proprie dei sistemi utilizzati.

In questo modo la Corte non solo « anticipa » i tempi ma si apre ad una visione avanzata e tecnologica del diritto penale e segna un passo fondamentale per non vincolare l'interpretazione normativa alla conformazione specifica degli apparati informatici, cogliendo proprio l'evoluzione di ogni apparato informatico attraverso la sua utilizzazione in rete anziché attraverso la sola elaborazione di dati e la registrazione di essi su supporti in forma digitale.

3. Nuove forme di condotte criminose, nuove condotte criminose.

Una prima differenziazione si impone tra reati i quali vengono ad essere commessi in rete concretando nuove forme commissive

Convenzione che definisce come « sistema informatico » qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati.

[32] Aggiunge la Corte che la valutazione circa il funzionamento di apparecchiature a mezzo di tali tecnologie costituisce giudizio di fatto insindacabile in cassazione ove sorretto da motivazione adeguata e immune da errori logici. Nella specie è stata ritenuta corretta la motivazione dei giudici di merito che avevano riconosciuto la natura di « sistema informatico » alla rete telefonica fissa — sia per le modalità di trasmissione dei flussi di conversazioni sia per l'utilizzazione delle linee per il flusso dei cosiddetti « dati esterni alle conversazioni » — in un caso in cui erano stati contestati i reati di accesso abusivo a sistema informatico e di frode informatica (Cass. Sez. 6, Sentenza n. 3067 del 4 ottobre 1999).

di condotte criminose tradizionali, e quindi ponendo inediti profili di prova in relazione alle specificità del mezzo o dei mezzi utilizzati per la commissione del reato e condotte criminose — di carattere informatico — assolutamente nuove che tramite la rete vengono ad essere concretate in un quadro di tipicità che si esprime attraverso il ricorso a forme di accesso e condivisione di dati e contenuti in modo organizzato e comunque controllato dall'utente.

Vengono, attraverso la rete, ad essere ampliate le forme commissive di molte condotte criminose tradizionali, per lo più basate sulla diffusione (o sulla acquisizione) di contenuti espressivi cui il contatto e l'interattività che la « forma » telematica assicura, fattispecie penali nelle quali la libertà della forma corrisponde ad un adattamento evolutivo in un certo senso naturale, è la modalità realizzativa dei reati che si adatta al nuovo messo e che viene gradualmente ad essere riconosciuta a livello giurisprudenziale.

In altri casi, si vedrà, sono poste espressamente nuove fattispecie di reato, specificamente riferite anche a modalità commissive di carattere informatico, è il caso di tutta la categoria dei c.d. « reati informatici » come la frode informatica, l'accesso abusivo nei sistemi informatici, il danneggiamento informatico, reati per i quali si pone quasi sempre una problematica interpretativa che mira più alla esatta ricomprensione di svariate condotte tecnologiche nel frattempo intervenute che non alla riconduzione alle categorie tradizionali. Si pongono problemi, in altri termini, che appaiono sempre di più legati al riconoscimento, alla interconnessione oggettiva e soggettiva dei soggetti agenti, ed interagenti, alla ricomposizione di un quadro estremamente sofisticato di comportamenti diretti ed indiretti, alla attribuibilità specifica di condotte apparentemente lontane o distanti, che l'indagine penale ricompone e qualifica.

Non ha comportato particolari problematiche né il riconoscimento della utilizzazione *on line* fraudolenta di strumenti di pagamento[33] né il primo riconoscimento di condotte criminali associative utilizzanti attraverso la rete, seppur rilevandosi i primi, significativi, spunti problematici in tema di competenza territoriale[34].

[33] Costituisce indebita utilizzazione di carta di credito, ai sensi dell'art. 12 del D.L. 3 maggio 1991 n. 143, convertito con modifiche in L. 5 luglio 1991 n. 197, l'effettuazione attraverso la rete internet di transazioni, previa immissione dei dati ricognitivi e operativi di una valida carta di credito altrui, acquisiti dall'agente fraudolentemente con il sistema telematico, nulla rilevando che il documento non sia stato nel suo materiale possesso (Sez. 1, Sentenza n. 37115 del 2 ottobre 2002).

[34] Così in tema di associazione per delinquere, trattandosi di reato permanente, la competenza territoriale va individuata *ex* art. 8, comma terzo, c.p.p., con la conseguenza che essa spetta al giudice del luogo in cui ha avuto inizio la consumazione del reato. Tuttavia, qualora gli atti del processo non offrano elementi certi per l'individuazione di tale luogo, deve farsi ricorso ai criteri sussidiari previsti dall'art. 9 c.p.p. Alla luce di tale disposizione, ove non siano comunque percepibili neppure elementi presuntivi che valgano a radicare la competenza territoriale nel luogo in cui il sodalizio criminoso si manifesti per la prima volta all'esterno, possono utilizzarsi criteri desumibili dai reati fine, con particolare riferimento a quello della consuma-

Così anche l'estensione funzionale delle fattispecie dello sfruttamento e del favoreggiamento della prostituzione avviene con la trasposizione dal reale al virtuale mediante un collegamento « funzionale » tra condotte che si sofferma sui caratteri della prestazione sessuale retribuita anche mediante il semplice contatto telematico e non l'effettivo svolgimento di attività di contatto « fisiche »[35].

In relazione al reato di falso documentale il riconoscimento appare del pari legato alle caratteristiche del sistema utilizzato per produrre o estrarre informazioni anziché alla condotta a carattere logico-informatico, tanto più in situazioni quasi coincidenti[36].

zione dell'ultimo reato fine, specialmente nel caso in cui detti reati siano stati tutti commessi nello stesso luogo e siano tutti dello stesso tipo. Nella specie, nella quale l'associazione aveva ad oggetto i reati di accesso abusivo a sistema informatico e frode informatica, mediante ingresso in rete telefonica, attraverso un'utenza dalla quale venivano abusivamente raggiunte, in modo fraudolento e reiterato, utenze estere, si è ritenuto territorialmente competente il giudice del luogo dell'ultima telefonata (Sez. 6, Sentenza n. 3067 del 4 ottobre 1999).

[35] Le prestazioni sessuali eseguite in videoconferenza in modo da consentire al fruitore delle stesse di interagire in via diretta ed immediata con chi esegue la prestazione, con la possibilità di richiedere il compimento di atti sessuali determinati, assume il valore di atto di prostituzione e configura il reato di sfruttamento della prostituzione a carico di coloro che abbiano reclutato gli esecutori delle prestazioni o ne abbiano consentito lo svolgimento creando i necessari collegamenti via internet o ne abbiano tratto guadagno, atteso che è irrilevante il fatto che chi si prostituisce ed il fruitore della prestazione si trovino in luoghi diversi in quanto il collegamento in videoconferenza consente all'utente di interagire con chi si prostituisce in modo tale da potere richiedere a questi il compimento di atti sessuali determinati che vengono immediatamente percepiti da chi ordina la prestazione sessuale a pagamento (Sez. 3, Sentenza n. 25464 del 22 aprile 2004). La prestazione sessuale eseguite in videoconferenza via *web-chat*, in modo da consentire al fruitore delle stesse di interagire in via diretta ed immediata con chi esegue la prestazione, con la possibilità di richiedere il compimento di determinati atti sessuali, assume il valore di prostituzione e rende configurabile il reato di sfruttamento della prostituzione nei confronti di coloro che abbiano reclutato gli esecutori delle prestazioni o che abbiano reso possibile i collegamenti via internet, atteso che l'attività di prostituzione può consistere anche nel compimento di atti sessuali di qualsiasi natura eseguiti su se stesso in presenza di colui che, pagando un compenso, ha richiesto una determinata prestazione al fine di soddisfare la propria *libido*, senza che avvenga alcun contatto fisico fra le parti (Sez. 3, Sentenza n. 15158 del 21 marzo 2006).

[36] Integra il reato di cui agli artt. 476, comma primo e 491-*bis* c.p. (falso materiale in atto pubblico) la condotta del pubblico ufficiale che, in qualità di addetto al servizio di inserimento dati nel sistema di verbalizzazione informatica, alteri documenti informatici pubblici relativi alla predisposizione di verbali di accertamento di violazioni delle norme del codice della strada; né, a tal fine, rileva la circostanza che il sistema informatico coesista con quello cartaceo di supporto, in quanto l'art. 491-*bis* c.p. — che sanziona sia la falsità concernente direttamente i dati o le informazioni dotati, già in sé, di rilevanza probatoria sia quella relativa a programmi specificamente destinati ad elaborarli — riguarda tanto l'ipotesi in cui il sistema informatico sia supportato da riscontro cartaceo quanto quella in cui il sistema informatico sia del tutto sostitutivo di quello cartaceo (Sez. 5, Sentenza n. 45313 del 21 settembre 2005). Integra la condotta di falsità materiale in atto pubblico la falsificazione di atti contenuti nei supporti del sistema informatico di un ente pubblico, anche quando gli stessi siano documentati in forma cartacea. Nella specie, era stato alterato nel sistema informatico di un ospedale il contenuto di un referto medico (Sez. 6, Sentenza n. 7752 del 16 gennaio 2009). È configurabile il reato previsto dall'art. 479 c.p. in relazione alla formazione di carte di circolazione ad opera di un dipendente della

Non senza qualche iniziale prudenza viene gradualmente ammessa la configurabilità del reato di esercizio abusivo di giuochi e scommesse e quindi per il giuoco d'azzardo attraverso internet, in tal caso percependo più l'elusività del mezzo rispetto al precetto penale che ricostruendone realmente il sistema di funzionamento *on line* nella raccolta di puntate e nella relativa distribuzione[37].

Più articolato appare invece il percorso giurisprudenziale in tema di diffamazione, ove certamente il mezzo di comunicazione è oggetto di approfondimento, esprimendosi inizialmente una posizione attenta alle dimensioni internazionali della rete in rapporto al sindacato giurisdizionale ed ai suoi limiti territoriali[38] fino a

Motorizzazione civile, addetto ad altro servizio di certificazione, attraverso l'accesso al sistema informatico della Direzione generale della M.C.T.C. (Sez. 6, Sentenza n. 35839 del 9 aprile 2008).

[37] Integra il reato di attività organizzata per la accettazione e raccolta, anche per via telefonica o telematica di scommesse, senza l'autorizzazione ministeriale prevista dall'art. 88 del T.U.L.P.S. — previsto dall'art. 4 della legge 13 dicembre 1989, n. 401 — l'attività svolta da un intermediatore mediante la messa a disposizione del proprio conto scommesse tramite accesso internet, atteso che il decreto ministeriale 15 febbraio 2001 n. 156 (relativo alla raccolta telefonica o telematica delle giocate relative a scommesse, giochi e concorsi pronostici) continua a richiedere l'esistenza di un rapporto diretto tra il concessionario e lo scommettitore ed il decreto ministeriale del 31 maggio 2002, consentendo l'attivazione da parte del cliente di un conto scommesse personale presso il concessionario, esige che tale conto sia da questi utilizzato a titolo personale e non diventi oggetto di transazioni da parte di soggetti diversi (Sez. 3, Sentenza n. 26849 del 4 maggio 2004).

Integra il reato di cui all'art. 4 della L. 13 dicembre 1989, n. 401 l'attività di accettazione e raccolta di scommesse su eventi sportivi, svolta mediante comunicazioni telefoniche o telematiche da parte di soggetto intermediario sprovvisto della licenza prevista dall'art. 88 T.u.l.p.s., anche se munito dell'autorizzazione ministeriale di cui all'art. 25 del Codice delle comunicazioni. La Corte ha precisato che il possesso dell'autorizzazione all'installazione dei macchinari per la costituzione di un « internet point » non esenta il titolare del centro di trasmissione dati dell'obbligo di munirsi dell'autorizzazione per l'esercizio dell'attività di raccolta di scommesse (Sez. 3, Sentenza n. 5914 del 10 novembre 2009). Non integrerebbe il reato di attività organizzata per la accettazione e la raccolta, per via telematica, di scommesse, senza l'autorizzazione ministeriale di cui all'art. 88 del T.U.L.P.S., previsto dall'art. 4 della legge n. 401 del 1989, la condotta del titolare di esercizio commerciale che si limiti, tramite postazione internet, a fornire il supporto tecnico per l'inoltro dei dati dallo scommettitore al concessionario, in tal modo rimanendo estraneo al rapporto di scommessa (Sez. 3, Sentenza n. 26912 del 5 maggio 2009). Integra il delitto di cui all'art. 4, comma quarto-*bis*, L. 13 dicembre 1989, n. 401, e non la contravvenzione di cui all'art. 4, comma primo della legge citata, l'esercizio abusivo, mediante collegamento a siti internet di « bookmakers » esteri, di attività organizzata finalizzata all'accettazione, alla raccolta o al favoreggiamento dell'accettazione per via telematica di scommesse su partite di calcio del campionato italiano, trattandosi di scommesse pronostici su attività sportive gestite dal CONI (Sez. 3, Sentenza n. 26757 del 5 maggio 2010). Configura il reato di esercizio di giuoco d'azzardo l'installazione in un pubblico esercizio di un apparecchio automatico elettronico che, collegandosi in rete a sito internet dedicato, consenta di scegliere tra le diverse applicazioni possibili quella denominata « videopoker », caratterizzata dall'alea e dal fine di lucro, consistente nell'accumulo di crediti utilizzabili per ulteriori partite e trasferibili su « smart card » nel conto punti dell'avventore (si trattava del sequestro preventivo di apparecchio del tipo « totem internet » denominato « NetShop ») Sez. 3 (Sentenza n. 11877 del 18 febbraio 2010).

[38] Ed ancora si è affermato che il giudice italiano è (sempre) competente a conoscere della diffamazione compiuta mediante l'inserimento nella rete telematica (internet) di frasi offensive e/o immagini denigratorie, anche nel caso in cui il sito web sia

pervenire alla considerazione primaria dell'effetto del contenuto offensivo e nella relativa percezione[39] anche quale possibile elemento dirimente nella definizione della competenza territoriale, aspetto ancora non ben definito con precisione.

Emerge, quindi, la specificità del tema della diffamazione entro un contesto informativo continuativo ed organizzato redazionalmente[40], sia pure intravedendo in alcune posizioni specificità problematiche legate a singole figure di reato[41] almeno nelle condotte di tipo commissivo rispetto alle quali il mezzo telematico assicura una nuova forma di azione senza alterarne la tipicità funzionale delle singole condotte concretamente individuabili.

Gradualmente, e sia pure con qualche difficoltà, comincia ad emergere la consapevolezza della peculiarità della rete quale strumento di carattere informativo essenziale e quindi tale da meritare particolare attenzione sul piano del rispetto dei diritti di cronaca e di critica[42]. Finalmente le posizioni più recenti appaiono più sen-

stato registrato all'estero e purché l'offesa sia stata percepita da più fruitori che si trovino in Italia; invero, in quanto reato di evento, la diffamazione si consuma nel momento e nel luogo in cui i terzi percepiscono la espressione ingiuriosa (Sez. 5, Sentenza n. 4741 del 17 novembre 2000).

[39] La diffamazione, che è reato di evento, si consuma nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa e dunque, nel caso in cui frasi o immagini lesive siano state immesse sul web, nel momento in cui il collegamento viene attivato (Sez. 5, Sentenza n. 25875 del 21 giugno 2006). Il reato di diffamazione consistente nell'immissione nella rete Internet di frasi offensive e/o immagini denigratorie, deve ritenersi commesso nel luogo in cui le offese e le denigrazioni sono percepite da più fruitori della rete, pur quando il sito « web » sia registrato all'estero (Sez. 2, Sentenza n. 36721 del 21 febbraio 2008).

[40] Ai fini dell'integrazione del delitto di diffamazione (art. 595 c.p.), si deve presumere la sussistenza del requisito della comunicazione con più persone qualora il messaggio diffamatorio sia inserito in un sito internet per sua natura destinato ad essere normalmente visitato in tempi assai ravvicinati da un numero indeterminato di soggetti, quale è il caso del giornale telematico, analogamente a quanto si presume nel caso di un tradizionale giornale a stampa, nulla rilevando l'astratta e teorica possibilità che esso non sia acquistato e letto da alcuno (Sez. 5, Sentenza n. 16262 del 4 aprile 2008).

[41] In tema di rivelazione di segreti d'ufficio, risponde del reato a titolo di concorso con l'autore principale il direttore responsabile di un sito internet ove sia stata effettuata la pubblicazione di un atto amministrativo a carattere riservato. Nel caso di specie, la Corte ha ravvisato l'astratta ipotizzabilità del concorso nel reato di cui all'art. 326 c.p., ritenendo sussistente il requisito del « *fumus commissi delicti* » in ordine al sequestro preventivo della pagina di un sito « web » su cui era avvenuta la pubblicazione delle notizie riservate (Sez. 6, Sentenza n. 30968 del 28 giugno 2007). Non sussiste — ancora — simulazione di reato quando l'alterazione del vero riguarda modalità e circostanze di fatto che non influiscono sulla configurazione giuridica del reato effettivamente commesso. In applicazione di tale principio, la Corte ha escluso la configurabilità del reato di cui all'art. 367 c.p. nella condotta di una persona che, dopo aver presentato una querela per diffamazione in relazione alla pubblicazione su internet di foto che la ritraevano in atteggiamenti pornografici, aveva negato in una dichiarazione integrativa, contrariamente al vero, che le foto riguardassero la sua persona (Sez. 6, Sentenza n. 38571 del 30 settembre 2008).

[42] L'immissione via internet del contenuto di una denunzia presentata nei confronti di una società e relativa a scarico di cancerogeni nell'ambiente esterno costituisce manifestazione del diritto di cronaca e anche di critica che spetta, *ex* art. 21 Cost., ad ogni individuo « *uti civis* » e non solo ai giornalisti o a chi svolge professionalmente attività di informazione, e che è tuttavia sottoposto all'osservanza di limiti, rappresen-

sibili alla definizione di una graduazione di responsabilità redazionale in rete che non è immediatamente corrispondente né assimilabile alla tradizionale responsabilità redazionale nella stampa o nella radiotelevisione, ma che richiede una puntuale dimostrazione in termini di condotta commissiva o omissiva tenendo conto delle specifiche caratteristiche del mezzo e del sistema di individuazione e di organizzazione dei contenuti immessi[43].

Non sono mancate posizioni attente ai profili commissivi tipici dei reati di istigazione, come nel caso di siti recanti contenuti di propaganda di idee fondate sulla superiorità e sull'odio razziale e religioso[44] e di istigazione all'uso di sostanze stupefacenti[45].

La tematica della posta elettronica costituisce ancora una volta un terreno di confine nel quale convivono aspetti di tutela della *privacy* ed esigenze di garanzia individuale di comunicazione, an-

tati dalla rilevanza sociale dell'argomento, dalla verità obbiettiva dei fatti riferiti e dal rispetto della continenza nelle espressioni utilizzate, che va accertata dal giudice di merito. In applicazione di tale principio la S.C. ha censurato la decisione del giudice di appello il quale ha escluso, in riforma della sentenza di primo grado, l'esistenza del reato di diffamazione, omettendo — ancorché la persona del denunziante coincidesse con quella del diffusore della notizia, la quale non consisteva nella mera comunicazione della esistenza di una denunzia ma nella esplicitazione del contenuto e degli elementi fattuali portati a sostegno di essa — di accertare la rispondenza al vero dei fatti denunziati e di fornire al riguardo adeguata motivazione (Sez. 5, Sentenza n. 31392 del 1 luglio 2008).

[43] Puntualizza la posizione del responsabile di contenuti *on line* in tema di diffamazione altra decisione secondo la quale sul piano pratico, poi, non andrebbe trascurato che la c.d. interattività (la possibilità di interferire sui testi che si leggono e si utilizzano) renderebbe, probabilmente, vano — o comunque estremamente gravoso — il compito di controllo del direttore di un giornale on line. Dunque, accanto all'argomento di tipo sistematico (non assimilabilità normativamente determinata del giornale telematico a quello stampato e inapplicabilità nel settore penale del procedimento analogico in malam partem), andrebbe considerata anche la problematica esigibilità della ipotetica condotta di controllo del direttore (con quel che potrebbe significare sul piano della effettiva individuazione di profili di colpa). Da ultimo, va considerata anche la implicita *voluntas legis*, atteso che, da un lato, risultano pendenti diverse ipotesi di estensione della responsabilità *ex* art. 57 c.p. al direttore del giornale telematico (il che costituisce ulteriore riprova che — ad oggi — tale responsabilità non esiste), dall'altro, va pur rilevato che il legislatore, come ricordato dal ricorrente, è effettivamente intervenuto, negli ultimi anni, sulla materia senza minimamente innovare sul punto (Sez. 5 sent. 35511 del 16 luglio 2010).

[44] In tema di atti di discriminazione razziale ed etnica, anche a seguito delle modifiche apportate dall'art. 13 della L. 24 febbraio 2006, n. 85 all'art. 3, comma primo, lett. *a*) della L. 13 ottobre 1975, n. 654 (come modificato dall'art. 1 del D.L. 26 aprile 1993, n. 122, conv. con modd. in L. 25 giugno 1993, n. 205), sussiste continuità normativa tra le corrispondenti fattispecie incriminatrici, in quanto la condotta consistente nel « propagandare » idee fondate sulla superiorità o sull'odio razziale o etnico era già ricompresa in quella, originariamente prevista, consistente nel « diffondere » in qualsiasi modo le medesime idee. Concreta tale ipotesi anche la predisposizione di un sito internet contenente espressioni razziste ed antisemite (Sez. 3, Sentenza n. 37581 del 7 maggio 2008).

[45] È configurabile il reato d'istigazione all'uso di sostanze stupefacenti nel caso in cui, unitamente ai semi di canapa indiana, si forniscano agli acquirenti dettagliate informazioni circa le modalità e gli strumenti idonei alla coltivazione di essi. Nella specie si contestava all'indagato di aver posto in vendita e pubblicizzato, anche tramite Internet, semi di canapa indiana, con accessori, DVD e libri contenenti spiegazioni sulle più opportune modalità di coltivazione (Sez. 4, Sentenza n. 23903 del 20 maggio 2009).

che in questo caso la giurisprudenza della S.C. sembra consapevole di muoversi in un ambito particolarmente delicato, essa cioè sembra insieme ricomporre gli aspetti critici in un tentativo di analisi della duplice funzione comunicativa che lo strumento assume, insieme di espressione individuale e di contatto collettivo ed immediato.

Ne consegue, anche per tale ultimo profilo, che l'analisi giurisprudenziale si presenta attenta sotto l'aspetto evolutivo ed insieme rivolta alla definizione di un insieme di principi regolatori uniformanti le nuove metodologie comunicative. Fattispecie nuove, in parte derivanti dalle leggi speciali, in parte innestate nelle tradizionali figure di reato del Codice penale vengono così a costituire oggetto di indagine e riferimento puntuale di stringente attualità.

Così si valuta la diffusione di indirizzi di posta elettronica nel rapporto con le disposizioni in tema di protezione di dati personali, escludendone l'applicabilità nei casi di diffusione occasionale e di reperibilità on line dei medesimi[46], si dà spazio al diritto di critica esercitato attraverso l'invio di *e mail* di carattere sindacale[47], si riconosce i caratteri del reato di sostituzione di persona nella attivazione abusiva di un *account* di posta elettronica e nella successiva generazione di messaggi imputabili a terzi[48]. Cauta ap-

[46] Il trattamento dei dati personali, che non siano sensibili né abbiano carattere giudiziario, effettuato da un soggetto privato per fini esclusivamente personali è soggetto alle disposizioni del Testo unico in materia di trattamento dei dati personali solo se i dati siano destinati ad una comunicazione sistematica o alla diffusione ed è in tal caso subordinato al consenso dell'interessato, a meno che il trattamento riguardi dati provenienti da pubblici registri od elenchi conoscibili da chiunque. Nel caso di specie la Suprema Corte ha ritenuto che l'aver comunicato ad alcuni « provider » le generalità, l'indirizzo, ivi compreso quello di posta elettronica, il numero di telefono e il codice fiscale di una persona senza il suo consenso, al fine di aprire un sito internet e tre nuovi indirizzi di posta elettronica a nome di tale persona, non integra il reato di cui all'art. 167, comma primo D.Lgs. n. 196 del 2003 (Sez. 3, Sentenza n. 5728 del 17 novembre 2004).

[47] In tema di diffamazione, il divieto di « excepio veritatis », alla luce di un'interpretazione costituzionalmente orientata dell'art. 596, comma primo, c.p., non può trovare applicazione qualora l'autore del fatto incriminato abbia agito nell'esercizio di un diritto, *ex* art. 51 c.p. e, quindi, non solo nell'ipotesi di diritto di cronaca spettante al giornalista ma in ogni caso in cui si prospetti il legittimo esercizio del diritto di critica. In applicazione di questo principio la S.C. ha censurato la decisione con cui il giudice di appello ha confermato la responsabilità a titolo del reato di cui all'art. 595 c.p. — nei confronti di alcuni collaboratori di una società che avevano indirizzato ai clienti della stessa società una « e-mail » con la quale si attribuiva a quest'ultima l'inosservanza del contratto collettivo di lavoro e l'inadempimento degli obblighi retributivi — rigettando l'istanza di produzione documentale volta a dimostrare la veridicità delle affermazioni contenute nella missiva, senza avere motivatamente escluso che il messaggio di posta elettronica incriminato fosse stato inviato nell'esercizio di un diritto di critica (Sez. 5, Sentenza n. 1369 del 5 novembre 2008).

[48] Integra il reato di sostituzione di persona (art. 494 c.p.), la condotta di colui che crei ed utilizzi un « account » di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete « internet » nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a le-

pare invece la posizione giurisprudenziale in tema di uso improprio della posta elettronica, escludendo la rilevanza penale di condotta di cognizione in ambito aziendale della posta di dipendenti ove ciò sia corrispondente ad un protocollo di condotta preesistente[49], ed escludendo la rilevanza anche sotto il profilo delle molestie di messaggi di posta elettronica[50] che tuttavia, se caratterizzati da una insistenza temporale e da contenuti particolarmente offensivi ed umilianti possono allora ben concretare l'ipotesi di reato di atti persecutori di cui all'art. 612-*bis* c.p.[51].

Più complessa appare invece la riflessione che muove dalle integrazioni normative in tema di contrasto alla pornopedofilia via Internet[52]. Qui l'impatto con la rete appare diretto, e le questioni affrontate vengono immediatamente ad enuclearsi in dettaglio quali aspetti innovativi consistenti e per di più in un ambito socialmente (ed internazionalmente) molto sensibile.

Vengono così ad essere affrontate le questioni legate alla distribuzione di contenuti pornografici riguardanti minori nelle forme più varie[53] con particolare attenzione alle fattispecie introdotte dalla L. n. 269 del 1998 e progressivamente integrate.

derne l'immagine e la dignità (Sez. 5, Sentenza n. 46674 del 8 novembre 2007).

[49] Non integra il reato di cui all'art. 616 c.p. la condotta del superiore gerarchico che prenda cognizione della posta elettronica contenuta nel computer del dipendente, assente dal lavoro, dopo avere a tal fine utilizzato la password in precedenza comunicatagli in conformità al protocollo aziendale (Sez. 5, Sentenza n. 47096 del 11 dicembre 2007).

[50] Non integra il reato di molestia o disturbo alla persona col mezzo del telefono o l'invio di un messaggio di posta elettronica che provochi turbamento o fastidio nel destinatario (Sez. 1, Sentenza n. 24510 del 17 giugno 2010).

[51] Integra l'elemento materiale del delitto di atti persecutori (art. 612-*bis* c.p. il reiterato invio alla persona offesa di « sms » e di messaggi di posta elettronica o postati sui cosiddetti « social network » (ad esempio « facebook »), nonché la divulgazione attraverso questi ultimi di filmati ritraenti rapporti sessuali intrattenuti dall'autore del reato con la medesima (Sez. 6, Sentenza n. 32404 del 16 luglio 2010).

[52] Su cui cfr. MANNA A., *Considerazioni sulla responsabilità penale dell'Internet provider in tema di pedofilia*, in questa *Rivista*, 2001, p. 145.

[53] Rientrano nella fattispecie di cui all'art. 600-*ter* c.p.: *a*) il commercio di materiale pornografico inerente i minori che richiede la predisposizione di un attività di impresa, con adeguati strumenti di distribuzione, nella prospettiva di una offerta del prodotto destinata a durare nel tempo; *b*) la distribuzione, che si configura come forma particolare di commercializzazione, la quale deve ritenersi integrata dalla diffusione fisica del materiale mediante l'invio ad un novero, definito o meno, di destinatari; *c*) la divulgazione e pubblicazione, le quali richiedono sia che la condotta sia destinata a raggiungere una serie indeterminata di persone, con cui l'agente ha stabilito un rapporto di comunicazione, sia un mezzo di diffusione accessibile ad una pluralità di soggetti. La cessione occasionale, singolarmente effettuata (ex comma 4), del materiale è fattispecie per sua natura sussidiaria rispetto a quelle previste nei commi precedenti dello stesso art. 600-*ter* c.p., che non può trovare applicazione quando sussistano gli elementi per la operatività degli stessi. Conseguentemente la Corte ha ritenuto che integrasse il reato di cui all'art. 600, comma 3, c.p. l'avere veicolato fotografie oscene di minori attraverso la rete Internet (Sez. 3, Sentenza n. 2421 del 13 giugno 2000). Sussiste il delitto di cui all'art. 600-*ter* c.p. qualora il soggetto inserisca foto pornografiche minorili in un sito accessibile a tutti ovvero quando le propaghi attraverso usenet, inviandole ad un gruppo o lista di discussione da cui chiunque le possa scaricare; mentre è configurabile l'ipotesi più lieve di cui all'art. 600-*ter*, comma 4, quando il sogget-

Viene ad essere riconosciuto un carattere obiettivo dei contenuti in quanto tali offensivi per la dignità della persona rappresentata che trascende, in qualche modo, dalle finalità della organizzazione e della raccolta dei contenuti stessi, per esprimersi in funzione essenzialmente protettiva della persona del minore[54].

E ciò ben si correla alle disposizioni della Convenzione internazionale sui diritti dell'infanzia e dell'adolescenza approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre del 1989 a New York ed è entrata in vigore il 2 settembre 1990 e ratificata con la L. n. 176 del 27 maggio 1991 che pone obiettivi fondamentali in modo espresso (art. 34) per cui gli Stati parti si impegnano a proteggere il fanciullo contro ogni forma di sfruttamento sessuale e di violenza sessuale. A tal fine, gli Stati adottano in particolare ogni adeguata misura a livello nazionale, bilaterale e mul-

to invii dette foto ad una persona determinata allegandole ad un messaggio di posta elettronica, sicché solo questa abbia la possibilità di prelevarle (Sez. 3, Sentenza n. 5397 del 3 dicembre 2001) Ai fini della configurabilità del reato di cui all'art. 600-*ter*, comma 3, c.p. (distribuzione, divulgazione o pubblicizzazione del materiale pornografico minorile con qualsiasi mezzo, anche in via telematica) non è sufficiente la cessione di detto materiale a singoli soggetti ma occorre che esso sia propagato ad un numero indeterminato di persone. Ne consegue che non è sufficiente ad integrare il reato di cui all'art. 600-*ter*, comma 3, c.p. il mero utilizzo della rete internet — essendo comunque necessario che l'offerta sia diretta ad un numero indeterminato di persone in quanto ove l'offerta sia destinata a persone determinate, sussiste la più lieve ipotesi di cui all'art. 600-*ter*, comma 4, c.p., indipendentemente dall'uso o meno del mezzo telematico —, ma occorre accertare quale tipo di connessione telematica sia utilizzata al momento della commissione del reato, in quanto, ove si accerti trattarsi di connessione aperta, sussiste il reato più grave di cui all'art. 600-*ter*, comma 3, c.p., mentre, nell'ipotesi di connessione riservata, sussiste il reato più lieve di cui all'art. 600-*ter*, comma 4, c.p. (Sez. 3, Sentenza n. 12372 del 28 gennaio 2003).

[54] Poiché il delitto di pornografia minorile di cui al primo comma dell'art. 600-*ter* c.p. — mediante il quale l'ordinamento appresta una tutela penale anticipata della libertà sessuale del minore, reprimendo quei comportamenti prodromici che, anche se non necessariamente a fine di lucro, ne mettono a repentaglio il libero sviluppo personale con la mercificazione del suo corpo e l'immissione nel circuito perverso della pedofilia — ha natura di reato di pericolo concreto, la condotta di chi impieghi uno o più minori per produrre spettacoli o materiali pornografici è punibile, salvo l'ipotizzabilità di altri reati, quando abbia una consistenza tale da implicare concreto pericolo di diffusione del materiale prodotto. Nell'occasione la Corte ha altresì precisato che è compito del giudice accertare di volta in volta la configurabilità del predetto pericolo, facendo ricorso ad elementi sintomatici della condotta quali l'esistenza di una struttura organizzativa anche rudimentale atta a corrispondere alle esigenze di mercato dei pedofili, il collegamento dell'agente con soggetti pedofili potenziali destinatari del materiale pornografico, la disponibilità materiale di strumenti tecnici di riproduzione e/o trasmissione, anche telematica idonei a diffondere il materiale pornografico in cerchie più o meno vaste di destinatari, l'utilizzo contemporaneo o differito nel tempo di più minori per la produzione del materiale pornografico — dovendosi considerare la pluralità di minori impiegati non elemento costitutivo del reato ma indice sintomatico della pericolosità concreta della condotta —, i precedenti penali, la condotta antecedente e le qualità soggettive del reo, quando siano connotati dalla diffusione commerciale di pornografia minorile nonché gli altri indizi significativi suggeriti dall'esperienza; ed ha di conseguenza escluso la ricorrenza del concreto pericolo di diffusione del materiale in un'ipotesi in cui l'agente aveva realizzato e detenuto alcune fotografie pornografiche che ritraevano un minorenne, consenziente, per uso puramente « affettivo », anche se perverso (Sez. U, Sentenza n. 13 del 5 luglio 2000).

tilaterale per impedire: *a*) che dei fanciulli siano incitati o costretti a dedicarsi a una attività sessuale illegale; *b*) che dei fanciulli siano sfruttati a fini di prostituzione o di altre pratiche sessuali illegali; *c*) che dei fanciulli siano sfruttati ai fini della produzione di spettacoli o di materiale cinematografico.

Inoltre proprio il contrasto alla pornopedofilia è al centro della Convenzione di Budapest del 2001 che detta una disciplina specifica (art. 9) in sostanza coincidente con disposizioni già vigenti in Italia con l'intervento normativo del 1998 che hanno introdotto gli artt. 600-*bis*, *ter*, *quater*, *quinquies*, *septies* del Codice Penale inquadrandone le diverse condotte tra i delitti contro la personalità individuale[55].

Trova riconoscimento pieno l'ipotesi di configurabilità di associazioni a delinquere *on line* basate sullo scambio sistematico ed organizzato di materiale pornografico riguardante minori[56] e si afferma progressivamente una esigenza di attenzione funzionale tanto nelle metodologie tecnologiche di accertamento dei reati che nelle concrete tecniche di acquisizione probatoria (posta in essere attraverso la polizia specializzata). Ne deriva una attenzione alle forme accertabili di accesso alla rete ed alle tecniche di con-

[55] Articolo 9. (*Reati relativi alla pornografia infantile*). — 1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesse intenzionalmente e senza alcun diritto: *a*) la produzione di pornografia infantile allo scopo della sua diffusione attraverso un sistema informatico; *b*) l'offerta o la messa a disposizione di pornografia infantile attraverso un sistema informatico; *c*) la distribuzione o la trasmissione di pornografia infantile attraverso un sistema informatico; *d*) il procurare pornografia infantile attraverso un sistema informatico per se stessi o altri; *e*) il possesso di pornografia infantile attraverso un sistema informatico o uno strumento di archiviazione di dati informatici.

2. Ai fini del Paragrafo 1. di cui sopra, l'espressione « pornografia infantile » include il materiale pornografico che raffigura: *a*) un minore coinvolto in un comportamento sessuale esplicito; *b*) un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito; *c*) immagini realistiche raffiguranti un minore coinvolto in un comportamento sessuale esplicito.

3. Ai fini del Paragrafo 2. di cui sopra, il termine « minore » include tutte le persone sotto i 18 anni di età. Una Parte può comunque richiedere un età minore, che non potrà essere inferiore ai 16 anni.

4. Ogni Parte può riservarsi il diritto di non applicare in tutto o in parte il paragrafo 1., sottoparagrafi *d*) ed *e*), e 2, sottoparagrafi *b*) e *c*).

[56] In tema di associazione per delinquere finalizzata allo scambio di materiale pedopornografico, sussiste l'elemento oggettivo della fattispecie nel caso in cui sussista una « comunità virtuale in internet », stabile ed organizzata, regolata dalle disposizioni dettate dal promotore e gestore, volta allo scambio ed alla divulgazione, tra gli attuali membri ed i futuri aderenti, di foto pedopornografiche di bambini di età minore e sussiste l'elemento soggettivo, nel fatto che tutti gli aderenti al « *consortium sceleris* » siano stati resi edotti dello scopo e delle finalità del gruppo, consistenti nello scambio virtuale di immagini pedoponografiche, condizione per l'ammissione alla comunità virtuale, unitamente all'impegno di inviare periodicamente altre foto pedopornografiche. Così il luogo di consumazione del reato coincide con il luogo nel quale è stato digitato il comando di invio delle foto per via internet. Tale momento corrisponde, infatti, al momento di perfezionamento della fattispecie, ossia all'immissione nella rete del materiale fotografico illecito, a disposizione dei potenziali destinatari (Sez. 3, Sentenza n. 8296 del 2 dicembre 2004).

nessione concretamente adoperate, specie al fine di dissimulare la reale attività posta in essere ovvero per sviare i controlli.

Sempre in relazione al delitto di detenzione di materiale pedopornografico, i risultati delle intercettazioni disposte in un diverso procedimento sono utilizzabili nell'ambito delle indagini preliminari, al fine di acquisire ulteriori fonti probatorie mediante una perquisizione ed il relativo sequestro del materiale[57]. Ed ancora si è sottolineata l'importanza del controllo giurisdizionale sulle attività di polizia giudiziaria on line nell'ambito di azioni (telematiche) sotto copertura[58] e la rilevanza, ai fini della configurabilità del reato di attività comunicative svolte in forma condivisa, anche mediante spazi gestiti nelle forme di accesso condizionato riservato a soli utenti abilitati e non aperto al pubblico indeterminato[59]. Entro questa coerente linea interpretativa sono stati riconosciuti rilevanti al fine della commissione del reato tanto i sistemi di condivisione « p2p » (*peer to peer*)[60] che i pagamenti effettuati intenzio-

[57] In tal caso, il sequestro risulta legittimo anche se i decreti emessi dal P.M. siano stati adottati ipotizzando la fattispecie criminosa di cui all'art. 600-*ter* c.p., diversa da quella per la quale l'indagato è sottoposto ad indagini (art. 604-*quater* c.p.), trattandosi di cose obiettivamente sequestrabili e soggette a confisca obbligatoria, con conseguente applicazione del principio « *male captum bene retentum* » (Sez. 3, Sentenza n. 41957 del 19 ottobre 2005).

[58] L'attività di contrasto attraverso un agente provocatore non può essere espletata per accertare elementi di prova in ordine al reato di detenzione di materiale pedopornografico, sì che gli elementi di prova così acquisiti sono inutilizzabili e tale inutilizzabilità è rilevabile in ogni stato e grado del procedimento, anche durante la fase delle indagini preliminari. Di conseguenza, l'eventuale sequestro probatorio del materiale pedopornografico è illegittimo in quanto non si può affermare la sussistenza del « fumus delicti » in base ad un risultato investigativo inutilizzabile. Nel caso di specie, la polizia giudiziaria di propria iniziativa, e senza la preventiva autorizzazione dell'autorità giudiziaria, aveva svolto attività di contrasto sotto copertura, stipulando un contratto di accesso ed iscrizione ad un sito pedopornografico, procurandosi in tal modo alcune immagini pedopornografiche commercializzate nella rete informatica (Sez. 3, Sentenza n. 13500 del 28 gennaio 2005).

[59] Commette così il delitto di divulgazione via internet di materiale pedo-pornografico previsto dal comma terzo dell'art. 600-*ter* c.p. e non quello di mera cessione dello stesso, prevista al comma quarto del medesimo articolo, non solo chi utilizzi programmi di « file-sharing peer to peer », ma anche chi impieghi una « chat line », spazio virtuale strutturato in canali, nella quale un solo « nickname », necessario ad accedere alla cartella-immagini o video, venga utilizzato da più persone alle quali siano state rese note l'« username » e la « password », le quali possono in tal modo ricevere e trasmettere materiale pedo-pornografico; tale sistema rende possibile trasferire il materiale pedo-pornografico a molteplici destinatari e non si differenzia perciò dalla divulgazione vera e propria, sempre che risulti provata in capo all'agente la volontà alla divulgazione, come nel caso in cui la trasmissione sia stata reiteratamente rivolta a più persone (Sez. 3, Sentenza n. 593 del 7 dicembre 2006).

[60] Il delitto di distribuzione, divulgazione o pubblicizzazione di materiale pornografico realizzato mediante lo sfruttamento di minori degli anni diciotto sussiste quando il materiale sia propagato ad un numero indeterminato di destinatari, come avviene con l'inserimento nella rete internet mediante il modello di comunicazione « peer to peer » di filmati aventi come oggetto esibizioni pornografiche da parte di minori di anni 18 ed anche di anni 14 (Sez. 3, Sentenza n. 23164 del 8 giugno 2006). Ai fini dell'integrazione del reato di cui all'art. 600-*ter*, comma terzo, c.p., la condotta di divulgazione di materiale pedopornografico che avvenga in via automatica mediante l'utilizzo di appositi programmi di scaricamento da « internet », che ne consentano al tempo stesso la condi-

nalmente a siti di pornografia dai quali sia stato attinto il materiale rinvenuto non rilevando eventuali profili di errore[61] in ordine al materiale pornografico selezionato o scaricato.

Più di recente sembrano farsi strada più di recente profili di particolare valutazione critica sulle modalità di fruizione e di condivisione dei contenuti[62], non senza addentrarsi in difficoltose distinzioni sui profili tecnologici della intervenuta fruizione[63] e facendosi carico delle particolari difficoltà esistenti nella definizione e nella dimostrazione di consapevole detenzione di contenuti nei casi di sistemi di *file sharing*[64]. Quanto ai limiti degli accertamenti di polizia giudiziaria, sia pure nell'ambito della materia del contrasto alla porno pedofilia, la Corte sembra farsi carico della sensibilità della materia in rapporto alla complessità degli accertamenti, ma sopratutto in rapporto alla particolare sensibilità e ri-

visione con altri utenti (ad esempio il programma « eMule »), presuppone comunque che i « files » di cui si compone detto materiale siano interamente scaricati e visionabili nonché lasciati nella cartella dei « files » destinati alla condivisione (Sez. 3, Sentenza n. 11169 del 7 novembre 2008).

[61] Integra sempre il reato previsto dall'art. 600-*quater* c.p. (detenzione di materiale pornografico utilizzando minori degli anni diciotto), la condotta consistente nel procurarsi materiale pedopornografico « scaricato » (cosiddetta operazione di « download ») da un sito internet a pagamento, in quanto il comportamento di chi accede al sito e versa gli importi richiesti per procurarsi il materiale pedopornografico offende la libertà sessuale e individuale dei minori coinvolti come il comportamento di chi lo produce. La Corte, nell'enunciare il predetto principio, ha altresì dichiarato manifestamente infondata la questione di costituzionalità della norma sanzionatoria sollevata dalla difesa per presunta violazione degli artt. 2, 3, 24, 25, 27 e 111 Cost. (Sez. 3, Sentenza n. 41570 del 20 settembre 2007).

[62] In tema di pornografia minorile, la condotta di divulgazione e diffusione nella rete « Internet'di materiale pornografico presuppone la consapevole detenzione del materiale stesso. In tal caso è stata ritenuta involontaria la divulgazione e diffusione via internet di « files » pedopornografici compiute automaticamente dal programma di condivisione dati installato sul computer dell'indagato, in quanto tali « files » erano stati rinvenuti nella memoria « cache » e non all'interno di una cartella (Sez. 3, Sentenza n. 3194 del 16 ottobre 2008).

[63] Integrerebbe così il reato di detenzione di materiale pedopornografico (art. 600-*quater*, c.p.) anche la semplice visione di immagini pedopornografiche « scaricate » da un sito internet, poiché, per un tempo anche limitato alla sola visione, le immagini sono nella disponibilità dell'agente. Si trattava, tuttavia, di fatto commesso prima delle modifiche introdotte dalla legge 26 febbraio 2006, n. 38 ed integra tale fattispecie anche la cancellazione di « files » pedopornografici, già « scaricati » da internet, mediante l'allocazione nel « cestino » del sistema operativo del personal computer, in quanto gli stessi restano comunque disponibili mediante la semplice riattivazione dell'accesso al « file ». Secondo tale prospettiva solo per i « files » definitivamente cancellati può dirsi cessata la disponibilità e, quindi, la detenzione (Sez. 3, Sentenza n. 639 del 6 ottobre 2010).

[64] La condotta di chi detenga consapevolmente materiale pedopornografico, dopo esserselo procurato (art. 600-*quater* c.p.), configura un'ipotesi di reato commissivo permanente, la cui consumazione inizia con il procacciamento del materiale e si protrae per tutto il tempo in cui permane in capo all'agente la disponibilità del materiale (Sez. 3, Sentenza n. 22043 del 21 aprile 2010). In tema di pornografia minorile, la sussistenza dell'elemento soggettivo del reato di divulgazione di materiale pedopornografico, implica la volontà consapevole di divulgare o diffondere lo stesso. La Corte, in applicazione di tale principio, ha infatti precisato che l'utilizzo, per lo scaricamento di « files » da « Internet », di un determinato tipo di programma di condivisione (file sharing), quale « Emule » o simili, non è sufficiente di per sé a far ritenere provata la volontà altresì di diffusione del materiale (Sez. 3, Sentenza n. 11082 del 12 gennaio 2010).

servatezza delle informazioni acquisibili mediante un uso indiscriminato degli strumenti investigativi[65].

È in materia di tutela del diritto d'autore in rete che emergono, per la prima volta, linee apparentemente contrastanti che però sembrano ricomporsi in un quadro funzionale. Così è stato ritenuto in via di principio configurabile il concorso nel reato di abusiva diffusione, a titolo di concorso nel reato, mediante internet, di contenuti protetti nel caso di siti « *web* », attraverso i quali erano state illecitamente trasmesse in diretta « *streaming-video* » partite del campionato di calcio italiano, mediante connessione ad emittenti cinesi che, acquistato il diritto di diffonderle localmente dal titolare dell'esclusiva[66] e nel caso di diffusione di informazioni volte a consentire comunque lo scambio veicolato di contenuti protetti[67], sembra tuttavia poter essere esclusa, invece la rilevanza penale di condotte di violazione della proprietà intellettuale via *web* non sia stata determinata da fini di lucro, emergendo l'assenza di vantaggio economico o l'assenza di attività concretamente organizzate per la violazione sistematica dei diritti protetti[68]. È

[65] Non necessita dell'autorizzazione dell'Autorità giudiziaria di cui all'art. 14 L. n. 269 del 1998, l'attività di polizia giudiziaria consistente esclusivamente nell'accesso, visione e « download » di « file » aventi contenuto pedopornografico mediante l'uso di un programma di condivisione (nella specie, il programma denominato « Winmx ») (Sez. 3, Sentenza n. 41743 del 6 ottobre 2009). In materia di attività di polizia giudiziaria diretta alla repressione dei delitti di pornografia, non costituisce « attività di contrasto », soggetta ad autorizzazione dell'autorità giudiziaria, l'attività di accertamento di intercorsa connessione tra un indirizzo IP ed un sito Internet al fine di verificare l'operato acquisto di materiale pedopornografico (Sez. 3, Sentenza n. 29616 del 8 luglio 2010).

[66] È configurabile il concorso nel reato di abusiva diffusione, mediante internet, di immagini protette da diritto di esclusiva anche in capo al soggetto che, pur non avendole immesse in rete, abbia inoltrato sul web, in epoca antecedente alla loro immissione ad opera di altri, informazioni sui collegamenti e sui programmi necessari alla loro visione, in tal modo agevolando la connessione e la loro indebita diffusione. Si trattava di sequestro preventivo di due portali « web », attraverso i quali erano state illecitamente trasmesse in diretta via internet partite del campionato di calcio italiano, mediante connessione ad emittenti cinesi che, acquistato il diritto di diffonderle localmente dal titolare dell'esclusiva, avevano ritenuto di immettere in rete la trasmissione degli eventi sportivi (Sez. 3, Sentenza n. 33945 del 4 luglio 2006).

[67] Concorre nel reato di diffusione mediante la rete Internet di un'opera dell'ingegno protetta dal diritto d'autore (art. 171-*ter*, comma secondo, lett. *a-bis*) il titolare del sito web che, portando a conoscenza degli utenti le « chiavi di accesso » e le informazioni in ordine alla reperibilità, in tutto o in parte, dell'opera, consente agli stessi lo scambio dei files relativi mediante il sistema di comunicazione « peer to peer » (Sez. 3, Sentenza n. 49437 del 29 settembre 2009). Rientrano, infine, nella fattispecie penale prevista dall'art. 171-*ter*, comma primo, lett. *f-bis*), L. 22 aprile 1941, n. 633, tutti i congegni principalmente finalizzati a rendere possibile l'elusione delle misure tecnologiche di protezione apposte su materiali od opere protette dal diritto d'autore, non richiedendo la norma incriminatrice la loro diretta apposizione sulle opere o sui materiali tutelati. Si trattava in tal caso di sequestro di dispositivi che consentivano l'utilizzazione, su « consolle » videoludiche di differenti marche, di videogiochi illecitamente duplicati o scaricati abusivamente da internet (Sez. 3, Sentenza n. 23765 del 11 maggio 2010).

[68] Ad esempio escludendo la sanzionabilità penale di condotte consistite nalla predisposizione di server FTP a accesso riservato a singoli utenti, Per fine di lucro, secondo la S.C. deve cioè intendersi un fine di guadagno economicamente apprezzabile o di incremento patrimoniale da parte del-

nella materia della tutela on line della proprietà intellettuale, del resto, che il conflitto tra soggetti produttori di contenuti e soggetti che gestiscono servizi interattivi assume toni esasperati di vero e proprio conflitto, e la giurisprudenza rivela i suoi limiti nel definire soglie di punibilità che apparentemente si pongono in conflitto con le più elementari esigenze informative, e per converso l'evoluzione tecnologica e la stessa condivisione dei contenuti viene a rappresentare — o meglio spesso ad essere rappresentata — come occasione di sostanziale svuotamento delle posizioni giuridiche tutelate.

Sulle modalità di accesso alla rete da postazioni commercialmente organizzate a tal fine (c.d. « *Internet point* ») la Corte ha avuto modo di affermare la esigenza di specifica regolamentazione amministrativa volta appunto a prevenire abusi derivanti da un accesso incontrollato[69] pur affermando la particolare problematicità di configurare un concorso nel reato commesso in rete ad opera del gestore[70].

Sulla configurabilità di condotte criminose (tipicamente di accesso abusivo) rispetto a sistemi telematici pubblici o di interesse pubblico, quale quello bancario sembrano invece emergere posizioni diversificate, da un lato tendenti a qualificare l'installazione di apparati per intercettazione di comunicazioni intercorrenti tra i sistemi per finalità fraudolente (c.d. *skimmer*) come reato di pericolo[71] e dall'altro affermando l'esigenza di puntualizzare nei casi

l'autore del fatto, che non può identificarsi con un qualsiasi vantaggio di altro genere. Né l'incremento patrimoniale può automaticamente identificarsi con il mero risparmio di spesa derivante dall'uso di copie non autorizzate di programmi o altre opere dell'ingegno, al di fuori dello svolgimento di una attività economica da parte dell'autore del fatto (Sez. 3, Sentenza n. 33945 del 4 luglio 2006).

[69] È sottoposto alla licenza del questore di cui all'art. 7 D.L. 27 luglio 2005, n. 144, convertito con modifiche nella legge 31 luglio 2005, n. 155, l'esercizio nel quale venga offerto al pubblico il collegamento a reti telematiche mediante la messa a disposizione di apparecchi terminali idonei all'accesso diretto alla rete pubblica, dovendosi intendere per tali anche le postazioni telefoniche atte a garantire una connessione telematica mediante il collegamento di apparecchiature non fornite dall'esercente (Sez. 1, Sentenza n. 45102 del 16 novembre 2010).

[70] Non sussiste la responsabilità del gestore di un punto internet (cosiddetto « internet point ») a titolo di diffamazione per non avere impedito l'evento (art. 40, comma secondo, e 595 c.p.) qualora l'utente invii una e-mail avente contenuto diffamatorio, in quanto il gestore non solo non ha alcun potere di controllo e, quindi, alcuna conoscenza sul contenuto della posta elettronica inviata, ma gli è addirittura impedito di prenderne contezza — *ex* art. 617-*quater* c.p. che vieta l'intercettazione fraudolenta di sistemi informatici e telematici — mentre ha l'obbligo di identificare gli utenti che facciano uso del terminale ai soli fini della prova dell'utilizzazione e non per impedire l'eventuale reato (Sez. 5, Sentenza n. 6046 del 11 novembre 2008).

[71] Integra il reato installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.) la condotta di colui che installi, all'interno del sistema bancomat di un'agenzia di banca, uno scanner per bande magnetiche con batteria autonoma di alimentazione e microchip per la raccolta e la memorizzazione dei dati, al fine di intercettare comunicazioni relative al sistema informatico. trattandosi di reato di pericolo, non è necessario accertare, ai fini della sua con-

di accesso abusivo in rete il carattere obiettivamente proprio del sistema interessato[72]. Per altro verso si ricorre alle tradizionali categorie quando l'ipotesi di reato appare complessa e quando, pur nella certezza della rilevanza penale dell'attività criminosa accertata la condotta « informatica » si salda in senso funzionale con altre fattispecie penali, che in un certo senso ne costituiscono la premessa logica[73].

Proprio in tema di accesso abusivo a sistemi informatici[74], tema forse non immediatamente coinvolto nelle tematiche oggetto della presente trattazione, ma certamente rilevante e centrale in tema di diritto penale dell'informatica emergono due linee contrastanti

sumazione, che i dati siano effettivamente raccolti e memorizzati (Sez. 5, Sentenza n. 36601 del 9 luglio 2010). Integra il delitto di cui all'art. 617-*quinquies* c.p. la condotta di colui che installa abusivamente apparecchiature atte ad intercettare comunicazioni relative ad un sistema informatico posizionando nel « postamat »di un ufficio postale una fotocamera digitale, considerato che l'intercettazione implica l'inserimento nelle comunicazioni riservate, traendo indebita conoscenza delle stesse (Sez. 5, Sentenza n. 3252 del 5 dicembre 2006).

[72] In tema di accesso abusivo ad un sistema informatico o telematico, ai fini della configurabilità della circostanza aggravante dell'essere il sistema di interesse pubblico non è sufficiente la qualità di concessionario di pubblico servizio rivestita dal titolare del sistema, dovendosi accertare se il sistema informatico o telematico si riferisca ad attività direttamente rivolta al soddisfacimento di bisogni generali della collettività. Nel caso di specie, relativo a gestore di rete di telefonia, la S.C. ha affermato la necessità di accertare se la condotta dell'imputato abbia riguardato la rete stessa ovvero la rete « parallela » predisposta per la gestione del credito (Sez. 5, Sentenza n. 1934 del 13 dicembre 2010).

Integra il delitto di abuso d'ufficio la condotta del pubblico dipendente di indebito uso del bene che non comporti la perdita dello stesso e la conseguente lesione patrimoniale a danno dell'avente diritto. Nella fattispecie, la Corte ha escluso la configurabilità del peculato, posto che il delitto era stato consumato da un pubblico dipendente che, a fini privati, usava il collegamento « a forfait » della P.A. a Internet — tariffa « flat » —, senza causare all'amministrazione un maggior costo e dunque senza che potesse configurarsi una condotta appropriativa (Sez. 6, Sentenza n. 31688 del 9 aprile 2008). Non integra né il delitto di peculato, né quello di abuso d'atti d'ufficio la condotta del pubblico funzionario che utilizzi per ragioni personali l'accesso ad internet del computer d'ufficio, qualora per il suo esercizio la P.A. abbia contratto un abbonamento a costo fisso (Sez. 6, Sentenza n. 41709 del 19 ottobre 2010).

[73] Così ad esempio risponde del reato di furto aggravato e non di appropriazione indebita, il dipendente di una banca che si impossessi, mediante movimentazioni effettuate con i terminali dell'ufficio, di somme di danaro di clienti depositate in conti correnti. Nell'affermare tale principio, la Corte ha altresì escluso che tale condotta sia sussumibile nella fattispecie di cui all'art. 640-*ter* c.p., quando le operazioni di spostamento del denaro siano effettuate attraverso operazioni ordinarie sul sistema informatico della banca (Sez. 6, Sentenza n. 32543 del 10 maggio 2007). In realtà già da tempo la S.C. aveva affermato la non sovrapponibilità del reato di accesso abusivo e di frode informatica ammettendone il concorso perché si tratta di reati diversi: la frode informatica postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del reato di accesso abusivo che, invece, può essere commesso solo con riferimento a sistemi protetti, requisito non richiesto per la frode informatica (Sez. 5, Sentenza n. 2672 del 19 dicembre 2003).

[74] Cfr. diffusamente Aronica G., *L'accesso abusivo ad un sistema informatico o telematico (art. 615-*ter *c.p.) nella giurisprudenza*, in *Indice Penale*, 2010, p. 199 e Civardi S., *La distinzione fra accesso abusivo a sistema informatico e abuso dei dati acquisiti*, in questa *Rivista*, 2009, p. 58; Gentiloni Silveri A., *L'accesso abusivo a sistema informatico da parte di funzionari pubblici: non c'è reato se i dati non sono riservati?*, in questa *Rivista*, 2008, p. 367.

nella giurisprudenza di legittimità, da una parte si configura il reato di accesso abusivo in relazione alle oggettive circostanze attraverso le quali l'operatore, pur abilitato interviene senza titolo e intromettendosi in spazi comunicativi organizzati ed esclusivi privo di autorizzazione espressa del titolare[75], dall'altra invece si sottolinea come vada qualificata tale fattispecie solo in presenza di una abusività dell'accesso in senso oggettivo con riferimento al momento dell'accesso ed alle finalità concrete dell'utente abilitato

[75] Ai fini della configurabilità del reato di accesso abusivo a un sistema informatico, la qualificazione di abusività va intesa in senso oggettivo, con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza apprestate dal titolare dello « ius excludendi », al fine di impedire accessi indiscriminati, a nulla rilevando le finalità che si propone l'autore e l'uso successivo dei dati, che, se illeciti, possono integrare un diverso titolo di reato (Sez. 5, Sentenza n. 40078 del 25 giugno 2009). Non commette il reato di accesso abusivo ad un sistema informatico o telematico il soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga per acquisire informazioni per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente configurabili, ove le suddette finalità vengano poi effettivamente realizzate. (Fattispecie in cui è stato contestato il concorso nel delitto di abusiva introduzione nel sistema informatico del C.E.D. della Corte di Cassazione da parte di ignoti pubblici ufficiali, i quali avrebbero fornito all'indagato, addetto alla cancelleria della Corte, informazioni riservate sullo stato di alcuni procedimenti pendenti, al fine di avvantaggiare la posizione processuale o detentiva di taluni imputati (Sez. 6, Sentenza n. 39290 del 8 ottobre 2008). Integra così accesso abusivo ad un sistema informatico o telematico la condotta del soggetto che, pur avendo titolo per accedere al sistema, vi si introduca con la « *password* » di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell'archivio informatico, in quanto l'art. 615-*ter* c.p. non punisce soltanto l'accesso abusivo ad un sistema informatico ma anche la condotta di chi vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo (Sez. 5, Sentenza n. 2987 del 10 dicembre 2009); Integra il reato di accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.) la condotta del soggetto che, avendo titolo per accedere al sistema, vi si introduca con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell'archivio informatico.. Si trattava di indebita acquisizione, con la complicità di appartenenti alla polizia di Stato, di notizie riservate tratte dalla banca dati del sistema telematico di informazione interforze del Ministero dell'Interno, per l'utilizzo in attività di investigazione privata, in agenzie facenti capo agli stessi indagati o nelle quali essi prestavano la loro attività (Sez. 5, Sentenza n. 18006 del 13 febbraio 2009); Il delitto di accesso abusivo ad un sistema informatico può concorrere con quello di frode informatica, diversi essendo i beni giuridici tutelati e le condotte sanzionate, in quanto il primo tutela il domicilio informatico sotto il profilo dello « ius excludendi alios », anche in relazione alle modalità che regolano l'accesso dei soggetti eventualmente abilitati, mentre il secondo contempla l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto. In applicazione di questo principio la S.C. ha ritenuto immune da censure la decisione con cui il giudice di appello ha ritenuto il concorso tra i due reati nei confronti dell'imputato che, in qualità di dipendente dell'Agenzia delle entrate, agendo in concorso con altri dipendenti nonché con commercialisti e consulenti tributari, si era abusivamente introdotto nel sistema informatico dell'amministrazione, inserendovi provvedimenti di sgravio fiscale illegittimi perché mai adottati in relazione a tributi già iscritti a ruolo per la riscossione coattiva, così alterando i dati contenuti nel sistema in modo tale da fare apparire insussistente il credito tributario dell'Erario nei confronti di numerosi contribuenti (Sez. 5, Sentenza n. 1727 del 30 settembre 2008); Commette il reato previsto dall'art. 615-*ter* c.p. (accesso abusivo ad un sistema informatico o telematico) il soggetto che, avendo titolo per accedere al sistema, lo utilizzi per finalità diverse da quelle consentite (Sez. 5, Sentenza n. 37322 del 8 luglio 2008).

che fa uso non autorizzato o improprio delle sue credenziali di accesso[76].

L'emersione di questo contrasto, destinato ad essere risolto da un intervento delle S.U. penali[77], non potrà che presagire ad ulteriori interventi interpretativi destinati a sottolineare o a enucleare, anziché gli aspetti soggettivi « formali » o le condotte conseguenti alla appropriazione delle informazioni o dei dati[78] — che sembrano in verità ancora indirettamente ispirati alle forme commissive del tradizionale delitto di violazione di domicilio[79] — pro-

[76] Ai fini della configurabilità del reato di accesso abusivo a un sistema informatico, la qualificazione di abusività va intesa in senso oggettivo, con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza apprestate dal titolare dello « ius excludendi », al fine di impedire accessi indiscriminati, a nulla rilevando le finalità che si propone l'autore e l'uso successivo dei dati, che, se illeciti, possono integrare un diverso titolo di reato (Sez. 5, Sentenza n. 40078 del 25 giugno 2009). Non commette il reato di accesso abusivo ad un sistema informatico o telematico il soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga per acquisire informazioni per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente configurabili, ove le suddette finalità vengano poi effettivamente realizzate. (Fattispecie in cui è stato contestato il concorso nel delitto di abusiva introduzione nel sistema informatico del C.E.D. della Corte di Cassazione da parte di ignoti pubblici ufficiali, i quali avrebbero fornito all'indagato, addetto alla cancelleria della Corte, informazioni riservate sullo stato di alcuni procedimenti pendenti, al fine di avvantaggiare la posizione processuale o detentiva di taluni imputati) (Sez. 6, Sentenza n. 39290 dell'8 ottobre 2008). Non integra il reato di accesso abusivo ad un sistema informatico (art. 615-*ter* c.p.) la condotta di coloro che, in qualità rispettivamente di ispettore della Polizia di Stato e di appartenente all'Arma dei Carabinieri, si introducano nel sistema denominato SDI (banca dati interforze degli organi di polizia), considerato che si tratta di soggetti autorizzati all'accesso e, in virtù del medesimo titolo, a prendere cognizione dei dati riservati contenuti nel sistema, anche se i dati acquisiti siano stati trasmessi a una agenzia investigativa, condotta quest'ultima ipoteticamente sanzionabile per altro e diverso titolo di reato. Nella fattispecie la Corte ha rilevato l'ininfluenza della circostanza che detto uso sia già previsto dall'agente all'atto dell'acquisizione e ne costituisca la motivazione esclusiva, in quanto la sussistenza della volontà contraria dell'avente diritto, cui fa riferimento l'art. 615-*ter* c.p., ai fini della configurabilità del reato, deve essere verificata solo ed esclusivamente con riguardo al risultato immediato della condotta posta in essere dall'agente con l'accesso al sistema informatico e con il mantenersi al suo interno e non con riferimento a fatti successivi che, anche se già previsti, potranno di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione da parte dell'agente (Cass., Sez. 5, Sentenza n. 2534 del 20 dicembre 2007) Non integra il reato di accesso abusivo ad un sistema informatico (art. 615-*ter* c.p.) — che ha per oggetto un sistema informatico protetto da misure di sicurezza e richiede che l'agente abbia neutralizzato tali misure — colui che, senza avere concorso nell'accesso abusivo e conseguente indebito trasferimento (cosiddetto trascinamento) della cartella contenente dati riservati del proprio datore di lavoro dall'area protetta alla cosiddetta area comune del sistema informatico, a cui possono accedere tutti i dipendenti, acceda all'area comune avvalendosi solo di dati e strumenti di cui sia legittimamente in possesso e prenda visione della cartella riservata trasferendola su un dischetto (Sez. 5, Sentenza n. 6459 del 4 dicembre 2006).

[77] Sez. V, Ord. 11714 dell'11 febbraio 2011.

[78] Così affermando, per esempio, come la duplicazione dei dati contenuti in un sistema informatico o telematico costituisce condotta tipica del reato previsto dall'art. 615-*ter* c.p., restando in esso assorbito il reato di appropriazione indebita (Sez. 5, Sentenza n. 37322 del 8 luglio 2008).

[79] Così espressamente Sez. 5, Sentenza n. 11689 del 6 febbraio 2007 che afferma come Il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la *violazione*

prio quei molteplici profili di connessione esistenti tra accesso abusivo e reati c.d. « satellite » con particolare riguardo alle effettive finalità informative e diffusive che all'accesso informatico o telematico abusivo si legano e che in un certo senso vi sono interagenti, in una prospettiva funzionale di trattamento illecito dei dati personali abusivamente ottenuti o estratti (art. 167 D.Lgs. n. 1996/2003 ove peraltro si riconnette alle operazioni di trattamento illecito anche la semplice « estrazione » ai sensi dell'art. 4 comma 1 lettera *a*)[80] ed alla utilizzabilità dei dati organizzati estratti per finalità fraudolente quali l'inoltro di messaggi ingannevoli e massivi di posta elettronica per indirizzare gli utenti verso siti « clone » (c.d. « *phishing* »)[81], fenomeno criminale fortemente in evoluzione *on line* nelle sue più varie forme.

È peraltro evidente che proprio in relazione alla definizione di accesso abusivo potrebbe rinvenirsi proprio nella Convenzione del 2001[82] un riferimento interpretativo fondamentale, poiché il contrasto giurisprudenziale non appare superabile altrimenti.

Dall'attenzione che la giurisprudenza di legittimità saprà ancora riservare alla rete ed alle sue complesse fenomenologie anche nel prossimo decennio dipende in buona parte anche la ricostruzione

del domicilio informatico, e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa. (Fattispecie in cui il reato è stato ravvisato nella condotta degli imputati, che si erano introdotti in una centrale Telecom ed avevano utilizzato apparecchi telefonici, opportunamente modificati, per allacciarsi a numerose linee di utenti, stabilendo, all'insaputa di costoro, contatti con utenze caratterizzate dal codice 899). Ed ancora ricorre al medesimo argomento nell'affermare che nel delitto di accesso abusivo ad un sistema informatico o telematico, la violazione dei dispositivi di protezione non assume rilevanza per sé, ma solo come eventuale manifestazione di una volontà contraria a quella di chi dispone legittimamente del sistema; l'art. 615-*ter* c.p., infatti, punisce, al comma 1, non solo chi abusivamente si introduce in tali sistemi, *ma anche chi vi si trattiene contro la volontà — esplicita o tacita — di colui che ha il diritto di escluderlo* (Sez. 5, Sentenza n. 12732 del 7 novembre 2000) proprio tale pronuncia richiama espressamente l'analogia con la violazione di domicilio.

[80] Nella nozione di « trattamento » rientra infatti qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

[81] Cfr. in merito il fondamentale lavoro di F. CAIANI, G. COSTABILE e G. MAZZARACO, *Phishing e furto d'identità digitale*, Padova 2008 nonché PERRI P., *Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing*, in *Ciberspazio e diritto*, 2008, p. 93.

[82] Ci si riferisce all'art. 2 della Convenzione di Budapest che Articolo 2 che detta la nozione di « Accesso illegale » al sistema informatico come l'accesso all'intero sistema informatico o a parte di esso senza autorizzazione. Ricomprendendo potenzialmente tanto l'ipotesi che il reato venga commesso violando misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico. E non appare senza influenza anche gli artt. 4, 5 e 6 che definiscono rispettivamente l'attentato all'integrità dei dati, del sistema informatico e l'utilizzazione abusiva di « apparati » tra cui vengono ricomprese anche le password.

— in chiave di sistematicità — di un quadro normativo complesso sia a livello nazionale che europeo ed internazionale.

Si tratta in definitiva di percepire e tradurre nel « diritto vivente » principi che non possono solo estrarsi (spesso in modo frammentato e disorganico) dalla tradizionale visione penalistica o dalla apparentemente rassicurante tradizione delle figure istituzionali esistenti. Dovendosi più che adattare fattispecie esistenti, o estendere, in chiave latamente analogica, metodologie formali di imputazione o di qualificazione di responsabilità, ricostruire sempre i fenomeni espressivi e comunicativi con cura e attenzione, cogliendone quello che è il senso e la portata anche in rapporto al contesto funzionale nel quale sono destinati effettivamente a ripercuotersi, cogliendo in definitiva non astrazioni ideali, seppure suggestive, ma l'espressione di una società « viva » nella rete e che della rete fa ogni giorno di più una sua articolazione essenziale e partecipativa. Di questa dimensione sono propri differenti spazi espressivi, differenti articolazioni e spazi di intervento e di controllo, differenti e innovativi modelli di diffusione di idee e di ricerca di contenuti, nel rispetto di valori di libertà e di garanzie essenziali e qualificanti che solo l'intervento giurisprudenziale può tradurre in beni giuridici ben definiti, così sciogliendone i nodi.