DIRITTO PENALE CONTEMPORANEO

IL LUOGO DI CONSUMAZIONE DEL DELITTO DI ACCESSO ABUSIVO A UN SISTEMA INFORMATICO O TELEMATICO: IN ATTESA DELLE SEZIONI UNITE

di Maurizio Bellacosa

Abstract. *Una recente ordinanza della Cassazione ha rimesso alle Sezioni Unite la questione del* locus commissi delicti *dell'accesso abusivo a un sistema informatico o telematico. Nel presente contributo si analizzano i diversi orientamenti interpretativi in argomento, per provare a fornire una risposta al quesito. La condotta tipica descritta nell'art. 615-ter c.p., letta alla luce delle peculiarità dei reati cibernetici, induce a ritenere che il reato si perfezioni nel momento e nel luogo in cui l'operatore abusivo digita alla tastiera del terminale periferico la serie di comandi necessari per acquisire le informazioni contenute nel sistema.*

SOMMARIO: 1. Le recenti pronunce in argomento della Corte di Cassazione. – 2. La fattispecie tipica del delitto *ex* art. 615-ter c.p. – 3. La condotta esecutiva di chi «si introduce» in un sistema informatico o telematico. – 4. I reati cibernetici e la crisi delle tradizionali categorie spazio-fisico-temporali. – 5. L'intrusione nel sistema informatico o telematico mediante la digitazione alla tastiera dei comandi necessari. – 6. L'esigenza processuale di perseguire il reato nel luogo in cui ha agito al computer l'autore della intrusione. – 7. L'ipotesi problematica in cui l'accesso abusivo sia realizzato dall'estero.

1. Le recenti pronunce in argomento della Corte di Cassazione.

La I Sezione penale della Corte di Cassazione, con l'ordinanza n. 52575/14[1] , resa a poco più di un anno di distanza dalla sentenza n. 40303/13[2], ha demandato alle

[1] Cass. pen., sez. I, ord. 28 ottobre 2014 (dep. 18 dicembre 2014), Pres. Siotto, Est. Locatelli, confl. comp. tra Trib. Napoli e Trib. Roma, pubblicata in *questa Rivista*, 20 gennaio 2015, con commento di P. DE MARTINO, *Rimessa alle Sezioni Unite una questione in tema di competenza territoriale del delitto di accesso abusivo ad un sistema informatico.*

[2] Cass. pen., sez. I, sent. 27 maggio 2013 (dep. 27 settembre 2013), Pres. Chieffi, Est. La Posta, confl. comp. tra GIP Roma e Trib. Firenze, pubblicata in *questa Rivista*, 11.10.2013, con commento di C. PECORELLA, *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico*; anche in *Riv. it. dir. proc. pen.*, 2014, p. 1502, con commento di C.F. GROSSO, *Su di un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*; nonché in *Cass. pen.*, 2014, p. 1704, con *Osservazioni* di S. ATERNO.

Sezioni Unite il quesito concernente la individuazione del momento e del luogo di consumazione – rilevante ai fini della competenza territoriale – del delitto di accesso abusivo a un sistema informatico o telematico (*ex* art. 615-ter c.p.[3]).

La chiamata in causa delle Sezioni Unite penali non appare come una scelta sorprendente, ma come una soluzione auspicata[4] e ragionevole. Invero, con la sentenza n. 40303/13 – relativa al caso di alcuni pubblici ufficiali che dal loro ufficio in Firenze si erano collegati alla banca dati riservata del Sistema d'informazione interforze del Ministero dell'Interno (c.d. SDI) – la Suprema Corte ha dapprima fissato il principio per il quale il *locus commissi delicti* "non è quello in cui vengono inseriti i dati idonei ad entrare nel sistema bensì quello dove materialmente è collocato il server che elabora e controlla le credenziali di autenticazione del cliente" ovvero in Roma, dove si trova il sistema centrale del Ministero. La stessa sentenza ha però suscitato nei commentatori notevoli perplessità, anche per la irragionevole conseguenza di dover sempre radicare la competenza territoriale per simili fatti nella città di Roma, laddove potrebbe risultare più complicato l'accertamento del reato, a causa della lontananza fisica dall'operatore abusivo[5].

Un'avvisaglia sul possibile cambio di indirizzo della Suprema Corte è poi intervenuta di recente, con la sentenza n. 34165/14[6]. In tale vicenda processuale, sempre concernente una ipotesi di accesso al sistema SDI del Ministero dell'Interno, ancora una volta il Giudice dell'udienza preliminare presso il Tribunale di Roma aveva sollevato il conflitto *ex* art. 28 c.p.p. con il Tribunale di Firenze, che aveva precedentemente dichiarato la propria incompetenza per ragioni di territorio. La Corte di Cassazione ha risolto il conflitto senza prendere espressamente posizione sulla individuazione del luogo di commissione del reato: ha infatti ravvisato la connessione (*ex* art. 12, co. 1, lett. a, c.p.p.) tra i fatti in questione e quelli già oggetto proprio della sentenza n. 40303/13, confermando così la già attribuita competenza del Tribunale di Roma. Nell'ambito della motivazione della sentenza in questione, la Suprema Corte ha però messo in luce la problematicità del tema, con affermazioni che preludevano a una nuova presa di posizione sull'argomento. Invero, in un passaggio cruciale della motivazione, i Giudici della Suprema Corte hanno riconosciuto "che, in astratto, le

---

[3] Art. 615-ter c.p. (introdotto dall'art. 4 della legge 23 dicembre 1993, n. 547): «Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni».

[4] L'intervento in argomento delle Sezioni Unite è stato auspicato da C.F. GROSSO, *Su di un'interessante controversia interpretativa*, cit., p. 1521.

[5] Cfr. C. PECORELLA, *La Cassazione sulla competenza territoriale*, cit., la quale evidenzia "l'incongruenza di una regola che porta a concentrare in un unico luogo tutti i procedimenti per accesso abusivo a uno stesso sistema informatico, indipendentemente dal luogo in cui si trovi il computer utilizzato per realizzare l'intrusione, e senza che quella concentrazione possa dirsi di regola funzionale ad una migliore repressione di episodi fra loro collegati, in quanto espressione di un disegno criminoso comune".

[6] Cass. pen., sez. I, ud. 15 luglio 2014 (dep. 1° agosto 2014), Pres. Vecchio, Rel. Di Tomassi, ric. Del Bo, in *Riv. it. dir. proc. pen*., 2014, p. 1503, con commento di C.F. GROSSO, *Su di un'interessante controversia interpretativa*, cit.

osservazioni del pubblico ministero che ha sollecitato il conflitto e del giudice che l'ha sollevato, così come quelle delle parti intervenute, hanno il pregio di sviscerare con maestria argomenti scientifici e giuridici, dibattuti sia in giurisprudenza sia in dottrina, meritevoli di attento vaglio critico, attesa la rilevanza delle questioni agitate e la ricordata incidenza su procedimenti che risultano svolti in ambiti territoriali diversi".

Il rinvio sembrava riguardare, in particolare, le osservazioni svolte dal GUP del Tribunale di Roma (Dott.ssa d'Alessandro) nella ordinanza del 16 aprile 2014[7], secondo cui: "Il delitto di accesso abusivo in un sistema informatico o telematico si consuma nel luogo in cui viene digitato il tasto d'ingresso nel sistema informatico e, pertanto, nella sede periferica del sistema presso la quale tale condotta è compiuta. L'introduzione avviene infatti nelle singole sedi periferiche e s'inserisce contestualmente nel sistema informatico centrale; tutto è contestualmente presente in tutti gli ambiti in cui il sistema opera (la banca dati centrale: come le sedi periferiche), non esistendo una ripartizione spaziale poiché si versa in un cyberspazio delocalizzato, in una rete di comunicazione telematica. L'unica cosa collocabile – secondo i parametri del mondo fisico, ben diverso da quello informatico – è la condotta umana, che finisce nelle sedi locali, con contegni non più arginabili negli esiti, e contestualmente produce modifiche nel sistema centrale. E' del tutto erroneo scindere il server, e definirlo nel caso di specie romano, poiché il sistema è un unicum che si alimenta di continue allegazioni e acquisizioni di dati contestualmente ovunque presenti. Luogo del commesso reato e giudice competente per territorio sono pertanto il luogo in cui viene digitato il tasto di accesso al sistema informatico ed il giudice competente su quel luogo".

Tali considerazioni, in radicale contrasto con le conclusioni della citata sentenza n. 40303/13, hanno fatto presa su un altro Collegio della stessa Sezione I penale della Corte di Cassazione, che, nel demandare alle Sezioni Unite la soluzione del quesito, ha ora affermato (ordinanza n. 52575/14): "Poiché il reato si perfeziona con l'introduzione abusiva nel sistema, a prescindere dalla effettiva acquisizione dei dati riservati in esso contenuti, si deve ritenere che la condotta materiale si perfeziona nel luogo fisico e nel momento in cui l'agente si introduce abusivamente nella postazione locale (nel caso in esame nel computer ubicato presso la sede della Motorizzazione Civile di Napoli), la quale non è un mero mezzo di accesso ma, al pari del computer denominato server ubicato presso la sede centrale, un componente informatico essenziale costituente articolazione territoriale del complessivo sistema informatico nazionale nella disponibilità del Ministero dei Trasporti".

In attesa dell'intervento delle Sezioni Unite, si possono ripercorrere i termini della questione e svolgere alcune riflessioni critiche in argomento.

---

[7] GUP Trib. Roma (Giudice d'Alessandro), ord. 16 aprile 2014, in *Riv. it. dir. proc. pen.*, 2014, p. 1502, con commento di C.F. GROSSO, *Su di un'interessante controversia interpretativa*, cit.; nonché in *Dir. inf.*, 2014, p. 945, con commento di R. ZANNOTTI, *Accesso abusivo ad un sistema telematico: quale il* locus commissi delicti?

2. La fattispecie tipica del delitto *ex* art. 615-ter c.p.

La fattispecie *ex* art. 615-ter c.p. sanziona due condotte tipiche: a) l'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza; b) il mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione. Come precisato dalle Sezioni Unite penali della Corte di Cassazione, a cavallo tra il 2011 e il 2012, integra il delitto in esame anche "la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema"[8].

La condotta incriminata è solo quella virtuale o elettronica, in quanto l'art. 615-ter c.p. fa riferimento all'accesso realizzato per via informatica o telematica e non all'ingresso fisico o materiale nei locali ove si trova il sistema da violare[9].

La figura criminosa in esame delinea un reato di mera condotta[10], di pericolo[11] e istantaneo[12], che si consuma al momento della introduzione *invito domino* in un sistema informatico o telematico protetto da misure di sicurezza ovvero allorquando sia scaduto il termine previsto per uscire dal sistema e il reo invece lì permanga, contro la volontà (espressa o tacita) del titolare dello *ius excludendi*.

L'accesso abusivo può avvenire sia "da vicino" ovvero mediante il contatto diretto del soggetto agente con la postazione di lavoro del sistema informatico altrui, sia "a distanza" ovvero attraverso un altro sistema informatico collegato per via

---

[8] Così Cass. pen., Sez. un., sent. 27 ottobre 2011 (dep. 7 febbraio 2012), Pres. Lupo, Rel. Fiale, ric. C., pubblicata in *questa Rivista*, 10.02.2012, con commento di G. ROMEO, *Le Sezioni unite sull'accesso a un sistema informatico o telematico*, nonché commentata da R. FLOR, *Verso una rivalutazione dell'art. 615 ter c.p.?*, in *Dir. pen. cont. – Riv. trim.*, n. 2, 2012, p. 126, e da R. BARTOLI, *L'accesso abusivo a un sistema informatico (art. 615 ter c.p.) a un bivio ermeneutico teleologicamente orientato*, in *Dir. pen. cont. – Riv. trim.*, n. 1, 2012, p. 123; anche in *Cass. pen.*, 2012, p. 3681, con commento di C. PECORELLA, *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*; e in *Riv. trim. dir. pen. ec.*, 2012, p. 369, con commento di I. SALVADORI, *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615* ter *c.p.*

[9] In tal senso, v. G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, p. 40; ID., *La disciplina penale degli illeciti in materia di tecnologie informatiche*, in *Riv. pen. ec.*, 1995, p. 403; G. FIANDACA-E. MUSCO, *Diritto penale. Parte speciale. I delitti contro la persona*, III ed., Bologna, 2011, p. 283; L. CUOMO, *La tutela penale del domicilio informatico*, in *Cass. pen.*, 2000, p. 3000; S. MARANI, *I delitti contro la persona*, Padova, 2007, p. 618.

[10] Cfr. Cass. pen., sez. V, sent. 6 febbraio 2007 n. 11689, ric. Cerbone, in *C.E.D.*, n. 236221.

[11] Si vedano R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo* jus excludendi alios, in *Dir. pen. proc.*, 2005, p. 88; L. CUOMO, *op. ult. loc.* cit.; S. MARANI, *I delitti contro la persona*, cit., p. 621; S. DE FLAMMINEIS, *Art. 615-*ter *c.p.: accesso legittimo ma per finalità estranee ad un sistema informatico*, in *Cass. pen.*, 2011, p. 2211; *contra*, S. ATERNO, *Sull'accesso abusivo a un sistema informatico o telematico*, in *Cass. pen.*, 2000, p. 2996, per il quale si tratta di un reato di danno.

[12] Cfr. F. ANTOLISEI, *Manuale di diritto penale. Parte speciale*, vol. I, XV ed., a cura di C.F. Grosso, Milano, 2008, p. 247; S. MARANI, *op. ult. loc. cit*.

telematica a quello cui si accede[13]. Proprio l'azione abusiva posta in essere con il collegamento a distanza dà vita al problematico quesito della individuazione del *locus commissi delicti*.

3. La condotta esecutiva di chi «si introduce» in un sistema informatico o telematico.

Nella sentenza n. 40303/13, la Corte di Cassazione ha ritenuto che l'accesso avvenga "nel luogo in cui viene effettivamente superata la protezione informatica e vi è l'introduzione nel sistema e, quindi, là dove è materialmente situato il sistema informatico (*server*) violato, l'elaboratore che controlla le credenziali di autenticazione del *client*", in quanto la "procedura di accesso deve ritenersi atto prodromico alla introduzione nel sistema che avviene solo nel momento in cui si entra effettivamente nel *server* dopo avere completato la validazione delle credenziali dell'utente"; in altre parole, "nell'ipotesi di accesso da remoto", "l'utente invia le credenziali al *server web* il quale le riceve «processandole» nella fase di validazione che è eseguita solo ed unicamente all'interno del sistema protetto e non potrebbe essere diversamente proprio per motivi di sicurezza del sistema stesso"[14].

Tali conclusioni, per quanto a prima vista plausibili, risultano – a una più approfondita analisi – non pienamente in linea con il moderno manifestarsi dei fenomeni informatici e telematici e sembrano discendere da una lettura per così dire "tradizionale" della impropria terminologia adoperata nell'art. 615-ter c.p.[15].

Invero, da tale ultimo punto di vista, la figura criminosa di accesso abusivo a un sistema informatico o telematico sconta un "difetto di origine" per essere stata eccessivamente modellata sulla fattispecie di violazione di domicilio (*ex* art. 614 c.p.[16]): così, la condotta di "accesso", che compare nella rubrica dell'art. 615-ter e che è sicuramente appropriata secondo il gergo tecnico-informatico, è stata tradotta *in primis* nel fatto di chi «si introduce» (in un sistema informatico o telematico), utilizzando in tal modo una locuzione che può risultare fuorviante per l'interprete, alludendo al passaggio fisico di chi varchi il confine spaziale di un luogo materiale[17]. Invece,

---

[13] Cfr. G. PICA, *La disciplina penale degli illeciti*, cit., p. 404; C. PECORELLA, *Il diritto penale dell'informatica*, Padova, 2000, p. 308; R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico*, cit., p. 91; G. FIANDACA-E. MUSCO, *op. ult. loc. cit.*; L. CUOMO, *op. ult. loc. cit*.

[14] Così Cass. pen., sez. I, sent. 27 maggio 2013 (dep. 27 settembre 2013), cit.

[15] Cfr. C.F. GROSSO, *Su di un'interessante controversia interpretativa*, cit., p. 1519; R. ZANNOTTI, *Accesso abusivo ad un sistema telematico,* cit., p. 949.

[16] Art. 614 c.p. - Violazione di domicilio: «Chiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione da sei mesi a tre anni.

Alla stessa pena soggiace chi si trattiene nei detti luoghi contro l'espressa volontà di chi ha diritto di escluderlo, ovvero vi si trattiene clandestinamente o con inganno».

[17] Cfr. F. PAZIENZA, *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Riv. it. dir. proc. pen*., 1995, p. 755; M. NUNZIATA, *La prima applicazione giurisprudenziale del delitto di "accesso abusivo ad*

l'intrusione in un sistema informatico o telematico va inteso in termini diversi rispetto ai tradizionali parametri fisico-spaziali.

D'altronde, l'oggetto di tutela della figura criminosa in esame non attiene alla c.d. pace domestica da godere nei luoghi di privata dimora, bensì al c.d. domicilio informatico, inteso come estensione virtuale del soggetto titolare di un sistema informatico[18], nella quale assicurare la protezione della riservatezza dei dati e dei programmi contenuti in un sistema informatico o telematico[19]. Peraltro, una parte della recente dottrina ritiene di allargare l'ambito del bene protetto del delitto *ex* art. 615 ter c.p. anche alla integrità dei dati e dei programmi informatici, nonché alla sicurezza delle comunicazioni informatiche[20].

4. I reati cibernetici e la crisi delle tradizionali categorie spazio-fisico-temporali.

In termini generali, i reati informatici (*computer crimes*) presentano elementi di tipizzazione, descrittivi di modalità, oggetti o attività, caratterizzati dalla tecnologia informatica, con la inevitabile conseguenza che l'azione penalmente rilevante va correttamente inquadrata secondo le peculiarità tecniche di procedure, elaborazioni e componenti informatiche[21].

L'esigenza di adattare l'interpretazione di tali nuove figure criminose alla loro dimensione tecnologica si è accentuata con il "passaggio epocale" – storicamente

---

un sistema informatico" ex art. 615 ter c.p., in *Giur. merito*, 1998, p. 709; I. SALVADORI, *Quando un* insider *accede*, cit., p. 376; R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico*, cit., p. 87.

[18] Nella relazione al disegno di legge (Camera dei Deputati, XI Legislatura, disegno di legge n. 2773), poi confluito nella legge n. 547/1993, si rappresenta che il sistema informatico o telematico costituisce "un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione".

[19] Cfr. G. FIANDACA-E. MUSCO, *op. ult. loc. cit.*; G.L. GATTA, *Delitti contro l'inviolabilità del domicilio*, in AA.VV., *Reati contro la persona e contro il patrimonio*, a cura di F. Viganò e C. Piergallini, Torino, 2011, p. 269; C. PECORELLA, *Il diritto penale dell'informatica*, cit., p. 322; P. GALDIERI, *La tutela penale del domicilio informatico*, in AA.VV., *Problemi giuridici dell'informatica nel MEC*, a cura di P. Galdieri, Milano, 1996, pp. 189 ss.; S. MARANI, *I delitti contro la persona*, cit., p. 613.

[20] Si vedano L. PICOTTI, *Sistematica dei reati informatici*, in AA. VV, *Il diritto penale dell'informatica nell'epoca di Internet*, a cura di L. Picotti, Padova, 2004, p. 76; ID., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in AA.VV., *Tutela penale della persona e nuove tecnologie*, a cura di L. Picotti, Padova, 2013, pp. 58 ss.; R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico*, cit., pp. 86 ss.; ID., *Art. 615* ter *c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. pen. proc.*, 2008, p. 110; ID., *Verso una rivalutazione dell'art. 615 ter c.p.?*, cit., pp. 135 ss.; I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in AA.VV., *Tutela penale della persona e nuove tecnologie*, cit., pp. 149 ss.; *contra*, v. C. PECORELLA, *L'attesa pronuncia delle Sezioni Unite*, cit. p. 3696, per la quale "l'ampliamento dell'ambito di applicazione dell'art. 615-*ter* c.p., in funzione della tutela di interessi diversi dalla riservatezza del contenuto di sistemi informatici protetti, non pare persuasivo né giustificabile alla luce del principio di proporzione".

[21] Cfr. L. PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec.*, 2011, pp. 844-845; ID., *Sistematica dei reati informatici*, cit., p. 89; I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico*, cit., p. 127.

collocabile negli anni '90 del secolo scorso – dovuto alla diffusione della rete Internet. Sul versante penalistico, alla commissione dei reati informatici hanno così fatto seguito le manifestazioni dei reati telematici, poi comunemente denominati "cibernetici" (*cybercrimes*)[22], realizzati nel c.d. *cyberspace* ovvero nello spazio informatico globale formato dalla integrazione tra tanti sistemi di elaborazione, comunicazione e connessione[23].

Nel *cyberspace* le tradizionali categorie spazio-fisico-temporali entrano in crisi, in quanto vengono in considerazione:

- la "smaterializzazione" di dati e informazioni, raccolti e scambiati in un contesto virtuale, senza contatto diretto o intervento fisico su di essi[24];

- la "delocalizzazione" di risorse e contenuti, collocabili in una sorta di "meta-territorio"[25]. Peraltro, la dimensione "aterritoriale" del cyberspazio si è incrementata negli ultimi anni con la diffusione del *cloud computing*, che permette di memorizzare, archiviare, elaborare e condividere *files* su "nuvole" delocalizzate in rete[26]. Il tradizionale criterio territoriale risulta dagli esiti incerti pure nei sistemi di *file sharing*, in cui due o più computer si scambiano informazioni mediante una particolare

---

[22] Il termine "*cyberspace*" è stato coniato dallo scrittore W. GIBSON nel racconto *Burning Chrome* del 1982 per indicare una realtà virtuale. Il significato della parola si è poi ampliato, per riferirsi al "mondo di internet" in senso generale (cfr. voce *Cyberspazio* su *Wikipedia*); così pure, il termine "*cybercrime*" ha ormai assunto una portata ampia, in quanto indica "*any criminal act dealing with computers and networks*" (così, voce *Cyber Crime* su *Webopedia*).

[23] V. L. PICOTTI, *La nozione di «criminalità informatica»*, cit., p. 830; ID., *Sistematica dei reati informatici*, cit., p. 89; ID., *La tutela penale della persona*, cit., p. 53; C. PECORELLA, *Il diritto penale dell'informatica*, cit., pp. 28 ss.
In argomento, nell'ampia letteratura straniera, v., tra gli altri, D.S. WALL, *Cyberspace crime*, Farnham, 2003, pp. 3 ss.; C. REED, *Making Laws for Cyberspace*, Oxford, 2012, pp. 25 ss.; S.W. BRENNER, *Toward a Criminal Law for Cyberspace: a New Model of Law Enforcement*, in *Rutgers Computer & Tech. Law Jour.*, n. 30/2004, pp. 1 ss.; ID., *Toward a Criminal Law for Cyberspace: Distributed Security*, in *Boston Un. Jour. of Science & Tech.*, n. 10/2004, pp. 1 ss.

[24] Cfr. L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 89; R. FLOR, Social networks *e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Riv. trim. dir. pen. ec.*, 2012, p. 648.

[25] Si vedano S. SEMINARA, *La pirateria su Internet e il diritto penale*, in *Riv. trim. dir. pen. ec.*, 1997, p. 102, per il quale "Ai fini della individuazione del *locus commissi delicti*, occorre partire dalla premessa che Internet… non consente alcuna delimitazione territoriale nell'accessibilità dei dati immessi e questi risultano raggiungibili da qualunque utente collegato"; F. RUGGIERO, *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in *Giur. merito*, 2002, p. 254; M. CAMMARATA, *Quali leggi per il "territorio Internet"?*, in www.interlex.it, 19.06.1997; N. GARRAPA, *Internet e diritto penale: tra lacune legislative, presunte o reali, panorami transnazionali, analisi* de iure condito *e prospettive* de iure condendo, in www.diritto.it, gen. 1999.

[26] Cfr. L. PICOTTI, *La nozione di «criminalità informatica»*, cit., p. 831; R. FLOR, Social networks *e violazioni penali*, loc. cit.; S. ATERNO-M. MATTIUCCI, Cloud Forensics e *nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.*, 2013, pp. 876-877. Come opportunamente rileva S. ATERNO, *Osservazioni*, cit., p. 1707, "Il *cloud* nella sua accezione più pura, non consente a nessuno di accertare con un minimo grado di attendibilità il luogo fisico in cui si trova il *server* che contiene il documento informatico o la banca dati"; v. pure R. ZANNOTTI, *Accesso abusivo ad un sistema telematico*, cit., p. 952; C.F. GROSSO, *Su di un'interessante controversia interpretativa*, cit., p. 1531.
Per una descrizione dei più diffusi servizi di *cloud computing*, da Dropbox a iCloud o Drive, v. F. FOSSETTI, *L'ufficio aperto sulle nuvole*, in *La Repubblica*, 13.09.2014.

modalità di connessione, denominata "*peer to peer*", che consente il reciproco trasferimento di dati senza farli transitare da un server centrale[27];

- la "detemporalizzazione" delle attività, che possono essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente, in modo da non aver poi bisogno di un collegamento o contatto fisico tra persona e sistema informatico[28];

- la possibilità per l'utente di avvalersi delle caratteristiche di "ubiquità", velocità e (entro certi limiti) anonimato offerte dalla rete globale a chi vi opera[29].

5. L'intrusione nel sistema informatico o telematico mediante la digitazione alla tastiera dei comandi necessari.

Tali peculiari connotati del mondo informatico e cibernetico si rinvengono anche nei casi concreti sottoposti a valutazione nelle recenti sentenze della Corte di Cassazione.

Invero, il Sistema d'informazione interforze del Ministero dell'Interno (c.d. SDI) è un'applicazione informatica del Centro elaborazione dati (c.d. CED) istituito presso il medesimo Ministero ai sensi dell'art. 8 della legge 1° aprile 1981, n. 121[30]. In tale banca dati vengono acquisiti, a cura della Polizia di Stato, dell'Arma dei Carabinieri, del Corpo della Guardia di Finanza e degli altri Corpi di Polizia[31], «tutte le informazioni ed i dati in loro possesso in materia di tutela dell'ordine e della sicurezza pubblica e di prevenzione e repressione della criminalità» (cfr. art. 1 del D.P.R. 3 maggio 1982 n. 378[32]).

Per i soggetti abilitati[33], «L'accesso ai dati e alle informazioni conservati negli archivi magnetici del centro elaborazione dati, … avviene di norma attraverso la rete periferica dei terminali collegati al sistema integrato di elaboratori facente capo al suddetto centro» (cfr. art. 10 del D.P.R. n. 378/1982).

Lo SDI è pertanto un sistema telematico, composto da numerosi terminali periferici connessi al sistema integrato di elaboratori facente capo al Centro elaborazione dati, che interagiscono tra di loro attraverso il collegamento assicurato da una rete intranet, alla quale possono accedere soltanto le persone munite di apposita abilitazione. Il sistema si caratterizza proprio per la costante e continua interazione: da

---

[27] Sulle caratteristiche del *file sharing*, v. M. ZONARO, *Le 50 parole della Digital Forensics più utilizzate nelle Aule di Giustizia*, Roma, 2014, p. 27.

[28] In tal senso, v. R. FLOR, *op. ult. loc. cit*.

[29] V. L. PICOTTI, *La tutela penale della persona* , cit., p. 49.

[30] In argomento, cfr. A.A. DALIA, *Commento agli artt. 7-11 l. 121/1981*, in *Leg. pen.*, 1982, p. 56; F. MUCCIARELLI, voce *Computer (disciplina giuridica del) nel diritto penale*, in *Digesto disc. pen.*, vol. II, Torino, 1988, p. 387.

[31] Di cui all'art. 16, comma 2, della legge 1° aprile 1981, n. 121.

[32] Contenente il "Regolamento sulle procedure di raccolta, accesso, comunicazione, correzione, cancellazione, ed integrazione dei dati e delle informazioni, registrati negli archivi magnetici del centro elaborazione dati di cui all'art. 8 della legge 1° aprile 1981, n. 121".

[33] Si tratta dei soggetti elencati nell'art. 9 della legge n. 121/1981 e nell'art. 9 del D.P.R. n. 378/1982.

una parte, le postazioni periferiche (*clients*) consentono l'immissione di nuove informazioni e la consultazione di dati già raccolti; dall'altra parte, il patrimonio comune di dati acquisiti ed elaborati è contestualmente compresente e consultabile presso tutte le postazioni remote abilitate.

Qualora l'apparato in questione fosse osservato secondo le tradizionali, ma insufficienti, categorie fisico-spaziali, si potrebbe essere indotti a scomporre e suddividere il sistema, separando i terminali periferici dal server centrale. In realtà, sulla base del più corretto punto di vista tecnico-informatico, il sistema è da intendersi come un *unicum* "smaterializzato" e "delocalizzato", in quanto il bagaglio conoscitivo di dati informatici accumulati e messi a disposizione (dei soggetti abilitati) nel cyberspazio (la rete intranet), si trova allo stesso tempo nella piena disponibilità di consultazione (con possibilità di integrazione dei dati) di ciascun operatore periferico. Ne consegue che le singole postazioni remote non sono meri "strumenti di accesso" al sistema[34], ma costituiscono esse stesse il sistema[35], in quanto partecipano in modo interattivo alla acquisizione e integrazione dei dati e hanno in ogni momento, e contestualmente, la disponibilità delle informazioni raccolte nel *data-base*.

Le medesime considerazioni possono valere per sistemi analoghi allo SDI, come il sistema dell'Anagrafe Tributaria ovvero la banca dati istituita dal D.P.R. 29 settembre 1973, n. 605 e utilizzata per la raccolta e l'elaborazione dei dati relativi alla fiscalità dei contribuenti italiani[36]; oppure per il sistema informatico del Ministero delle Infrastrutture e dei Trasporti (c.d. sistema SIMOT.DTT)[37].

In tali situazioni, l'intrusione nel sistema informatico o telematico risulta integrata già con la digitazione alla tastiera dei comandi con cui si richiede a un sistema informatico di fornire determinati dati o eseguire una operazione e questo risponde in modo positivo, instaurando un dialogo logico e automatizzato con il sistema richiedente[38].

D'altronde, il delitto in esame è un reato di condotta e l'azione - da intendersi quale movimento corporeo dell'uomo, percepibile dall'esterno, nonché cosciente e volontario[39] - si esaurisce con il fatto dell'operatore abusivo che digita le credenziali sul terminale periferico, preme il tasto di invio e si mette così nella condizione di acquisire

---

[34] Così, invece, Cass. pen., sez. I, sent. 27 maggio 2013 (dep. 27 settembre 2013), cit.

[35] Cfr. Cass. pen., sez. I, ord. 28 ottobre 2014 (dep. 18 dicembre 2014), cit.

[36] Per casi giudiziari di accesso abusivo (ex art. 615-ter c.p.) all'Anagrafe Tributaria, v. Cass. pen., sez. V, sent. 24 aprile 2013 (dep. 22 maggio 2013), n. 22024, in www.italgiure.giustizia.it; Cass. pen., sez. V, sent. 30 settembre 2008 (dep. 16 gennaio 2009), n. 1727, in C.E.D., n. 242938; Trib. Nola, sent. 11 dicembre 2007, in *Dir. inf.*, 2008, p. 367.

[37] Cfr. il caso esaminato nella ordinanza n. 52575/14 della Corte di Cassazione, I sez. pen., del 28 ottobre-18 dicembre 2014.

[38] V. I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico*, cit., p. 135; ID., *Quando un* insider *accede*, cit., p. 376. V. anche M. NUNZIATA, *La prima applicazione giurisprudenziale*, cit., p. 711.

[39] Cfr., per tutti, F. ANTOLISEI, *Manuale di diritto penale. Parte generale*, XVI ed., a cura di L. Conti, Milano, 2003, p. 223; G. FIANDACA-E. MUSCO, *Diritto penale. Parte generale*, VI ed., Bologna, 2010, p. 218.

le informazioni contenute nel server centrale, senza allontanarsi fisicamente dalla propria postazione[40].

Ne consegue che il reato si perfeziona nel momento in cui il soggetto si introduce nel sistema violato (oppure dal momento in cui vi permane oltre il limite consentito) e nel luogo (rilevante *ex* artt. 6 c.p. e 8 c.p.p.) in cui egli digita alla tastiera la serie di comandi necessari per l'accesso abusivo al sistema.

Tale conclusione interpretativa è peraltro l'unica razionalmente e praticamente percorribile rispetto ai casi in cui la banca dati violata non si trovi in un luogo fisicamente individuabile, ma sia delocalizzata in "nuvole" accessibili attraverso il sistema (*cloud computing*)[41].

Così pure, la soluzione proposta appare idonea a orientare l'interprete nei casi in cui il collegamento al sistema sia realizzato da un terminale periferico in movimento (ad es., da un viaggiatore in treno che utilizzi un *tablet* o uno *smartphone*). In tali evenienze, qualora non sia possibile ricostruire con precisione il luogo attraversato al momento dell'accesso abusivo, la competenza per territorio sarebbe comunque determinabile attraverso le regole suppletive di cui all'art. 9 c.p.p.[42].

6. L'esigenza processuale di perseguire il reato nel luogo in cui ha agito al computer l'autore della intrusione.

Pur in assenza di un espresso intervento legislativo in argomento[43], il problematico quesito della individuazione del *locus commissi delicti* dell'accesso abusivo a un sistema informatico o telematico può pertanto essere risolto in modo soddisfacente sulla base delle norme vigenti, in modo da assicurare, peraltro, la perseguibilità dell'episodio criminoso nel luogo in cui ha agito al computer l'autore dell'intrusione, ai fini di un più efficace accertamento del reato e di una appropriata applicazione della pena. Invero, il fatto delittuoso in questione merita di essere accertato e giudicato nel contesto locale della postazione periferica ovvero laddove, nella normalità dei casi, si sono concentrati i tratti salienti dell'episodio criminoso, dalla insorgenza del proposito delittuoso, alla eventuale programmazione dell'accesso abusivo, all'accordo tra correi, ecc.

---

[40] Cfr. GUP Trib. Roma (Giudice d'Alessandro), ord. 16 aprile 2014, cit.; C.F. GROSSO, *Su di un'interessante controversia interpretativa*, cit., p. 1527; R. ZANNOTTI, *Accesso abusivo ad un sistema telematico*, cit., p. 951.

[41] Si vedano C.F. GROSSO, *Su di un'interessante controversia interpretativa*, cit., p. 1531; R. ZANNOTTI, *Accesso abusivo ad un sistema telematico*, cit., p. 952. In argomento, v. *retro*, par. 4.

[42] Art. 9 c.p.p.: «Se la competenza non può essere determinata a norma dell'art. 8, è competente il giudice dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione (co. 1). Se non è noto il luogo indicato nel comma 1, la competenza appartiene successivamente al giudice della residenza, della dimora o del domicilio dell'imputato (co. 2). Se nemmeno in tale modo è possibile determinare la competenza, questa appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'art. 335 (co. 3)».

[43] L'intervento del legislatore in materia è auspicato da C. PECORELLA, *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo*, cit.; nonché da S. ATERNO, *Osservazioni*, cit., p. 1707.

Viene così rispettata in pieno la *ratio* ispiratrice del criterio generale *ex* art. 8 c.p.p. – secondo cui «La competenza per territorio è determinata dal luogo in cui il reato è stato consumato» - volta a integrare il requisito di "naturalità" del giudice, richiesto dall'art. 25, co. 1, Cost.; in particolare, il principio del giudice naturale risponde all'esigenza di vedere giudicato il fatto da chi, essendo il più vicino all'ambiente nel quale esso si è verificato, risulta maggiormente legittimato a pronunciare il relativo giudizio[44].

Sulla base di tale premessa, il radicamento della competenza territoriale presso il *locus commissi delicti* persegue il duplice scopo di agevolare la raccolta delle prove e di assicurare la esemplarità che consegue all'attuazione della punizione nel medesimo luogo in cui il reato è stato commesso; vengono pertanto in considerazione ragioni sia di efficienza della giurisdizione che di esemplarità della pena[45].

Non a caso, le stesse Sezioni Unite penali della Corte di Cassazione, ora chiamate a pronunciarsi sul *locus commissi delicti* dell'accesso abusivo a sistema informatico e telematico, in altra occasione hanno già avuto modo di evidenziare come "l'individuazione del giudice penale territorialmente competente a giudicare un dato reato debba richiedere la presenza di un collegamento con il luogo di commissione del reato stesso, per tutta una serie di intuitive ragioni, che vanno dall'esigenza di assicurare un effettivo controllo sociale, a quella di agevolare la raccolta delle prove, a quella di ridurre i disagi per le parti e per i testi"[46].

7. L'ipotesi problematica in cui l'accesso abusivo sia realizzato dall'estero.

---

[44] In argomento, la Corte Costituzionale ha sottolineato che "la locuzione «giudice naturale» non ha nell'art. 25 Cost. un significato proprio e distinto, e deriva per forza di tradizione da norme analoghe di precedenti Costituzioni, nulla in realtà aggiungendo al concetto di «giudice precostituito per legge»; ma deve riconoscersi che il predicato della «naturalità» assume nel processo penale un carattere del tutto particolare, in ragione della «fisiologica» allocazione di quel processo nel *locus commissi delicti* (…) giacché la celebrazione di quel processo in «quel» luogo, risponde ad esigenze di indubbio rilievo, fra le quali, non ultima, va annoverata anche quella – più che tradizionale – per la quale il diritto e la giustizia devono riaffermarsi proprio nel luogo in cui sono stati violati": così C. Cost., sent. n. 168 del 5-21 aprile 2006, in *Giur.cost*., 2006, p. 1495. In dottrina, in termini analoghi, cfr., per tutti, A.A. DALIA-M. FERRAIOLI, *Manuale di diritto processuale penale*, VIII ed., Padova, 2013, p. 92.

[45] Si vedano, tra gli altri, A. NAPPI, *Guida al Codice di Procedura Penale*, IX ed., Milano, 2004, p. 36; ID., voce *Competenza penale*, in *Digesto disc. pen*., vol. II, Torino, 1988, p. 351; A. GIARDA-G. SPANGHER (a cura di), *Codice di procedura penale commentato*, IV ed., Milano, 2010, p. 264; E. ZAPPALA', *Commento all'art. 8*, in G. CONSO-V. GREVI (a cura di), *Commentario breve al codice di procedura penale*, Padova, 2005, p. 16; G. BELLAVISTA, voce *Competenza penale*, in *Nov. Digesto it*., vol. III, Torino, 1959, p. 771; G.M. BACCARI, *La cognizione e la competenza del giudice*, Milano, 2011, p. 205. V. anche Corte Cost., sent. n. 280 del 23 giugno-6 luglio 1994, in *Giur. cost*., 1994, p. 2481 (con nota di P. VENTURA), secondo cui "il criterio del *forum commissi delicti*, pur se ispirato da finalità attinenti in modo prevalente alla economia processuale" risponde anche alla "esigenza di una più facile raccolta delle prove e dunque evidentemente incide, rendendolo più agevole, sull'esercizio del diritto di difesa".

[46] Così Cass. pen., Sez. un., sent. n. 40537 del 20 ottobre 2009, Pres. Gemelli, Rel. Franco, confl. comp. tra GIP Roma e Trib. Tivoli, in *Cass. pen*., 2010, p. 2121.

La soluzione interpretativa qui prescelta, nel senso di radicare la competenza per territorio nel luogo ove si trova la postazione periferica di accesso al sistema, risulta sufficientemente efficace e ragionevole anche rispetto ai casi in cui l'intrusione sia realizzata dall'estero nei confronti di un data-base italiano.

Invero, in tali ipotesi, le caratteristiche sopra descritte del *cyberspace*[47], con la "smaterializzazione", "delocalizzazione" e "ubiquità" dei dati accessibili e consultabili, dappertutto e in contemporanea, nell'ambito del sistema integrante un *unicum*, fanno sì che la condotta abusiva posta in essere dal terminale situato all'estero abbia una sua inevitabile "proiezione" estesa al *server* centrale collegato in Italia; si potrebbe quindi arrivare a sostenere che l'azione criminosa, seppur compiuta dall'operatore senza allontanarsi fisicamente dalla postazione periferica, sia in realtà realizzata, secondo la dimensione digitale e immateriale dei fenomeni cibernetici, in parte all'estero e in parte, contemporaneamente, in Italia, con la conseguenza che il reato si potrebbe considerare comunque commesso nel territorio dello Stato italiano (cfr. art. 6, co. 2, c.p.)[48], consentendo l'applicazione della disciplina della competenza per territorio prevista (ai sensi dell'art. 10, co. 3, c.p.p.[49]) dalle regole generali *ex* art. 8 c.p.p. e dalle regole suppletive *ex* art. 9. c.p.p.

In alternativa, in tali casi, qualora – sempre seguendo il criterio qui suggerito della individuazione del *locus commissi delicti* sulla base della collocazione della postazione periferica ove agisca l'operatore – il reato di accesso abusivo a sistema informatico o telematico fosse considerato interamente commesso all'estero, ma ai danni di un server situato sul territorio italiano, si potrebbe comunque radicare la giurisdizione in Italia, qualora ricorrano i requisiti e le condizioni previsti dagli artt. 7, 8, 9 o 10 c.p.[50].

Ad ogni modo, con riguardo alla eventuale dimensione transfrontaliera dell'accesso abusivo a sistema informatico o telematico, appare confortante il costante interesse in materia del legislatore europeo. Invero, dopo la Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001 (c.d. Convenzione *Cybercrime*)[51] e la Decisione quadro 2005/222/GAI sugli attacchi ai sistemi di informazione, è stata più recentemente emanata la Direttiva 2013/40/UE del

---

[47] V. *retro*, par. 4.

[48] Cfr. GUP Trib. Roma (Giudice d'Alessandro), ord. 16 aprile 2014, cit.; C.F. GROSSO, *Su di un'interessante controversia interpretativa*, cit., p. 1530.

[49] Sulla disciplina della competenza per i reati commessi in parte all'estero, cfr., per tutti, F. CORDERO, *Procedura penale*, IX ed., Milano, 2012, p. 143.

[50] Rispetto ai possibili autori del delitto di accesso abusivo a sistema informatico o telematico, appaiono di particolare rilievo, nella elencazione dei "Reati commessi all'estero" e puniti secondo la legge italiana, ai sensi dell'art. 7 c.p., i "delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alle loro funzioni" (cfr. art. 7, n. 4, c.p.).

[51] Ratificata in Italia con la legge 18 marzo 2008, n. 2008. In argomento, v. L. PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, p. 696, nonché L. LUPARIA, *I profili processuali*, *ivi*, p. 717; C. SARZANA DI S. IPPOLITO, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. proc.*, 2008, p. 1562; L. PICOTTI, *La tutela penale della persona*, cit., p. 41; I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico*, cit., p. 128.

Parlamento europeo e del Consiglio del 12 agosto 2013 (che sostituisce la Decisione quadro del 2005)[52].

Ai fini che qui maggiormente interessano, tale Direttiva si segnala, in primo luogo, per la previsione del reato di "Accesso illecito a sistemi di informazione", delineato nei seguenti termini: «Gli Stati membri adottano le misure necessarie per garantire che, se intenzionale, l'accesso senza diritto a un sistema di informazione o a una parte dello stesso, sia punibile come reato qualora commesso in violazione di una misura di sicurezza, almeno per i casi che non sono di minore gravità» (art. 3). Come si vede, la condotta tipica del reato è descritta (in linea con la Convenzione *Cybercrime* del 2001 e la Decisione quadro del 2005[53]) nella più appropriata forma dell'«accesso», e non della «introduzione»[54], a un sistema di informazione[55].

In secondo luogo, la Direttiva dedica particolare attenzione alla competenza giurisdizionale (art. 12) e allo scambio di informazioni tra Stati membri (art. 13)[56], prevedendo, tra l'altro, che «Gli Stati membri stabiliscono la propria competenza giurisdizionale relativamente ai reati» informatici di cui agli articoli da 3 a 8 della stessa Direttiva (ovvero: accesso illecito a sistemi di informazione; interferenza illecita relativamente ai sistemi; interferenza illecita relativamente ai dati; intercettazione illecita; strumenti utilizzati per commettere i reati; istigazione, favoreggiamento, concorso e tentativo), «quando il reato sia stato commesso: a) in tutto o in parte sul loro territorio; o b) da un loro cittadino, quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso» (art. 12, par. 1)[57].

---

[52] Per un commento a tale Direttiva, v. S. CIVELLO CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *questa Rivista*, 30 ottobre 2013.

[53] Sulla fattispecie di accesso illecito a un sistema di informazione prevista da tali fonti sovranazionali, cfr. L. PICOTTI-I. SALVADORI, *National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices*, in www.coe.int/cybercrime, 28.08.2008.

[54] Per una analisi comparatistica sui modi in cui il reato di accesso abusivo a sistema informatico è descritto nei vari ordinamenti, v. I. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico*, cit., p. 133; ID., *L'esperienza giuridica degli Stati Uniti d'America in materia di* hacking *e* cracking, in *Riv. it. dir. proc. pen.*, 2008, p. 1247; L. PICOTTI-I. SALVADORI, *National legislation implementing*, cit.

[55] Il "sistema di informazione" è definito dalla Direttiva 2013/40/UE come «un'apparecchiatura o gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati da tale apparecchiatura o gruppo di apparecchiature, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione» (art. 2, lett. a).

[56] Sulla esigenza di ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, nonché di migliorare la cooperazione di polizia e giudiziaria in tale settore, a fronte della dimensione transfrontaliera della criminalità informatica, si vedano, in particolare, i considerando nn. 1, 27 e 28 della Direttiva.

[57] La disciplina della "Competenza giurisdizionale" è poi completata dalle seguenti previsioni: «Nello stabilire la propria competenza giurisdizionale conformemente al paragrafo 1, lettera a), uno Stato membro assicura di avere competenza giurisdizionale qualora: a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato» (art. 12, par. 2); «Uno

Poiché la Direttiva in questione deve essere recepita entro il 4 settembre 2015 (cfr. art. 16), si può auspicare che il legislatore italiano colga l'occasione per una rinnovata riflessione sui profili sostanziali e procedurali dei reati informatici e cibernetici, al fine di adeguare la disciplina alle moderne e attuali manifestazioni di tale tipologia di criminalità.

Stato membro informa la Commissione ove decida di stabilire la competenza giurisdizionale per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, anche qualora: a) l'autore del reato risieda abitualmente nel suo territorio; o b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio» (art. 12, par. 3).