GIP TRIBUNALE ROMA
ORDINANZA
16 APRILE 2014
GIUDICE: D'ALESSANDRO

- **Reati informatici**
- **Accesso abusivo ad un sistema telematico**
- **Banche dati**
- **Accesso da un terminale periferico**
- **Giudice competente per territorio**
- **Giudice del luogo ove avviene l'accesso**

Nel caso di accesso abusivo ad un sistema telematico realizzato da un soggetto che si è collegato alla banca dati da un terminale periferico è competente il Giudice del luogo dal quale il soggetto si è collegato e non il Giudice del luogo nel quale è fisicamente collocato il sistema informatico, il server o la banca dati obiettivo dell'intrusione.

1. Il Pubblico Ministero di Firenze, sempre ritenendo la propria competenza per territorio, ha promosso l'azione penale (12.4.2010) e il Giudice per l'udienza preliminare di Firenze ha rigettato l'eccezione di incompetenza territoriale (22.12.2010).

Appariva, invero, *ictu oculi* non condivisibile il rilievo che il reato dovesse ritenersi commesso a Roma, per essere il *server* situato in Roma, con l'introduzione di una distinzione fisica — non ammissibile in un sistema informatico — tra periferia e centro.

[...*omissis*...]

Il Tribunale di Roma diviene così, nella prospettiva prescelta, una sorta di Giudice speciale, *ratione materiae*, per tutte le fattispecie informatiche, essendo Roma la sede non solo del *server* del Viminale — Ministero degli Interni — ma anche dei *server* di svariate altre banche dati: Poste Italiane; Ferrovie dello Stato; ISVAP; Bankitalia.

[...*omissis*...]

Va poi evidenziato in fatto, con ricostruzione delle condotte oggetto di contestazione, che si controverte dell'abusiva introduzione e del mantenimento dell'*extraneus* nella banca dati riservata del sistema d'informazione interforze del Ministero dell'Interno (SDI). Da tale sistema sono stati acquisiti, secondo l'accusa, dati segreti su centinaia di persone, che poi erano comunicati — da alcuni degli imputati — a chi aveva commissionato l'illecita ricerca.

È pacifico che la banca dati in questione si trovi fisicamente situata in Roma, nell'ambito degli uffici del Ministero dell'Interno, e che ad essa si acceda ogni volta che viene fatta una interrogazione proveniente da terminali collegati, dopo la digitazione delle credenziali di accesso. Altrettanto indiscutibile, però, è che i terminali del sistema siano situati su tutto il territorio nazionale, negli uffici decentrati del Ministero medesimo, o negli uffici comunque abilitati all'accesso.

L'accesso nel sistema avviene tramite digitazione delle credenziali dell'utente (*username* e *password*) in ciascuna sede di digitazione.

L'introduzione di un dato avviene nelle singole sedi periferiche e si inserisce contestualmente a Roma, nel sistema informatico centrale: tutto è contestualmente presente in tutti gli ambiti in cui il sistema opera: Roma, come le sedi periferiche.

Non esiste una ripartizione spaziale poiché si versa in un *cyber*spazio 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.

È del tutto erroneo scindere il *server* e definirlo 'romano', poiché il sistema è un *unicum* che si alimenta di continue allegazioni e acquisizioni di dati contestualmente ovunque compresenti.

L'abusiva introduzione nel sistema informatico o il mantenimento al suo interno contro la volontà espressa o tacita di chi ha il diritto di esclusione sono le condotte incriminate, con la conseguenza che, ai fini della determinazione del luogo di consumazione del reato e della competenza territoriale, non è rilevante il luogo dell'acquisizione abusiva dell'informazione.

Rilevante è il luogo dell'accesso, e sul concetto di accesso — se si tratti dell'inserimento nel terminale locale, non revocabile, negli esiti, una volta posto in essere; o se si tratti di materiale immissione all'interno della banca dati, con trasposizione nel sistema informatico del concetto naturalistico di evento materiale — esiste contrasto tra questo Giudice e il Tribunale di Firenze.

Per entrambi gli orientamenti deve escludersi che vengano in qualsivoglia rilievo le condotte successive all'introduzione o al mantenimento nel sistema, ossia la lettura e l'uso dell'informazione, che, ovunque avvengano, sono irrilevanti ai fini della competenza, quasi un post fatto non punibile, successivo ad un reato già consumato e tipico in virtù dell'accesso.

Viene, al contrario, in rilievo il luogo nel quale si è posta in essere l'attività umana di introduzione o mantenimento volontaria e tipica, ossia il luogo in cui si è effettuata — da parte dell'autore del reato — la digitazione delle credenziali di accesso, *ex se* bastevole a determinare il fatto, secondo questo GUP; idonea, viceversa ad integrare il reato solo se produttiva di ingresso nel *data base*, secondo il Tribunale di Firenze.

[...*omissis*...]

È da escludersi che possa farsi riferimento all'accesso al *data base* centrale come evento naturalistico coessenziale al reato, dal momento che la giurisprudenza di legittimità stessa — avvertendo l'artificiosità della costruzione — riconduce la fattispecie a reato di mera condotta.

La competenza non va pensata con parametri di fisicità — secondo gli abituali schemi concettuali di condotta ed evento, cui si fa riferimento in un mondo materiale, dominato dai concetti di azione e reazione — per l'ottimo motivo che non si versa in un sistema materiale, ma in un sistema informatico, e, più precisamente, in una rete di comunicazione telematica.

L'accesso da terminale al sistema informatico risponde alla logica fisica appena detta e consente di collocare l'operatore e il suo agire in uno spazio.

Ciò non vale certo per quello che accade all'interno del sistema.

Ossia, l'ultima attività umana che si connota per fisicità è quella dell'accesso da terminale, ma tutto ciò che segue — ossia l'ingresso informatico vero e proprio nel *data base*, nel cuore del sistema, ingresso indipendente, si badi bene, dalle successive, e, come già sopra detto,

irrilevanti attività umane di lettura e divulgazione — va escluso da ogni rilievo ai fini della competenza.

Va vagliato il luogo della condotta umana tipica e volontaria per determinare la competenza e tale luogo è quello di collocazione del terminale attivato per l'accesso: la riconduzione del luogo nel quale la condotta di accesso è maturata al sito di collocazione del terminale consente alle norme sulla competenza di essere fino in fondo ciò per cui sono state pensate. E cioè non un criterio regolatore astratto, ma un sistema per ricondurre l'attività accertativa al luogo nel quale — nel caso di specie tramite terminale — si sono poste in essere le condotte umane idonee a completare disegni criminosi molto più ampi, e fisicamente collocati.

Si tratta, in sintesi, e secondo una razionale attività interpretativa, di consentire alle norme sulla competenza di essere norme regolatrici dell'attività processuale idonea ad agevolarne il compimento nell'interesse delle prerogative accusatorie del Pubblico Ministero, ma anche delle esigenze di prospettazione della difesa.

[...*omissis*...]

In questo senso costituisce precedente non valicabile la pronuncia sopra citata della Corte di cassazione, che ricostruisce l'accesso abusivo a sistema informatico come reato di mera condotta e non già di evento.

[...*omissis*...]

La condotta umana, nel suo prevalente o più significativo svolgersi, è quella che determina la competenza per territorio, e nel caso di specie l'unica condotta umana rilevante e territorialmente collocabile è quella di accesso al terminale.

Tale condotta, una volta posta in essere, non è più suscettibile di essere interrotta nei suoi esiti, sicché l'esatta e doverosa valorizzazione del luogo della sua realizzazione consente di evitare la conclusione interpretativa del tutto irrazionale e incoerente di allontanare il luogo dell'indagine — e quindi della sede delle forze di polizia, o della residenza dei testimoni, delle persone offese, degli indagati — da quello dei fatti solo perché il *data base* interno al sistema informatico attivato si trovi, in ipotesi, a Roma, o Milano, o Londra, o Bruxelles.

E che questa sia la soluzione più logica, imposta dalla esatta enucleazione della *ratio* delle norme sulla competenza, emerge anche dal rilievo che all'interno del sistema informatico attivato non può esservi concettualmente un luogo di collocazione fisica della banca dati idoneo a spostare giuridicamente la competenza, come si operasse all'interno di un sistema fisico dominato dai canoni di spazio e tempo o di azione ed evento.

[...*omissis*...]

Appare evidente a questo Giudice l'inesattezza interpretativa: il concetto di collocazione spaziale è un concetto fisico che non ha diritto di cittadinanza in una rete telematica fondata sulla coesistenza dei flussi informativi, ed è, anzi, con essa incompatibile.

[...*omissis*...]

Per le considerazioni che precedono, il GUP di Roma eleva conflitto con il Tribunale di Firenze.

Accesso abusivo ad un sistema telematico: quale il locus commissi delicti*?*

0. - L'ordinanza che si annota, emessa dall'Ufficio del Giudice per l'udienza preliminare del Tribunale di Roma, solleva conflitto di competenza in ordine alla questione concernente la competenza territoriale a conoscere del delitto di accesso abusivo ad un sistema telematico previsto dall'art. 615-*ter* c.p. [1].

La questione è nota e ricorrente e trae origine dal numero sempre crescente di fatti realizzati da pubblici ufficiali che accedono abusivamente a varie banche dati [si pensi, ad esempio, all'Anagrafe tributaria o al Sistema di Indagine (SDI) del Ministero dell'Interno] per acquisire la conoscenza di informazioni ivi contenute, per farne poi un utilizzo illecito (ad esempio, per cederle ad organi di stampa o per comunicarle ad altre persone). In casi di tal fatta, normalmente i pubblici ufficiali detengono gli strumenti (*password* e altre chiavi d'identificazione) per accedere a detti sistemi telematici per ragioni del loro ufficio; però l'accesso viene effettuato non per ragioni d'ufficio, ma per entrare in possesso di dati o informazioni da cedere a terzi, i quali ovviamente hanno interesse ad acquisirli. Ma il profilo affrontato dalla pregevole ordinanza annotata non concerne l'abusività dell'accesso: già in un recente passato, infatti, le Sezioni Unite hanno definitivamente chiarito che integra il delitto previsto dall'art. 615 *ter* c.p. colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema [2].

Il punto di diritto che invece affronta l'ordinanza del GUP di Roma riguarda l'individuazione del *locus commissi delicti* quando l'accesso abusivo si realizza in un sistema telematico. Si tratta di una questione che necessita di approfondimento, in quanto nella maggior parte dei casi che pervengono a conoscenza dell'Autorità giudiziaria l'agente opera da un terminale periferico per 'interrogare' una banca dati situata in altro luogo, che in alcuni casi potrebbe addirittura non possedere i caratteri della fisicità (si pensi a tutte quelle situazioni nelle quali i *server* sono

[1] V., in termini generali, AA. VV., *Profili penali dell'informatica*, a cura di Borruso R.-Buonomo G.-Corasaniti G., Milano, 1994; Aterno S., *Sull'accesso abusivo ad un sistema informatico o telematico*, in *Cass. pen.*, 2000, p. 2990 ss.; Corrias Lucente G., *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in questa *Rivista*, 2001, p. 492 ss.; Farci E., *L'accesso abusivo ad un sistema informatico o telematico*, in AA. VV., *Diritto dell'informatica*, a cura di Finocchiaro G. e Delfini F., Torino, 2014, p. 1095 ss.; Flor R., *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. 89 ss.; Pecorella C., *Il diritto penale dell'informatica*, II ediz., Padova, 2006; Pestelli G., *Brevi note in tema di accesso abusivo ad un sistema informatico o telematico*, in *Cass. pen.*, 2012, p. 2320 ss..

[2] Cass., ss. uu., 27 ottobre 2011, n. 4694, in *Cass. pen.*, 2012, p. 3681, con nota di C. Pecorella; anche in *Foro it.*, 2012, II, c. 375 ss., con nota di S. Di Paola.

collocati in *cloud*, cioè sono del tutto dematerializzati). Si pone dunque il problema di decidere se Giudice competente è quello del luogo ove è stato effettuato materialmente l'accesso oppure quello del luogo di allocazione del *server*.

L'esigenza di individuare correttamente il Giudice competente a giudicare i fatti di accesso abusivo ad un sistema telematico suscita anzitutto una constatazione preliminare: le nuove tecnologie informatiche hanno creato, anche con riferimento alla legislazione, una dimensione totalmente nuova, insuscettibile di essere governata basandosi su schemi obsoleti. In tale contesto l'interprete troppo spesso cede alla tentazione di applicare, anche con riferimento a tali nuove dimensioni, che invece esigerebbero nuovi schemi concettuali, una regolamentazione giuridica ancorata a concetti tradizionali, non comprendendo che schemi completamente nuovi (quali certamente sono quelli introdotti dall'informatica) richiedono soluzioni altrettanto nuove, sganciate dall'esperienza passata [3]. Nel caso di specie l'estensore dell'ordinanza che si annota possiede piena consapevolezza di ciò ed utilizza, ai fini dell'individuazione del Giudice competente, la soluzione maggiormente adeguata alla tipicità del fatto e al bene protetto, alla luce della particolarità del sistema violato (che nel caso di specie è sistema telematico e non informatico).

1. - La tesi sostenuta finora, almeno in parte, della giurisprudenza di merito [4] e di legittimità [5], è quella secondo la quale per individuare il giudice competente per territorio occorra fare riferimento al luogo dove si trova il *server*, indipendentemente dalla località ove si trova il terminale dal quale è partita la richiesta. In questo modo si verrebbe peraltro a determinare, posto che gran parte dei *server* delle amministrazioni pubbliche si trovano a Roma, una sorta di competenza esclusiva, per fatti di accesso abusivo, degli uffici giudiziari capitolini: ciò non rappresenta certamente un criterio che da solo possa orientare verso una tesi o verso quella opposta, ma non v'è dubbio che l'interprete debba tener conto anche delle conseguenze sul piano pratico.

Ma ciò che conta è che la tesi sostenuta dalla prevalente giurisprudenza si basa su concetti non chiaramente definiti e, per certi aspetti, contraddittori ed erronei.

Punto centrale dell'orientamento giurisprudenziale sopra cennato, descritto da ultimo nella sentenza della prima sezione penale della Corte di cassazione del 27 maggio 2013, è che "l'accesso...avviene nel luogo in cui viene effettivamente superata la protezione informatica e vi è l'intro-

[3] V., in tal senso, PICA G., voce *Internet* (diritto penale), in *Digesto pen.*, II aggiornamento, Torino, 2004, *passim*.

[4] V., da ultimo, Trib. Napoli, sez. I pen., 12 marzo 2014, n. 3581, in *DeJure*; deve però evidenziarsi che l'orientamento sul punto dei giudici di merito non è uniforme, posto che — ad esempio — in occasione degli accessi abusivi effettuati nel 2006 per conoscere la situazione patrimoniale dell'allora Presidente del consiglio Romano Prodi e di sua moglie, la competenza territoriale per i singoli accessi è stata pacificamente individuata nelle sedi giudiziarie ove si erano verificate le singole intrusioni.

[5] Cass., sez. I pen., c.c. 27 maggio 2013, n. 40303/13, in *Cass. pen.*, 2014, p. 1704, con nota di S. ATERNO; v. altresì, nello stesso senso, Cass., sez. I pen., 15 luglio 2014, n. 3415, in *Riv. it. dir. proc. pen.*, 2014, p. 1503 ss., con nota 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*.

duzione nel sistema e, quindi, là dove è materialmente situato il sistema informatico *server*) violato, l'elaboratore che controlla le credenziali di autenticazione del *client*" [6]. La tesi appare già a prima vista erronea e marcatamente contraddittoria, posto che ad una prima affermazione pacifica e condivisibile ("l'accesso avviene nel luogo in cui viene effettivamente superata la protezione informatica") fa riscontro una conseguenza esplicativa erronea ("e quindi là dove è materialmente situato il sistema informatico violato"). Per sanare la contraddizione la giurisprudenza precisa che "nel momento in cui l'utente dà l'invio all'esito della digitazione delle credenziali non fa cessare la propria condotta, ma la fa strumentalmente proseguire, ancorché smaterializzata, sino alla verifica all'ingresso delle misure di sicurezza logiche presenti sul *server web*, essendo queste che manifestano lo *jus excludendi* del *dominus loci*".

Anzitutto è necessaria una precisazione di carattere tecnico: le c.d. banche dati, quali — ad esempio — lo SDI o l'Anagrafe tributaria, sono *sistemi telematici chiusi*, accessibili soltanto attraverso terminali certificati, da persone debitamente autorizzate in sede locale [7]. Di conseguenza il c.d. terminale certificato periferico non è accessibile da parte di chiunque, ma soltanto da quella persona in possesso di specifica abilitazione, che dovrà essere 'riconosciuta' fin da subito, cioè dal primo momento in cui l'agente abilitato digita le proprie credenziali sul terminale remoto. Già questa specificazione dovrebbe di per sé essere sufficiente a fissare la competenza, posto che la prima (e ineliminabile) azione di 'forzatura' del sistema avviene, in virtù di quanto dianzi specificato, *proprio sul terminale periferico*: in altri termini, l'accesso è già abusivo nel momento in cui l'operatore accede al *computer* remoto e si fa riconoscere per compiere ricerche non autorizzate, indipendentemente dalle operazioni che compirà (o comunque che il sistema effettuerà in seguito).

2. - Ma, al di là di tale facile constatazione di fatto, vi sono altresì tutta una serie di considerazioni sul piano giuridico che confermano la bontà della tesi sostenuta dall'ordinanza che si annota.

In primis, l'attenzione va concentrata sul concetto di azione. Il delitto di accesso abusivo ad un sistema telematico è un reato commissivo doloso di mera condotta [8], che si perfeziona con il semplice accesso nel sistema. Ora è risaputo che sul terreno del reato commissivo "la condotta criminosa assume la forma di un'azione in senso stretto" [9]: e *azione in senso stretto* non può che significare un *movimento del corpo* idoneo ad offendere l'interesse protetto dalla norma [10].

[6] Così, testualmente, Cass., sez. I pen., c.c. 27 maggio 2013, cit.

[7] Sul concetto di telematica v., in generale, Borruso R. - Tiberi C., *L'informatica per il giurista. Dal Bit a Internet*, II ed., Milano, 2001, p. 413 ss.; comunque "sistema telematico è il complesso organico degli elementi (il *computer* con banca dati, i terminali dialoganti, il c.d. *modem*, cioè il modulatore-demodulatore che codifica e decodifica i segnali elettronici, ecc.), componenti un apparato per la comunicazione a distanza di dati: per tale definizione v. Mantovani F., *Diritto penale.* Parte speciale I. Delitti contro la persona, V ediz., Padova, 2013, p. 571. L'esempio più comune di sistema telematico è il circuito Bancomat.

[8] Cass., sez. V pen., 6 febbraio 2007, n. 11689, ric. Cerbone, in CED Cass. pen., 2007.

[9] Così letteralmente Fiandaca G.-Musco E., *Diritto penale.* Parte generale, VI ediz., Bologna, 2010, p. 218.

[10] Fiandaca G.-Musco E., *op. loc. cit.*;

Nel caso di specie l'unico movimento muscolare ravvisabile è quello dell'operatore, il quale digita le proprie credenziali sul terminale periferico. È in tale momento che avviene l'accesso nel sistema telematico, posto che il movimento corporeo delle dita dell'operatore costituisce proprio quell'azione, caratterizzata peraltro dalla partecipazione effettiva della coscienza e volontà, così come richiesto dall'art. 42, primo comma, c.p.

Deve peraltro tenersi presente che i sistemi quali quelli della cui violazione si tratta sono sistemi telematici complessi, estremamente articolati e diffusi, cosicché il meccanismo per fondare la competenza territoriale non può che basarsi sul luogo ove è iniziata la condotta illecita. Tutto ciò che avviene successivamente configura un *post factum* irrilevante ai fini della consumazione del reato, posto che il delitto di cui all'art. 615-*ter* c.p. è reato istantaneo [11], che quindi si consuma nel primo momento dell'introduzione nel sistema, allorquando viene violata la riservatezza del sistema stesso. Ragionare nei termini utilizzati dalla giurisprudenza di legittimità equivale ad utilizzare un concetto di azione 'spurio', composto da comportamenti fisici e conseguenze automatiche 'dematerializzate', che non apporta alcuna utilità al concetto stesso.

Certamente quella che dalla giurisprudenza di legittimità viene, con riferimento al caso specifico di un sistema telematico chiuso, descritta come azione, in realtà è qualcosa di ben diverso. Infatti il soggetto agente (*id est*, chi accede abusivamente) non agisce direttamente nel *server*, ma si limita a digitare sul terminale periferico di accesso al sistema telematico. È ben vero che a seguito di tale digitazione si inviano una serie di dati alfanumerici al *server*, ma ciò in termini penalistici costituisce una conseguenza inevitabile, che però nel caso specifico non va confusa con l'azione.

3. - Poche parole restano ora da spendere con riferimento alle norme processuali che disciplinano la competenza per territorio [12]. Nel caso in esame, determinata la condotta (in termini penalistici) nell'accesso tramite il terminale periferico, non vi sono difficoltà a fare applicazione della regola generale di cui all'art. 8, primo comma, c.p.p. e, di conseguenza, ad individuare il Giudice territorialmente competente in quello del luogo ove si è realizzato l'accesso. Opportunamente l'ordinanza annotata riconosce che "l'unica condotta umana rilevante e territorialmente collocabile è quella di accesso al terminale", posto che in tal modo viene — tra l'altro — a realizzarsi quell'esigenza tipica sottesa alla competenza per territorio, che deve consentire di attivare e svolgere le indagini nel modo più agevole, rendendo nel contempo più semplice la possibilità di difendersi da parte dell'imputato. Peraltro deve altresì osservarsi che l'individuazione del giudice competente in quello del territorio dove è stato realizzato l'accesso al terminale periferico consente di risolvere agevolmente anche tutte quelle situazioni, destinate a divenire sempre più numerose, nelle quali la banca dati non si trova in un luogo fisicamente individuabile, ma

MANTOVANI F., *Diritto penale*, parte generale, VIII ediz., Padova, 2013, p. 130.

[11] ANTOLISEI F., *Manuale di diritto penale*. Parte speciale I, XIV ediz., Milano, 2002, p. 238.

[12] V., in termini generali, SARGENTI B., *Giurisdizione e competenza territoriale in materia penale*, in *Giur. mer.*, 2012, p. 2641 ss.

in un luogo dematerializzato (*cloud computing*). Posto che "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 ... la banca dati" [13] è solo facendo riferimento al momento iniziale dell'accesso sul terminale periferico che in questi casi può determinarsi la competenza per territorio.

4. - In conclusione: l'ordinanza annotata fa, con riferimento al caso specifico del sistema telematico, buon governo delle categorie penalistiche applicate ad un reato informatico così poliedrico quale è l'art. 615-*ter* c.p. e dimostra ancora come nel settore dei reati informatici non vi siano soluzioni preconfezionate, valide per ogni situazione. È sempre più urgente una rilettura delle categorie generali per giungere ad una "revisione di molteplici categorie concettuali e di numerosi assetti di tutela" [14].

ROBERTO ZANNOTTI

[13] Così ATERNO S., in *Cass. pen.*, 2014, cit.

[14] SEMINARA S., *La pirateria su Internet e il diritto penale*, in *Riv. trim. dir. pen. econ.*, 1997, p. 71 ss.