Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico, di Paolo De Martino

www.penalecontemporaneo.it, 11 maggio 2015

Cass., Sez. Un., sent. 26 marzo 2015 (dep. 24 aprile 2015) n. 17325, Pres. Santacroce, Rel. Squassoni

1. Come già segnalato in questa *Rivista*, con ordinanza 28 ottobre 2014 (dep. 18 dicembre 2014), la Prima Sezione della Corte di Cassazione aveva rimesso alle Sezioni unite il seguente quesito: *"se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615*-ter*, cod. pen., sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il* server *che elabora e controlla le credenziali di autenticazione fornite dall'agente".*

Si anticipa, sin da ora, che la Suprema Corte, con la sentenza qui commentata, ha risolto il contrasto secondo questi termini: *"**il luogo di consumazione del delitto di accesso abusivo del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615*-ter *cod. pen., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente**".*

2. Al fine di meglio comprendere le ragioni poste a fondamento di tale decisione, corre d'uopo ripercorrere il caso di specie che ha generato l'ordinanza di rimessione.

Nel caso in esame, la Pubblica Accusa presso il Tribunale di Napoli formulava l'imputazione ai sensi degli artt. 81, 110, 615-*ter*, commi 2 e 3, cod. pen. nei confronti di una dipendente del Ministero dei Trasporti impiegata presso la Motorizzazione Civile di Napoli e dell'amministratore di fatto di una agenzia automobilistica, per essersi introdotti, in modo abusivo, nel sistema informatico del succitato ente pubblico, avvalendosi delle credenziali d'accesso dell'imputata e delle postazioni informatiche di altri suoi colleghi.

Con sentenza del 2 dicembre 2013, il Giudice dell'udienza preliminare presso il Tribunale di Napoli dichiarava la propria incompetenza territoriale in favore del g.i.p. di Roma, in ragione del fatto che i *server* del Ministero dei Trasporti - Motorizzazione Civile di Napoli - sono fisicamente ubicati in Roma.

Dopodiché, il Pubblico Ministero di Roma richiedeva il rinvio a giudizio dei due imputati. Nell'ambito della correlata udienza preliminare, il giudice procedente capitolino sollevava conflitto negativo di competenza, ritenendo che il giudice naturale fosse quello partenopeo, essendo Napoli il luogo ove si era effettuato l'accesso materiale al *server* da parte dei due imputati.

Chiamato a dirimere il conflitto negativo di competenza territoriale, il giudice nomofilattico, prevedendo che in fattispecie non dissimili da quella in esame possano sorgere questioni di competenza territoriale, postulava l'intervento esegetico delle Sezioni Unite.

3. Le Sezioni Unite, prima di trattare i principi generali desumibili dal sistema, rilevano come **siano sempre più frequenti i casi di introduzione abusiva** (**o abusivo mantenimento**) nel sistema informatico da una piattaforma dislocata rispetto all'ubicazione del *server*.

Segue, poi, una attenta disamina dogmatica del delitto di accesso abusivo ad un sistema informatico cui ci si riporta per dovere di sintesi. Ai fini in esame, si ritiene, però, opportuno richiamare la definizione di sistema informatico elaborata in seno alla Convenzione Europea di Budapest del 23 novembre 2001 a cui hanno fatto riferimento le Sezioni Unite. In particolare, l'art. 1 della Convenzione ne tratteggia i confini in questi termini: *"qualsiasi apparecchiature o gruppi di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione dei dati".*

Per evitare *deficit* nel perseguimento dell'obiettivo di protezione del sistema informatico e telematico, risulta conveniente delineare una nozione ampia di *computer*, così come, del resto, il giudice di legittimità ha già fatto in punto di carte di pagamento, constando in mezzi capaci di trasmettere dati elettronici dal luogo ove si connettono mediante le apparecchiature denominate POS[1].

Anche le Sezioni Unite - così come l'ordinanza di rimessione - valorizzano come precedente in materia un arresto (n. 40303 del 2013)[2] inerente una fattispecie di accesso abusivo al *server* del Ministero dell'Interno (SDI), nel cui ambito è stata radicata la competenza territoriale nel luogo di collocazione della banca dati centralizzata dove viene addebitato l'accesso abusivo al sistema informatico.

Tale indirizzo poggia sul fatto che l'effettivo ingresso nel sistema informatico centralizzato da remoto mediante l'autentificazione delle credenziali è come se avvenisse direttamente presso il sistema centrale.

Altra pronuncia di legittimità è addivenuta alle suddette conclusioni con riguardo ad una fattispecie di frode informatica, senza però riflettere a fondo sulle ragioni che hanno portato il giudice nomofilattico ad individuare il *locus commissi delicti* ove è ubicato il sistema centralizzato[3].

Invece, stando all'ordinanza di rimessione, il luogo di perfezionamento del reato previsto dall'art. 615-*ter* cod. pen. nella forma decentralizzata coincide con lo spazio di ubicazione di una articolazione territoriale. Tale postazione periferica di accesso non costituirebbe un mezzo accessorio, bensì una componente informatica essenziale alla stregua del *server* centralizzato.

4. L'inquadramento normativo e giurisprudenziale del delitto di accesso abusivo ad un sistema informatico *ex* art. 615-*ter* cod. pen. porta le Sezioni Unite a privilegiare la tesi avallata dall'ordinanza di remissione che privilegia lo spazio informatico come virtuale, seppur l'art. 8 del codice di rito sia parametrato su una idea fisica della dimensione spaziale.

Dunque, le condotte di abusiva introduzione in un sistema informatico/ telematico o di trattenimento contro la volontà di chi può esercitare lo *jus excludendi* sono collegate ad una dimensione ultimamente elettronica dello spazio che, non a caso, si chiama "virtuale".

Sotto un profilo tecnico, il sistema informatico o telematico va inteso in senso unitario tramite un *software* che governa il funzionamento della rete.

Invece, in modo errato, la citata pronuncia n. 40303 del 2013 fa sua una definizione di sistema informatico che poggia su una dimensione materiale, **con l'effetto di frammentare gli elementi sistemici dando una irragionevole priorità al *server* fisicamente inteso e, quindi, alla sua ubicazione.**

L'introduzione nel sistema informatico si perfeziona nel luogo in cui è ubicata la postazione informatica dalla quale l'operatore digita le credenziali di accesso.

Si badi che il luogo in cui l'utente opera sul *computer* combacia quasi sempre con quello **ove si possono acquisire le prove** e dove **la collettività percepisce il disvalore del delitto posto in essere**. Anche per queste ragioni, le Sezione Unite ritengono che la propria impostazione meglio si addica al canone del giudice naturale sancito all'art. 25, comma 1, della Carta costituzionale.

Viene altresì chiarito come la regola della competenza radicata nel luogo dove si trova il *client* non trovi eccezioni per le forme aggravate del reato di introduzione abusiva ad un sistema informatico. Si consideri che il luogo dove si esercita la violenza prevista dal comma 2 e ove viene danneggiato il sistema informatico (comma 3) coincide con quello in cui è avvenuto l'accesso decentralizzato.

Analogamente, i principi testé citati trovano applicazione anche per le condotte di mantenimento nel sistema informatico contro la volontà di chi ha diritto di escluderlo. Qui la condotta omissiva rilevante ai fini del delitto previsto dall'art. 615-*ter* cod. pen. è quella che coincide con *"uso illecito dello elaboratore, con o senza captazione di dati"* (pag. 12). Di contro, nelle ipotesi meramente residuali in cui non risulta rintracciabile la piattaforma su cui ha operato il *client*, trovano ambito applicativo i criteri tracciati dall'art. 9 c.p.p.

5. In definitiva, le Sezioni Unite confermano la strada partenopea quale luogo di ubicazione della Motorizzazione civile di Napoli, impostazione correttamente suggerita dal giudice rimettente che era stato chiamato a risolvere il conflitto negativo di competenza *ratione territori*. Irrilevante è il fatto che il giudice capitolino coincida con il luogo ove si trova il *server* in quanto, considerando il sistema informatico nella sua unitarietà e immaterialità, non v'è ragione alcuna per centralizzare la competenza

REPUBBLICA ITALIANA

In nome del Popolo Italiano

LA CORTE SUPREMA DI CASSAZIONE

SEZIONI UNITE PENALI

Composta da

Giorgio Santacroce	- Presidente -	Sent. n. sez. 10
Gennaro Marasca		CC 26/03/2015
Claudia Squassoni	- Relatore -	R.G.N. 35519/2014
Giovanni Conti		
Giacomo Paoloni		
Luisa Bianchi		
Paolo Antonio Bruno		
Alberto Macchia		
Margherita Cassano		

ha pronunciato la seguente

SENTENZA

sul conflitto di competenza sollevato dal
Giudice della udienza preliminare del Tribunale di Roma
nel procedimento nei confronti di
1. Rocco Michelina, nata a Cervinara il 01/09/1957
2. Schettino Giuseppe, nato a Castellammare di Stabia il 13/09/1979

visti gli atti;
udita la relazione svolta dal componente Claudia Squassoni;
udito il Pubblico Ministero, in persona dell'Avvocato generale Carlo Destro, che ha concluso chiedendo che sia dichiarata la competenza del G.u.p. del Tribunale di Napoli;
udito per la parte civile Ministero delle Infrastrutture l'Avvocato dello Stato Wally Ferrante, che ha concluso chiedendo che sia dichiarata la competenza del G.u.p. del Tribunale di Napoli;

uditi i difensori degli imputati Rocco Michelina e Schettino Giuseppe, rispettivamente, avv. Luigi Sena e avv. Pasquale Crea, che hanno entrambi concluso chiedendo che sia dichiarata la competenza del G.u.p. del Tribunale di Roma.

RITENUTO IN FATTO

1. Il Procuratore della Repubblica presso il Tribunale di Napoli ha esercitato l'azione penale nei confronti di Michelina Rocco e Giuseppe Schettino in ordine al reato previsto dagli artt. 81, 110, 615-*ter*, secondo e terzo comma, cod. pen., perché, in concorso tra loro ed agendo la Rocco in qualità di impiegata della Motorizzazione civile di Napoli, si introducevano abusivamente e ripetutamente nel sistema informatico del Ministero delle Infrastrutture e dei Trasporti per effettuare visure elettroniche che esulavano dalle mansioni della imputata ed interessavano lo Schettino (amministratore di una agenzia di pratiche automobilistiche).

Con sentenza in data 2 dicembre 2013, il Giudice della udienza preliminare del Tribunale di Napoli ha dichiarato la propria incompetenza per territorio ritenendo competente il Giudice del Tribunale di Roma in ragione della ubicazione della banca-dati della Motorizzazione civile presso il Ministero delle Infrastrutture e dei Trasporti con sede in Roma.

Chiesto il rinvio a giudizio da parte del Procuratore della Repubblica per entrambi gli imputati, il Giudice della udienza preliminare del Tribunale di Roma, con ordinanza del 16 giugno 2014, ha sollevato conflitto negativo di competenza per territorio ritenendo che il luogo di consumazione del reato di accesso abusivo ad un sistema informatico dovesse radicarsi ove agiva l'operatore remoto e, pertanto, a Napoli.

2. La Prima Sezione penale, cui il ricorso è stato assegnato tabellarmente, con ordinanza n. 52575 del 28 ottobre 2014, depositata il 18 dicembre 2014, rilevato un potenziale contrasto di giurisprudenza, ha rimesso gli atti alle Sezioni Unite.

Con decreto in data 23 dicembre 2014 il Primo Presidente ha assegnato il ricorso alle Sezioni Unite, fissandone per la trattazione l'odierna udienza camerale.

CONSIDERATO IN DIRITO

1. Il quesito posto alle Sezioni Unite è il seguente: "*Se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615*-ter*, cod. pen., sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il* server *che elabora e controlla le credenziali di autenticazione fornite dall'agente*".

1.1. La questione è di particolare rilievo dal momento che il reato informatico, nella maggior parte dei casi, si realizza a distanza in presenza di un collegamento telematico tra più sistemi informatici con l'introduzione illecita, o non autorizzata, di un soggetto, all'interno di un elaboratore elettronico, che si trova in luogo diverso da quello in cui è situata la banca-dati.

Gli approdi ermeneutici hanno messo in luce due opposte soluzioni che si differenziano nel modo di intendere la spazialità nei reati informatici: per alcune, competente per territorio è il tribunale del luogo nel quale il soggetto si è connesso alla rete effettuando il collegamento abusivo, per altre, il tribunale del luogo ove è fisicamente allocata la banca-dati che costituisce l'oggetto della intrusione.

1.2. Una sola sentenza della Corte di cassazione ha approfondito il tema in esame, individuando la competenza territoriale nel luogo ove è allocato il *server* (Sez. 1, n. 40303 del 27/05/2013, Martini, Rv. 257252).

Secondo tale impostazione, ciò che rileva ai fini della integrazione del delitto è il momento in cui viene posta in essere la condotta che si connota per l'abusività (inconferenti essendo le finalità perseguite) che si perfeziona quando l'agente, interagendo con il sistema informatico o telematico altrui, si introduce in esso contro la volontà di chi ha il diritto di estromettere l'estraneo.

Posta la centralità del *jus excludendi*, la fattispecie si perfeziona nel momento in cui il soggetto agente entra nel sistema altrui, o vi permane, in violazione del domicilio informatico, sia che vi si introduca contro la volontà del titolare sia che vi si intrattenga in violazione delle regole di condotta imposte. Il delitto può, di conseguenza, ritenersi consumato solo se l'agente, colloquiando con il sistema, ne abbia oltrepassato le barriere protettive o, introdottosi utilizzando un valido titolo abilitativo, vi permanga oltre i limiti di validità dello stesso.

Deriva che l'accesso si determina nel luogo ove viene effettivamente superata la protezione informatica e si verifica la introduzione nel sistema e, quindi, dove è materialmente situato il *server* violato, l'elaboratore che controlla le credenziali di autenticazione del *client*.

Il luogo di consumazione del reato non è dunque quello in cui vengono inserite le credenziali di autenticazione, ma quello in cui si entra nel *server* dal momento che la procedura di accesso deve ritenersi atto prodromico alla introduzione nel sistema.

Nella ipotesi di accesso da remoto, l'attività fisica viene esercitata in luogo differente da quello in cui si trova il sistema informatico o telematico protetto, ma è certo che il *client* invia le chiavi logiche al *server web* il quale le riceve "processandole" nella fase di validazione che è eseguita unicamente all'interno dell'elaboratore presidiato da misure di sicurezza.

In sostanza, l'opzione ermeneutica che ha fissato presso il *server* il luogo di consumazione del reato fa leva sulla constatazione che l'effettivo ingresso di cui trattasi si verifica solo presso il sistema centrale con il superamento delle barriere logiche dopo la immissione delle credenziali di autenticazione da remoto.

Altra sentenza (Sez. 3, n. 23798 del 24/05/2012, Casalini, Rv. 253633), pur senza approfondire, ha affermato, in riferimento al diverso reato di frode informatica, che la competenza territoriale deve essere individuata nel luogo in cui si trova il *server* all'interno del quale sono archiviati i dati oggetto di abusivo trattamento.

1.3. Un significativo segnale di mutamento in ordine alla riflessione giurisprudenziale sul luogo di consumazione del reato di accesso abusivo a sistema informatico può cogliersi in una decisione (Sez. 1, n. 34165 del 15/06/2014, De Bo, non massimata); la Corte, nel risolvere il conflitto di competenza sollevato dall'autorità giudiziaria del luogo di digitazione della *password* di accesso alle risorse informatiche, ha rilevato come la questione (non conferente nel caso in esame) fosse fondata su argomenti giuridici e scientifici meritevoli di attento esame critico e, quindi, di ulteriore analisi in sede di ricostruzione dell'elemento oggettivo del reato di cui all'art. 615-*ter* cod. pen.

La ordinanza di rimessione alle Sezioni Unite – dopo avere evidenziato che il *client* ed il *server* sono componenti di un unico sistema telematico – osserva che l'accesso penalmente rilevante inizia dalla postazione remota ed il perfezionamento del reato avviene nel luogo ove si trova l'utente (diverso da quello in cui è ubicato il *server*).

1.4. La impostazione della ricordata sentenza n. 40303 del 2013 della Corte di cassazione è criticata dal Giudice rimettente (e da parte della dottrina) che puntualizza come l'intera architettura di un sistema per la gestione e lo scambio di dati (*server*, *client*, terminali e rete di trasporto delle informazioni) corrisponde, in realtà, ad una sola unità di elaborazione, altrimenti definita "sistema telematico".

In questa prospettiva, il terminale mediante il quale l'operatore materialmente inserisce *username* e *password* è ricompreso, quale elemento strutturale ed essenziale, nell'intera rete di trattamento e di elaborazione dei dati, assumendo rilevanza il luogo di ubicazione della postazione con cui l'utente accede o si introduce nel sistema che contiene l'archivio informatico.

2. Prima di esaminare la questione controversa, è opportuno puntualizzare, nello stretto ambito richiesto per risolvere il quesito, la struttura della fattispecie dell'art. 615-*ter* cod. pen., iniziando dalla nozione di introduzione e trattenimento nel sistema.

La materia è già stata passata al vaglio delle Sezioni Unite (sent. n. 4694 del 27/10/2011, Casani, Rv. 25129) che ha precisato come le condotte descritte dalla norma sono punite a titolo di dolo generico e consistono:

a) nello introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza – da intendere come l'accesso alla conoscenza dei dati o informazioni contenute nello stesso – effettuato sia da lontano (condotta tipica dello *hacker*), sia da vicino (cioè da persona che si trova a diretto contatto con lo elaboratore);

b) nel mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione, da intendere come il persistere nella già avvenuta introduzione, inizialmente autorizzata o casuale, violando le disposizioni, i limiti e i divieti posti dal titolare del sistema.

2.1. Nel caso che ci occupa (almeno dagli atti in visione di questa Corte) risulta che la Rocco, pur avendo titolo e formale abilitazione per accedere alle informazioni in ragione della sua qualità di dipendente della competente amministrazione e di titolare di legittime chiavi di accesso, si è introdotta all'interno del sistema, in esecuzione di un previo accordo criminoso con il coimputato al fine di consultare l'archivio per esigenze diverse da quelle di servizio; pertanto, la condotta deve essere considerata di per sé illecita sin dal momento dell'accesso, essendo irrilevante la successiva condotta di mantenimento.

2.2. Per quanto concerne il bene giuridico, va ricordato che l'art. 615-*ter* cod. pen è stato introdotto nel nostro ordinamento in esito alla Raccomandazione del Consiglio di Europa del 1989 per assicurare una protezione all'ambiente informatico o telematico che contiene dati personali che devono rimanere riservati e conservati al riparo da ingerenze ed intrusioni altrui e rappresenta un luogo inviolabile, delimitato da confini virtuali, paragonabile allo spazio privato dove si svolgono le attività domestiche.

Per questo la fattispecie è stata inserita nella Sezione IV del Capo III del Titolo XII del Libro II del codice penale, dedicata ai delitti contro la inviolabilità del domicilio, che deve essere inteso come luogo, anche virtuale, dove l'individuo esplica liberamente la sua personalità in tutte le sue dimensioni e manifestazioni.

E' stato notato che, con la previsione dell'art. 615-*ter* cod. pen. il legislatore ha assicurato la protezione del domicilio informatico quale spazio ideale in cui sono contenuti i dati informatici di pertinenza della persona ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene costituzionalmente protetto; all'evidenza il parallelo con il domicilio reale – sulla cui falsariga è stata strutturata la norma – è imperfetto.

In realtà, la fattispecie offre una tutela anticipata ad una pluralità di beni giuridici e di interessi eterogenei e non si limita a preservare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma ne offre una protezione da qualsiasi tipo di intrusione che possa avere anche ricadute economico-patrimoniali (Sez. 4, n. 3067 del 04/10/1999, Piersanti, Rv. 214946).

E' condivisa l'opinione secondo la quale il delitto previsto dall'art. 615-*ter* cod. pen. è di mera condotta (ad eccezione per le ipotesi aggravate del comma secondo, nn. 2 e 3) e si perfeziona con la violazione del domicilio informatico – e, quindi, con la introduzione nel relativo sistema – senza la necessità che si verifichi una effettiva lesione del diritto alla riservatezza dei dati (Sez. 5, n. 11689 del 06/02/2007, Cerbone, Rv. 236221).

Dal momento che oggetto di tutela è il domicilio virtuale, e che i dati contenuti all'interno del sistema non sono in via diretta ed immediata protetti, consegue che l'eventuale uso illecito delle informazioni può integrare un diverso titolo di reato (Sez. 5, n. 40078 del 25/05/2009, Genchi, Rv. 244749).

2.3. Il legislatore, introducendo con la legge 23 dicembre 1993, n. 547, i cosiddetti *computer's crimes*, non ha enunciato la definizione di sistema informatico o telematico (forse per lasciare aperta la nozione in vista dell'evoluzione della tecnologia), ma ne ha presupposto il significato.

In argomento, l'art. 1 della Convenzione Europea di Budapest del 23 novembre 2001, definisce sistema informatico «qualsiasi apparecchiature o gruppi di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati».

La giurisprudenza ha fornito una definizione tendenzialmente valida per tutti i reati facenti riferimento alla espressione "sistema informatico", che deve intendersi come 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 una attività di

"codificazione" e "decodificazione", dalla "registrazione" o "memorizzazione" tramite impulsi elettronici, su supporti adeguati, di "dati", cioè, di rappresentazioni elementari di un fatto, effettuata attraversi simboli (*bit*) in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni costituite da un insieme più o meno vasto di informazioni organizzate secondo una logica che consente loro di esprimere un particolare significato per l'utente (Sez. 6, n. 3067 del 04/10/1999, Piersanti, Rv. 214945).

In generale, un dispositivo elettronico assurge al rango di sistema informatico o telematico se si caratterizza per l'installazione di un *software* che ne sovrintende il funzionamento, per la capacità di utilizzare periferiche o dispositivi esterni, per l'interconnessione con altri apparecchi e per la molteplicità dei dati oggetto di trattamento.

Per evitare vuoti di tutela e per ampliare la sfera di protezione offerta ai sistemi informatici e telematici, è opportuno accogliere la nozione più ampia possibile di *computer* o unità di elaborazione di informazioni, come del resto la Corte ha già fatto in materia di carte di pagamento, trattandosi di strumenti idonei a trasmettere dati elettronici nel momento in cui si connettono all'apparecchiatura POS (così Sez. F, n. 43755 del 23/08/2012, Chiriac, Rv. 253583).

Nell'ambito della protezione offerta dall'art. 615-*ter* cod. pen. ricadono anche i sistemi di trattamento delle informazioni che sfruttano l'architettura di rete denominata *client-server*, nella quale un *computer* o terminale (il *client*) si connette tramite rete ad un elaboratore centrale (il *server*) per la condivisione di risorse o di informazioni, che possono essere rese disponibili a distanza anche ad altri utenti.

La tutela giuridica è riservata ai sistemi muniti di misure di sicurezza perché, dovendosi proteggere il diritto di uno specifico soggetto, è necessario che questo abbia dimostrato di volere riservare l'accesso alle persone autorizzate e di inibire la condivisione del suo spazio informatico con i terzi.

3. La condotta illecita commessa in un ambiente informatico o telematico assume delle specifiche peculiarità per cui la tradizionale nozione – elaborata per una realtà fisica nella quale le conseguenze sono percepibili e verificabili con immediatezza – deve essere rivisitata e adeguata alla dimensione virtuale.

In altre parole, il concetto di azione penalmente rilevante subisce nella realtà virtuale una accentuata modificazione fino a sfumare in impulsi elettronici; l'*input* rivolto al *computer* da un atto umano consapevole e volontario si traduce in un trasferimento sotto forma di energie o *bit* della volontà dall'operatore all'elaboratore elettronico, il quale procede automaticamente alle operazioni di

codificazione, di decodificazione, di trattamento, di trasmissione o di memorizzazione di informazioni.

L'azione telematica viene realizzata attraverso una connessione tra sistemi informatici distanti tra loro, cosicché gli effetti della condotta possono esplicarsi in un luogo diverso da quello in cui l'agente si trova; inoltre, l'operatore, sfruttando le reti di trasporto delle informazioni, è in grado di interagire contemporaneamente sia sul *computer* di partenza sia su quello di destinazione.

E' stato notato che nel *cyberspace* i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorte di meta-territorio).

Pertanto non è sempre agevole individuare con certezza una sfera spaziale suscettibile di tutela in un sistema telematico, che opera e si connette ad altri terminali mediante reti e protocolli di comunicazione.

Del resto, la dimensione aterittoriale si è incrementata da ultimo con la diffusione dei dispositivi mobili (*tablet*, *smartphone*, sistemi portatili) e del *cloud computing*, che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate dalle quali è possibile accedere da qualunque parte del globo.

Va comunque precisato che, se i dati oggetto di accesso abusivo sono archiviati su *cloud computing* o resi disponibili da *server* che sfruttano tali servizi, potrebbe risultare estremamente difficile individuare il luogo nel quale le informazioni sono collocate.

4. Le esposte osservazioni sono utili per risolvere la questione sottoposta alle Sezioni Unite.

In estrema sintesi, si può rilevare che le due teorie contrapposte sul luogo del commesso reato si ancorano l'una (quella della Prima Sezione della Corte di cassazione) sul concetto classico di fisicità del luogo ove è collocato il *server* e l'altra (quella del Giudice rimettente) sul funzionamento delocalizzato, all'interno della rete, di più sistemi informatici e telematici.

Ora – pur non sminuendo le difficoltà di trasferire al caso concreto il criterio attributivo della competenza territoriale dell'art. 8 cod. proc. pen. parametrato su spazi fisici e non virtuali – la Corte reputa sia preferibile la tesi del Giudice remittente, che privilegia le modalità di funzionamento dei sistemi informatici e telematici, piuttosto che il luogo ove è fisicamente collocato il *server*.

4.1. Deve, innanzitutto, ricordarsi come l'abusiva introduzione in un sistema informatico o telematico – o il trattenimento contro la volontà di chi ha diritto di esclusione – sono le uniche condotte incriminate, e, per quanto rilevato, le relative nozioni non sono collegate ad una dimensione spaziale in senso tradizionale, ma a quella elettronica, trattandosi di sistemi informatici o telematici che archiviano e gestiscono informazioni ossia entità immateriali.

Tanto premesso, si rileva come la ricordata sentenza della Prima Sezione abbia ritenuto che l'oggetto della tutela concreta coincida con l'ambito informatico ove sono collocati i dati, cioè con il *server* posto in luogo noto.

Tale criterio di articolare la competenza in termini di fisicità, secondo gli abituali schemi concettuali del mondo materiale, non tiene conto del fatto che la nozione di collocazione spaziale o fisica è essenzialmente estranea alla circolazione dei dati in una rete di comunicazione telematica e alla loro contemporanea consultazione da più utenti spazialmente diffusi sul territorio.

Non può essere condivisa, allora, la tesi secondo la quale il reato di accesso abusivo si consuma nel luogo in cui è collocato il *server* che controlla le credenziali di autenticazione del *client*, in quanto, in ambito informatico, deve attribuirsi rilevanza, più che al luogo in cui materialmente si trova il sistema informatico, a quello da cui parte il dialogo elettronico tra i sistemi interconnessi e dove le informazioni vengono trattate dall'utente.

Va rilevato, infatti, come il sito ove sono archiviati i dati non sia decisivo e non esaurisca la complessità dei sistemi di trattamento e trasmissione delle informazioni, dal momento che nel cyberspazio (la rete *internet*) il flusso dei dati informatici si trova allo stesso tempo nella piena disponibilità di consultazione (e, in certi casi, di integrazione) di un numero indefinito di utenti abilitati, che sono posti in condizione di accedervi ovunque.

Non è allora esatto ritenere che i dati si trovino solo nel *server*, perché nel reato in oggetto l'intera banca dati è "ubiquitaria", "circolare" o "diffusa" sul territorio, nonché contestualmente compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate all'accesso.

A dimostrazione della unicità del sistema telematico per il trattamento dei dati, basti considerare che la traccia delle operazioni compiute all'interno della rete e le informazioni relative agli accessi sono reperibili, in tutto o in parte, sia presso il *server* che presso il *client*.

Né può in contrario sostenersi, come afferma l'orientamento che in questa sede si ritiene di non condividere, che le singole postazioni remote costituiscano meri strumenti passivi di accesso al sistema principale e non facciano altrimenti parte di esso.

4.2. Da un punto di vista tecnico-informatico, il sistema telematico deve considerarsi unitario, essendo coordinato da un *software* di gestione che presiede al funzionamento della rete, alla condivisione della banca dati, alla archiviazione delle informazioni, nonché alla distribuzione e all'invio dei dati ai singoli terminali interconnessi.

Consegue che è arbitrario effettuare una irragionevole scomposizione tra i singoli componenti dell'architettura di rete, separando i terminali periferici dal *server* centrale, dovendo tutto il sistema essere inteso come un complesso inscindibile nel quale le postazioni remote non costituiscono soltanto strumenti passivi di accesso o di interrogazione, ma essi stessi formano parte integrante di un complesso meccanismo, che è strutturato in modo da esaltare la funzione di immissione e di estrazione dei dati da parte del *client*.

I terminali, secondo la modulazione di profili di accesso e l'organizzazione della banca-dati, non si limitano soltanto ad accedere alle informazioni contenute nel *data base*, ma sono abilitati a immettere nuove informazioni o a modificare quelle preesistenti, con potenziale beneficio per tutti gli utenti della rete, che possono fruire di dati più aggiornati e completi per effetto dell'interazione di un maggior numero di operatori.

Alla luce di questa considerazione, va focalizzata la nozione di accesso in un sistema informatico, che non coincide con l'ingresso all'interno del *server* fisicamente collocato in un determinato luogo, ma con l'introduzione telematica o virtuale, che avviene instaurando un colloquio elettronico o circuitale con il sistema centrale e con tutti i terminali ad esso collegati.

L'accesso inizia con l'unica condotta umana di natura materiale, consistente nella digitazione da remoto delle credenziali di autenticazione da parte dell'utente, mentre tutti gli eventi successivi assumono i connotati di comportamenti comunicativi tra il *client* e il *server*.

L'ingresso o l'introduzione abusiva, allora, vengono ad essere integrati nel luogo in cui l'operatore materialmente digita la *password* di accesso o esegue la procedura di *login*, che determina il superamento delle misure di sicurezza apposte dal titolare del sistema, in tal modo realizzando l'accesso alla banca-dati.

Da tale impostazione, coerente con la realtà di una rete telematica, consegue che il luogo del commesso reato si identifica con quello nel quale dalla postazione remota l'agente si interfaccia con l'intero sistema, digita le credenziali di autenticazione e preme il testo di avvio, ponendo così in essere l'unica azione materiale e volontaria che lo pone in condizione di entrare nel dominio delle informazioni che vengono visionate direttamente all'interno della postazione periferica.

Anche in tal senso rileva non il luogo in cui si trova il *server*, ma quello decentrato da cui l'operatore, a mezzo del *client*, interroga il sistema centrale che gli restituisce le informazioni richieste, che entrano nella sua disponibilità mediante un processo di visualizzazione sullo schermo, stampa o archiviazione su disco o altri supporti materiali.

Le descritte attività coincidono con le operazioni di "trattamento", compiute sul *client*, che l'art. 4, lett. *a*), d.lgs. 30 giugno 2003, n. 196 (codice della *privacy*) definisce come «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».

La condotta è già abusiva (secondo la clausola di antigiuridicità speciale) nel momento in cui l'operatore non autorizzato accede al *computer* remoto e si fa riconoscere o autenticare manifestando, in tale modo, la sua volontà di introdursi illecitamente nel sistema con possibile violazione della integrità dei dati.

Deve precisarsi in ogni caso che, se il *server* non risponde o non valida le credenziali, il reato si fermerà alla soglia del tentativo punibile.

Nelle ipotesi, davvero scolastiche e residuali, nelle quali non è individuabile la postazione da cui agisce il *client*, per la mobilità degli utenti e per la flessibilità di uso dei dispositivi portatili, la competenza sarà fissata in base alle regole suppletive (art. 9 cod. proc. pen.).

4.3. Il luogo in cui l'utente ha agito sul *computer* – che nella maggior parte dei casi, è quello in cui si reperiscono le prove del reato e la violazione è stata percepita dalla collettività – è consono al concetto di giudice naturale, radicato al *locus commissi delicti* di cui all'art. 25 Cost.

La Corte costituzionale, infatti, non ha mancato di sottolineare al riguardo (v. sentenza n. 168 del 2006) come il predicato della "naturalità" del giudice finisca per assumere 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 quella – più che tradizionale – per la quale il diritto e la giustizia devono riaffermarsi proprio nel luogo in cui sono stati violati». In tale cornice, se l'azione dell'uomo si è realizzata in un certo luogo – sia pure attraverso l'uso di uno strumento informatico e, dunque, per sua natura destinato a produrre flussi di dati privi di una loro "consistenza territoriale" – non v'è ragione alcuna per ritenere che quel "fatto", qualificato dalla legge come reato, non si sia verificato proprio in quel

luogo, così da consentire la individuazione di un giudice anche "naturalisticamente" (oltre che formalmente) competente. Predicato, quello di cui si è detto, che, al contrario, non potrebbe ritenersi affatto soddisfatto ove si facesse leva sulla collocazione, del tutto casuale, del *server* del sistema violato.

4.4. D'altra parte, che il fulcro della attenzione normativa sia stato, per così dire, allocato nel luogo in cui si trova ad operare l'autore del delitto – evocando, dunque, una sorta di sincretismo tra la localizzazione dell'impianto informatico utilizzato per realizzare il fatto-reato e la persona che, proprio attraverso quell'impianto, accede e dialoga col sistema nella sua indefinibile configurazione spaziale – lo si può desumere anche dal modo in cui risultano strutturate le circostanze aggravanti previste dal comma secondo dell'art. 615-*ter* cod. pen.

Se si considera, infatti, l'aggravante di cui al numero 2 del predetto comma, non avrebbe senso alcuno immaginare una competenza per territorio saldata al luogo – in ipotesi del tutto eccentrico rispetto al "fatto" – in cui si trova il *server*, visto che è proprio l'attività violenta dell'agente (e, dunque, la relativa collocazione territoriale) a specificare, naturalisticamente, il *locus commissi delicti*. Allo stesso modo, è sempre il luogo in cui si trova ed opera l'agente ad essere quello che meglio individua il "fatto", ove da esso sia derivata, a norma del numero 3, la interruzione, la distruzione o il danneggiamento del sistema o di qualche sua componente: è l'operazione di manipolazione, infatti (si pensi alla introduzione di un *virus*) che qualifica, specificandola in chiave aggravatrice, la condotta punibile, con l'ovvia conseguenza che è l'azione umana (e non altro) a determinare il "fatto" e con esso il suo riferimento spazio-temporale. Circostanze, quelle testé evidenziate, che valgono anche per l'aggravante dell'abuso della qualità pubblica dell'autore del fatto di cui al numero 1, posto che – ancora una volta – è sempre la condotta di accesso a indicare "chi", "dove" e "quando" hanno realizzato la fattispecie incriminata, qualificandola "abusiva" in ragione delle specifiche disposizioni che regolano l'impiego del sistema.

5. Deve ora, per completezza, rilevarsi che la conclusione è trasferibile alla diversa ipotesi nella quale un soggetto facoltizzato ad introdursi nel sistema, dopo un accesso legittimo, vi si intrattenga contro la volontà del titolare eccedendo i limiti della autorizzazione.

In questo caso, non può farsi riferimento all'azione con la quale l'agente ha utilizzato le sue credenziali e dato l'avvio al sistema, dal momento che tale condotta commissiva è lecita ed antecedente alla perpetrazione del reato,

Necessita, quindi, fare leva sull'inizio della condotta omissiva che, come è stato puntualmente osservato, coincide con un uso illecito dello elaboratore, con o senza captazione di dati.

L'operatore remoto, anche in questo caso, si relaziona, con impulsi elettronici e colloquia con il sistema dalla sua postazione periferica presso la quale vengono trasferiti i dati con la conseguenza che è irrilevante il luogo in cui è collocato il *server* per le già dette ragioni.

6. Conclusivamente, va affermato il seguente principio di diritto:

"*Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615*-ter *cod. pen., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente*".

7. Consegue che nella specie deve essere dichiarata la competenza dell'autorità giudiziaria del Tribunale di Napoli, atteso che la condotta abusiva è stata contestata come materialmente realizzata dalla imputata Michelina Rocco negli uffici della Motorizzazione civile di Napoli, dove, servendosi del *computer* in dotazione dell'ufficio, essa si sarebbe introdotta abusivamente e ripetutamente nel sistema informatico del Ministero delle Infrastrutture e dei Trasporti.

P.Q.M.

dichiara la competenza del G.u.p. del Tribunale di Napoli, cui dispone trasmettersi gli atti.

Così deciso il 26/03/2015

Il Componente estensore
Claudia Squassoni

Il Presidente
Giorgio Santacroce

SEZIONI UNITE PENALI
Depositato in Cancelleria
il 24 APR. 2015
Il Funzionario Giudiziario
Leonardo Sacripanti

CORTE SUPREMA DI CASSAZIONE