M

40303/13

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

LA CORTE SUPREMA DI CASSAZIONE

PRIMA SEZIONE PENALE

UDIENZA CAMERA DI CONSIGLIO DEL 27/05/2013

Composta dagli Ill.mi Sigg.ri Magistrati:

Dott. SEVERO CHIEFFI	- Presidente -	SENTENZA N. 1921/2013
Dott. UMBERTO ZAMPETTI	- Consigliere -	
Dott. MARCELLO ROMBOLA'	- Consigliere -	REGISTRO GENERALE N. 49437/2012
Dott. MAURIZIO BARBARISI	- Consigliere -	
Dott. LUCIA LA POSTA	- Rel. Consigliere -	

ha pronunciato la seguente

SENTENZA

sul conflitto di competenza sollevato da:

GIP TRIBUNALE DI ROMA nei confronti di:

TRIBUNALE DI FIRENZE

con l'ordinanza n. 10547/2012 GIUDICE UDIENZA PRELIMINARE di ROMA, del 14/11/2012

sentita la relazione fatta dal Consigliere Dott. LUCIA LA POSTA;
letta/sentite le conclusioni del PG Dott. M. FRATICELLI che ha domandato dichiararsi la competenza del TRIBUNALE di FIRENZE;

Udito il difensore Avv. G. PULITI, difensore di ROSSO Silvio che ha chiesto dichiararsi la competenza del Tribunale di ROMA; nonché l'Avv. dello stesso Vv. FERRANTE che ha chiesto dichiararsi la competenza del Tribunale di FIRENZE;

RITENUTO IN FATTO

1. Con sentenza in data 29.6.2011 il Tribunale di Firenze dichiarava la propria incompetenza per territorio avuto riguardo al giudizio nei confronti degli imputati specificamente indicati in ordine ai reati agli stessi contestati e disponeva la trasmissione degli atti al Procuratore della repubblica presso il Tribunale di Roma.

Premessa la sussistenza della connessione tra i reati contestati e ritenuto più grave quello di cui all'art. 615 –*ter,* comma 2 e 3 cod. pen., affermava che – come sostenuto dalla difesa degli imputati – detta fattispecie deve ritenersi consumata in Roma, luogo in cui ha sede la banca dati riservata del Sistema d'informazione interforze del Ministero dell'Interno (SDI) nel quale, secondo la contestazione, è avvenuto l'accesso abusivo con l'acquisizione di dati segreti, successivamente comunicati dagli imputati ai committenti.

Evidenziava che l'interrogazione della banca dati con sede presso gli uffici del Ministero dell'Interno avviene attraverso terminali collegati, situati su tutto il territorio nazionale negli uffici abilitati, con la digitazione di credenziali di accesso dell'utente e che la condotta rilevante ai fini della consumazione del reato in contestazione è esclusivamente quella dell'introduzione nel sistema informatico, o della permanenza al suo interno. Pertanto, non possono prendersi in considerazione, ai fini della determinazione del luogo di consumazione del reato, né le eventuali condotte successive di acquisizione ed uso dei dati, né il luogo in cui l'accesso al sistema è iniziato attraverso i terminali i quali costituiscono strumenti di accesso privi di qualsiasi dato proprio. La procedura di accesso deve ritenersi, infatti, mero atto prodromico alla reale introduzione nel sistema informatico che avviene solo nel momento in cui si entra effettivamente nello SDI, dopo avere lanciato l'accesso e completato la validazione delle credenziali dell'utente che viene fatta dal sistema centrale che si trova a Roma.

Dava atto, altresì, della circostanza, introdotta dalla difesa, che quanto meno sino al 2009 il sistema informatico in oggetto era costituito da un unico grande elaboratore situato a Roma al quale si accedeva dai terminali periferici in grado di dialogare soltanto con l'elaboratore a cui erano collegati tramite *modem,* così che soltanto l'introduzione nell'elaboratore centrale consente il dialogo e la estrazione delle informazioni di interesse. Ad avviso del tribunale, quindi, le postazioni periferiche non possono essere neppure considerate parte integrante del sistema - come affermato dal pubblico ministero - in quanto, almeno sino alla data di consumazione dei reati contestati, il sistema in esame è costituito da un contenitore centrale, sito in Roma, nel quale bisogna

necessariamente introdursi per estrarne i dati, mentre i *computers* periferici sono lo strumento che rende possibile l'introduzione nel sistema.

Pertanto, è irrilevante, ai fini della individuazione del luogo di consumazione del reato, da quale luogo sia iniziata la procedura di accesso, tenuto conto che la norma di cui all'art. 615 *-ter* cod. pen. punisce la mera introduzione nella banca dati.

2. Il Gup del Tribunale di Roma, investito del procedimento con la richiesta di rinvio a giudizio del pubblico ministero, sollevava il conflitto di competenza, trasmettendo gli atti a questa Corte.

Concordava sulla circostanza che la banca dati si trova a Roma presso gli uffici del Ministero dell'Interno; che alla stessa si accede con interrogazione fatta dai terminali collegati dopo la digitazione delle credenziali di accesso; che ai fini della determinazione del luogo di consumazione del reato in oggetto non è rilevante il luogo dell'acquisizione dei dati, bensì, il luogo dell'accesso.

Rilevava, tuttavia, che l'accesso punito dall'art. 615 *-ter* cod. pen. si colloca in un contesto immateriale e delocalizzato che è la rete di comunicazione telematica ed è un reato di mera condotta che - come affermato dalla giurisprudenza di legittimità - si perfeziona con la violazione del domicilio informatico (Sez. 5, n. 11689 del 06/02/2007, Cerbone, rv. 236221). Per determinare la competenza, quindi, si deve avere riguardo all'ultima attività umana che si connota per fisicità, rappresentata dall'accesso dal terminale, ossia al luogo della collocazione del terminale attivato per l'accesso.

La condotta umana, infatti, 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, tenuto conto, altresì, che tale azione, una volta posta in essere, non è più suscettibile di essere interrotta nei suoi esiti.

Illogica sarebbe la soluzione di individuare all'interno di un sistema informatico un luogo di collocazione fisica idoneo a spostare giuridicamente la competenza come se si operasse all'interno di uno sistema caratterizzato da spazio e tempo. Del resto, secondo la Corte di legittimità deve intendersi per <<sistema informatico>> - con riferimento alla ricorrente espressione utilizzata nella legge 23 dicembre 1993, n. 547 che ha introdotto nel codice penale i cosiddetti *computer's crimes* - un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche che sono caratterizzate - per mezzo di un'attività di <<codificazione>> e <<decodificazione>> - dalla <<registrazione>> o <<memorizzazione>>, per mezzo di impulsi elettronici, su supporti adeguati di dati, cioè di rappresentazioni elementari di un fatto

effettuata attraverso simboli (bit) in combinazione diverse e dalla elaborazione automatica di tali dati in modo da generare informazioni costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente.

Affermava, quindi, che la tesi sostenuta dal Tribunale di Firenze sovrappone arbitrariamente le regole che dominano il sistema fisico, nel quale si commette il reato mediante accesso al terminale, a quelle del sistema informatico nel quale si verifica l'ingresso nella banca dati, mentre il concetto di collocazione spaziale è concetto fisico che non ha diritto di cittadinanza in una rete telematica fondata sulla coesistenza dei flussi informatici.

Infine, riteneva ingiustificati i timori manifestati dal giudice di Firenze in ordine alle conseguenze di possibili accessi abusivi ai sistemi informatici italiani commessi all'estero, tenuto conto delle disposizioni dell'art. 6 cod. pen..

3. Con memoria in data 9.5.2013 il Ministero dell'Interno, il Ministero della Difesa ed il Ministero dell'Economia, a mezzo dell'Avvocatura della Stato affermano la competenza del Tribunale di Firenze. Rilevano che la diversa interpretazione sostenuta dai giudici di Firenze è fondata sulla netta separazione tra la fase di immissione delle credenziali e quella del vero e proprio accesso al sistema con una non condivisibile frammentazione della condotta, atteso che l'immissione all'interno della banca dati non appare logicamente scindibile dall'accesso effettuato dal terminale remoto. Si ha accesso quando l'operatore è in grado di dialogare con il sistema avendo superato le iniziali validazioni, ossia nel momento in cui dal terminale remoto vengono inviate le <<stringhe di comando>> idonee a forzare il *firewall* o sistema di sicurezza posto a protezione dei dati. In tale momento la volontà delittuosa si realizza in modo inequivocabile ed irreversibile e, dunque, si consuma la condotta criminosa.

Lo SDI è la banca dati del Ministero dell'Interno, sistema informatico composto dall'*hardware* che si trova presso il ministero e da tutti i terminali remoti presenti sul territorio nazionale che interagiscono tra loro e attraverso i quali vengono alimentate e gestite tutte le informazioni che confluiscono nella banca dati. Pertanto, l'utilizzo di credenziali nell'elaboratore remoto determina l'istantaneo perfezionamento della fattispecie delittuosa.

4. L'imputato Silvio Russo, a mezzo del difensore di fiducia, con memoria depositata il 20.5.2013, chiede determinarsi la competenza del Tribunale di Roma, ribadendo quanto già rappresentato innanzi al Tribunale di Firenze.

CONSIDERATO IN DIRITTO

Il conflitto sussiste, in quanto due giudici ordinari contemporaneamente ricusano la cognizione del medesimo fatto loro deferito, dando così luogo a quella situazione di stallo processuale, prevista dall'art. 28 cod. proc. pen., e la cui risoluzione è demandata a questa Corte dalla norme successive.

Tale conflitto deve essere risolto, ad avviso del Collegio, dichiarando la competenza del Gup del Tribunale di Roma.

La fattispecie contestata agli imputati che, ai sensi dell'art. 16 cod. proc. pen. in quanto reato più grave, determina la competenza per territorio è quella di cui agli artt. 110, 81, 615 *–ter* comma 2 e 3 cod. pen., continuato abusivo accesso alla banca dati del Sistema telematico di informazione interforze del Ministero dell'Interno, commesso con la complicità di appartenenti alla polizia di Stato per l'acquisizione di notizie riservate tratte dagli archivi informatici d'ufficio per l'utilizzo in attività di investigazione privata in agenzie facenti capo agli indagati o nelle quali gli stessi prestavano la loro attività.

Entrambi i giudici convengono che il delitto di accesso abusivo ad un sistema informatico, previsto dall'art. 615 *–ter* cod.pen., è reato di mera condotta che si perfeziona con la violazione del domicilio informatico e, quindi, con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa (Sez. 5, n. 11689 del 06/02/2007, Cerbone, rv. 236221); tuttavia, pervengono a conclusioni difformi quanto alla individuazione del momento e del luogo in cui si perfeziona detta violazione.

Invero - come hanno chiarito le Sezioni unite di questa Corte (Sez. U, n. 4694, 27 ottobre 2011, Casani, rv. 251270) le condotte tipiche punite dall'art. 615 *-ter* cod. pen., a dolo generico, consistono: a) nell'introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, da intendersi come accesso alla conoscenza dei dati o informazioni contenuti nel sistema, effettuato sia da lontano (attività tipica dell'*hacker*) sia da vicino (da persona, cioè, che si trova a diretto contatto dell'elaboratore); b) nel mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione, nel senso di persistere nella già avvenuta introduzione, inizialmente autorizzata, continuando ad accedere alla conoscenza dei dati nonostante il divieto, anche tacito, del titolare del sistema. E' il caso in cui l'accesso di un soggetto sia autorizzato per il compimento di operazioni determinate e per il relativo tempo necessario ed il soggetto medesimo, compiuta l'operazione espressamente

consentita, si intrattenga nel sistema per la presa di conoscenza non autorizzata dei dati.

Ciò che rileva, pertanto, ai fini dell'integrazione del delitto e della sua consumazione è il momento in cui viene posta in essere la condotta che si connota per abusività, a prescindere dalle finalità perseguite, allorquando l'utente, relazionandosi con il sistema informatico altrui, si introduce in esso contro la volontà del soggetto che ha il diritto di esclusione dell'*extraneus,* ovvero si mantiene all'interno del medesimo contro lo stesso consenso del *dominus*. L'accesso o il mantenimento abusivi sono puniti, dunque, in quanto tali non rilevando lo scopo perseguito dall'utente che rimane un fatto ultroneo rispetto alla condotta punibile, potendo, infatti, il *client* abusivo aver voluto violare il sistema per mero atto dimostrativo, ma anche per danneggiare il sistema, ovvero per accedere a informazioni riservate onde apprenderle per le ragioni più svariate. Da qui la natura eventualmente strumentale dell'accesso abusivo che ben può concorrere con altri delitti, informatici e non.

L'abusività dell'intrusione o di mantenimento non consentito nel sistema, necessaria ai fini dell'integrazione del reato, presuppone che sia espressa in modo manifesto ed inequivocabile, avuto riguardo alle due condotte tipiche sopra delineate, la volontà dell'avente diritto di non consentire a chiunque l'accesso al proprio domicilio informatico, ovvero di regolamentarlo (nel tempo e nello spazio). Tale intenzione si esprime più comunemente mediante l'apposizione di misure di sicurezza logiche, anche di minima efficacia e facilmente aggirabili, che, tuttavia, assolvono alla specifica funzione di manifestare la volontà di non diffusione a persone non autorizzate. Ma lo *jus excludendi* può esercitarsi anche solo con la fissazione da parte del *dominus loci* di specifiche prescrizioni comportamentali per l'utente (spesso ben esplicitate al momento dell'accesso o sulla *home page* del sito) ovvero attraverso qualsiasi altro meccanismo di selezione dei soggetti abilitati come la collocazione di strumenti esterni al sistema e meramente organizzativi destinati a regolare l'ingresso fisico nei locali in cui gli impianti informatici sono custoditi. Ciò significa che la protezione può essere predisposta non solo con una perimetrazione logica (del tipo *password* o *hardware* del tipo *firewall*), ma anche soltanto con misure c.d. fisiche (es. servizio di vigilanza, porte blindate, sistemi di allarme ecc.).

Posta la centralità dello *jus excludendi* ai fini della configurabilità del reato, la fattispecie si perfeziona, quindi, nel momento in cui il soggetto agente entra nel sistema informatico altrui, o vi permane, in violazione del domicilio informatico, sia se vi si introduca *invito domino*, sia se vi si trattenga in trasgressione delle specifiche regole di condotta imposte.

Il delitto può ritenersi, conseguentemente, consumato solo se il soggetto agente, colloquiando con il sistema altrui, ne abbia oltrepassato le barriere

protettive o, introdottosi con un titolo abilitativo valido, vi permanga oltre i limiti di validità di tale titolo; solo con l'aggiramento del dissenso del *dominus loci* è leso l'interesse protetto dalla norma.

Quanto sin qui precisato influisce, all'evidenza, sulla individuazione del luogo e del momento in cui avviene l'accesso abusivo, ossia in cui si consuma il reato, con quel che ne consegue ai fini della determinazione della competenza territoriale.

L'accesso, per quel che si è detto, avviene 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.*

Tanto a maggior ragione nella fattispecie concreta che - stando, naturalmente, alla condotta descritta nelle imputazioni - si riferisce all'accesso ad un sistema ben individuato, il Sistema D'Indagine cd. SDI, che ha sede presso il Ministero dell'Interno, da parte di soggetti abilitati con le necessarie credenziali dalla postazione terminale ufficiale.

Detto sistema è stato istituito dall'art. 8 della legge n. 121 del 1981 presso il Ministero dell'Interno per la raccolta delle informazioni e dei dati inerenti all'attività di cui agli artt. 6, lett. a) e 7 della stessa legge che sono custoditi nello SDI e posti a disposizione delle forze di polizia. Si tratta di un sistema chiuso e accessibile solo da postazioni di lavoro certificate che consentono l'acquisizione delle informazioni in sede locale utilizzando una rete *intranet*, senza esporsi ad interazioni con la rete pubblica. L'accesso alla banca dati, quindi, è possibile solo a persone debitamente autorizzate in sede locale dal proprio funzionario/ufficiale responsabile e previa abilitazione di un apposito profilo, diversificato a seconda delle informazioni che il personale deve conoscere in ragione delle mansioni da svolgere, avuto riguardo anche all'incarico ricoperto.

Quindi – come è stato evidenziato dal Tribunale di Firenze – la contestazione si riferisce all'accesso <<abusivo>> ad un sistema costituito da un unico *server* che conserva tutti i dati con il quale è avvenuto il collegamento da parte di un operatore abilitato.

Il luogo in cui si consuma il reato, quindi, non è quello nel quale vengono inseriti i dati idonei a entrare nel sistema, bensì, quello in cui si entra nel sistema che, nella specie, è e non può che essere il *server* che si trova a Roma.

Non possono prendersi in considerazione, pertanto, ai fini della determinazione del luogo di consumazione del reato, nè le eventuali condotte successive di acquisizione ed uso dei dati, né il luogo in cui l'accesso al sistema è iniziato attraverso i terminali che costituiscono strumenti di accesso. 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 che viene fatta dal sistema centrale che, nella specie, si trova a Roma.

D'altro canto, il luogo in cui si forma la volontà dell'agente di commettere il reato, ovvero quello in cui l'agente predispone le attività prodromiche e preparatorie, finalizzate alla condotta illecita, ben può essere diverso da quello nel quale si pone in essere la condotta giuridicamente rilevante e in cui, per i reati di mera condotta come quello in esame, si consuma il reato. E la condotta sanzionata non è costituita dall'utilizzo delle credenziali o altra attività equipollente effettuata nell'elaboratore remoto.

Non vi è dubbio che l'attività fisica dell'utente – come ha rilevato il Gup del Tribunale di Roma - viene ad essere esercitata, nell'ipotesi di accesso da remoto, in un luogo differente da quello in cui si trova il sistema informatico protetto, ma è anche certo che 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. Quindi, nel momento in cui l'utente dà l'invio all'esito alla 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*. D'altro canto, è sempre il *server web* violato che conserva le informazioni dell'accesso o della permanenza del *client,* mantenendo la traccia sul proprio *file log* di tutte le attività compiute a partire dall'accesso sino alla sua uscita dal sistema; tra queste vi è il numero IP del *client*, la sua *login*, la data dell'accesso e le pagine visitate.

Tanto non è incompatibile con il concetto di collocazione spazio-temporale della condotta che caratterizza e si pone a fondamento della competenza per territorio. Invero, il progresso tecnologico ha determinato l'insorgere di nuovi luoghi di espressione della personalità dell'individuo tra cui vi è senz'altro il sistema informatico all'interno del quale il soggetto conserva dati personali la cui diffusione ha diritto ad impedire e a controllare l'utilizzo dei dati inseriti in banche dati. Con la fattispecie in disamina, che evidenza uno spazio qualificato virtuale definibile come domicilio informatico, è stato riconosciuto e tutelato il diritto di un soggetto ad impedire la diffusione incontrollata e non gestita di informazioni che lo riguardano. Tale spazio acquista, quindi, una sua entità propria che lo separa dall'esterno e grazie all'esercizio dello *ius excludendi* è possibile accedervi solo attraverso altre informazioni, come le chiavi logiche di accesso, o comunque superando le misure di sicurezza.

In tale modo riguardato il perimetro spazio-temporale nel quale si colloca la condotta sanzionata dall'art. 615 –*ter* cod.pen., la determinazione del luogo in

cui si è verificato l'accesso abusivo oltre ed indipendentemente dal momento e dallo spazio fisico in cui è stata posta in essere l'azione dell'agente non risulta, all'evidenza, incoerente neppure con le ragioni di indubbio rilievo cui risponde la regola per la quale la competenza per territorio è determinata dal luogo in cui il reato è stato commesso; tra queste l'esigenza di assicurare un effettivo controllo sociale, di rendere più agevole e rapida la raccolta delle prove ed il rilievo secondo il quale il diritto e la giustizia devono riaffermarsi proprio nel luogo in cui sono stati violati (Sez. U, n. 40537 del 16/07/2009, Orlandelli, rv. 244330; Corte cost. n. 168 del 2006).

Deve essere, pertanto, dichiarata la competenza del Gup del Tribunale di Roma al quale devono essere trasmessi gli atti.

P.Q.M.

Dichiara la competenza del Gup del Tribunale di Roma, cui dispone trasmettersi gli atti.

Così deciso, il 27 maggio 2013

Il Consigliere estensore
Lucia La Posta

Il Presidente
Severo Chieffi

DEPOSITATA
IN CANCELLERIA
27 SET 2013
IL CANCELLIERE
Pietro Di Meo