SENTENZA

Penale Sent. Sez. U Num. 17325 Anno 2015

Presidente: SANTACROCE GIORGIO

Relatore: SQUASSONI CLAUDIA

Data Udienza: 26/03/2015

sul conflitto di competenza sollevato dal Giudice della udienza preliminare del Tribunale di Roma nel procedimento nei confronti di

1. R. M., nata a_____il _____

2. S. G., _____ il _____

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 R.M. e S.G., rispettivamente, avv. L. S. e avv. P. C., 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 M. R. e G. S. 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 S. (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. 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 doud 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 intemet) 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 i nterconnessi. 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 dient, 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 M. R. 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