di Elena Bassoli

L'ACCESSO ABUSIVO A SISTEMA INFORMATICO E LA VIOLAZIONE DI DOMICILIO DIGITALE

Elena BASSOLI, avvocato di diritto e nuove tecnologie, è docente di "Diritto della comunicazione elettronica" presso l'Università di Genova, nonché del Master Universitario di II Livello in Cyber Security and Data Protection, presso il DIBRIS Unige, autore di oltre 150 pubblicazioni in materia dal 1995 ad oggi, è Formatore per il Ministero di Giustizia e già per il Ministero dell'Interno. È presidente nazionale ANGIF (Associazione nazionale giuristi informatici e forensi) e CSIG-Genova (Centro studi informatica giuridica).

Corte di Cassazione, Sezione V Penale, sentenza n.2905 del 2 ottobre 2018 e depositata il 22 gennaio 2019
Corte di Cassazione, Sezione V Penale, sentenza n.2942 dell'8 novembre 2018 e depositata il 22 gennaio 2019
Le due sentenze nn. 2905 e 2942 del gennaio 2019 della Suprema Corte di Cassazione ribadiscono che il reato di accesso abusivo a sistema informatico o telematico di cui all'art. 615-ter del codice penale si configura non solo quando il colpevole violi le misure di sicurezza poste a presidio del sistema informatico o telematico altrui, ma anche quando, pur inizialmente legittimato all'accesso da colui che aveva il diritto di ammetterlo o escluderlo, vi si mantenga per finalità differenti da quelle per le quali era stato inizialmente facoltizzato all'accesso.

1. *Introduzione*

Gli ultimi mesi sono stati testimoni di una vigorosa proliferazione delle decisioni della Cassazione in materia di accesso abusivo a sistema informatico o telematico di cui all'art. 615-*ter* del codice penale. In particolare a gennaio di questo anno sono state emanate dalla sezione quinta 2 sentenze che possono essere definite "gemelle" per l'identità di questioni trattate e per l'epilogo a cui entrambe sono giunte.

2. *La sentenza n. 2942 del 2019*

Con la sentenza n. 2942 del 31 gennaio 2019 la Suprema corte di Cassazione ha affrontato il tema dell'accesso abusivo a sistema informatico o telematico di cui all'art. 615-*ter* c.p.
La vicenda prende le mosse da una sentenza del 20/12/2017, con la quale la Corte di appello di Messina confermava la sentenza del 21/12/2016 del Tribunale di Messina che aveva dichiarato un soggetto responsabile dei reati di accesso abusivo a un sistema informatico e telematico (615-*ter* c.p.) e di sostituzione di persona (cd. "furto d'identità" ex art. 494 c.p.).

L'imputato nel 2010 si era infatti abusivamente introdotto in un profilo altrui di Facebook, nonché nel sistema di posta elettronica, modificando le relative password ed impedendo alla legittima titolare di accedervi.
Egli, con la propria condotta aveva inoltre integrato gli estremi del reato di sostituzione di persona, perché, al fine di creare un danno alla vittima, induceva in errore il di lei ex fidanzato sostituendo illegittimamente la propria persona a quella della parte lesa, legittima titolare del proprio profilo Facebook. Nel fare ciò, dopo essere abusivamente entrato sul profilo altrui aveva poi lanciato frasi ed epiteti ingiuriosi all'amico della donna.

Alla luce della conseguente condanna, l'imputato ricorreva per Cassazione con quattro motivi, tutti disattesi dalla Suprema Corte.
Il primo motivo viene pertanto dichiarato inammissibile, giudicando la Cassazione che la Corte di appello abbia correttamente valorizzato tanto le dichiarazioni della persona offesa, quanto le risultanze delle indagini tecniche, le quali hanno dimostrato come gli accessi abusivi ai profili della persona offesa siano stati effettuati da cinque indirizzi IP, tutti riconducibili all'utenza telefonica intestata all'imputato: il che priva di consistenza le argomentazioni del ricorrente.
Il fatto contestato risulta infatti, ad avviso del collegio di legittimità, nitidamente delineato dal tenore testuale dell'imputazione, laddove il luogo indicato nell'imputazione fa riferimento a quello in cui si sono prodotte le conseguenze lesive per la vittima, il che priva di consistenza la deduzione del ricorrente.

Parimenti inammissibile é il secondo motivo inerente il tentativo di discarico di responsabilità dovuto al fatto che l'imputato si trovasse al lavoro durante le connessioni "incriminate". La Corte di appello ha valutato la documentazione relativa ai prospetti della giornata lavorativa dell'imputato, rilevando che solo una delle varie connessioni abusive «coinciderebbe con le ore di lavoro in cui era impiegato» l'imputato, laddove tutte le altre si collocano al di fuori di detto orario.
Sul punto, afferma la Corte, le censure dell'imputato non inficiano il rilievo della Corte distrettuale e, laddove evocano la presenza di "qualcun altro" quale autore delle interferenze abusive (peraltro, una sola di quelle accertate) e la circostanza che la persona offesa (che, dopo la fine della relazione con l'imputato, aveva lasciato la Sardegna per trasferirsi a Messina) era ancora in possesso della chiave dell'immobile, sono manifestamente inidonee a disarticolare l'intero ragionamento svolto dal giudicante, determinando al suo interno radicali incompatibilità, cosi da vanificare o da rendere manifestamente incongrua o contraddittoria la motivazione (Sez. 1, n. 41738 del 19/10/2011, Longo, Rv. 251516), tanto più che l'imputato non allega alcuna prova della effettiva di possibilità di accesso alla propria utenza telefonica da parte di "qualcun altro", diverso dalla persona offesa, limitandosi a generiche contestazioni.

Parimenti del tutto generici appaiono al giudice di legittimità i rilievi circa i sentimenti di rancore che avrebbe nutrito la persona offesa e quelli circa la possibile conoscenza da parte di terzi della domanda segreta, dedotti - gli uni e gli altri - in carenza di completa e specifica individuazione degli atti processuali che il ricorrente intendeva far valere.
Le doglianze circa la conoscenza anche da parte del fratello della domanda segreta, necessaria per accedere alla password di accesso, e il mancato specifico accertamento dell'indirizzo IP al quale ricondurre la modifica delle credenziali di accesso, non inficiano comunque la circostanza delle plurime (non limitate a quella che ha determinato l'illecita modifica delle credenziali) connessioni remote tutte riconducibili alla linea telefonica dell'imputato.

3. La sentenza n. 2905 del 2019

Degli stessi giorni è la sentenza 2905/2019 del 22.1.2019 della Cassazione che ha ribadito che i reati descritti vigano anche tra coniugi, semmai ve ne fosse stato bisogno.
In tale pronuncia, come già affermato dalla stessa sezione in un caso analogo (Sez. 5, n. 52572 del 06/06/2017), la circostanza che il ricorrente sia a conoscenza delle chiavi di accesso della moglie al sistema informatico quand'anche fosse stata quest'ultima a renderle note e a fornire, così, in passato, un'implicita autorizzazione all'accesso - non escluderebbe comunque il carattere abusivo degli accessi *sub iudice*.

Mediante questi ultimi, infatti, si è ottenuto un risultato certamente in contrasto con la volontà della persona offesa ed esorbitante rispetto a qualsiasi possibile ambito autorizzatorio del titolare dello *ius excludendi alios*, vale a dire la conoscenza di conversazioni riservate e finanche l'estromissione dall'account Facebook della titolare del profilo e l'impossibilità di accedervi.

Tale interpretazione è confortata dalla recente Sez. U, n. 41210 del 18/05/2017, Savarese, Rv. 271061, che sia pure rispetto ad una situazione diversa – ha valorizzato i limiti dell'autorizzazione concessa

dal titolare del domicilio informatico da parte di soggetto autorizzato ad accedervi. Anche in questo caso il ricorso è stato dichiarato inammissibile con conseguente condanna del ricorrente.

4. *L'art. 615-ter e l'inviolabilità del domicilio*

Il reato su cui entrambe le pronunce si esprimono è forse il più rilevante tra quelli introdotti dalla, ormai non più giovane, Legge 547 del 1993 sui crimini informatici nel codice penale Rocco del 1930.
Il titolo XII del libro II del codice penale è dedicato ai delitti contro la persona. In particolare, la sezione IV del capo III è dedicata ai delitti contro l'inviolabilità del domicilio. È in questo contesto che è stato inserito l'art. 615-ter introdotto dalla legge 547 del 1993.

Questo reato punisce l'accesso all'interno di un sistema informatico, qualora questo accesso non si svolga secondo quanto legittimamente prescritto. Il concetto di domicilio è stato così esteso al perimetro dei sistemi informatici, superando in tal modo tutte le difficoltà incontrate in precedenza nei casi di accesso abusivo[1].
E proprio tale norma è stata elevata a modello[2] nel delineare il reato *de quo*, che - almeno nelle intenzioni del legislatore- protegge il "domicilio informatico" quale "espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost. e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli art. 614 e 615 c.p."[3], con una equiparazione suggestiva, che rivela la crescente importanza degli strumenti digitali nella vita quotidiana di ciascuno, ma che può risultare fuorviante per l'interprete.[4]

La Suprema Corte di Cassazione ancora recentemente si è espressa sulla disposizione rimarcando come la condotta punibile possa essere da una parte quella di colui che si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza e dall'altra, di colui che vi si mantiene 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[5].

La legge considera reato anche il solo accedere a un sistema informatico senza danneggiarlo, concetto in seguito rafforzato dalla legge sulla tutela dei dati personali che difende tali dati da un uso non legittimo. L'articolo prevede che il sistema sia protetto da misure di sicurezza ma non richiede che tali misure siano necessarie, potendosi qualificare l'accesso comunque abusivo se effettuato contro la volontà di chi ha il potere di escludere l'intruso.
Per misure di sicurezza si intendono tutti i mezzi di protezione logici e fisici (codici di accesso, *password*, chiavi elettroniche)[6], che dimostrino la volontà del soggetto che gestisce il sistema informatico di volere espressamente autorizzare l'accesso e la permanenza nel sistema solo a persone ben determinate[7].

Secondo la dottrina e la giurisprudenza di legittimità, infatti, le misure di sicurezza (logiche o fisiche) rilevano come indici della volontà del titolare di impedire l'accesso ad estranei, e non è quindi richiesta la loro idoneità a prevenire intrusioni[8].
Il ruolo di tale elemento costitutivo è ulteriormente ridimensionato dalla previsione dell'alternativa condotta di "mantenimento", realizzata da chi, avendo acceduto legittimamente, si trattenga (continui l'utilizzo) anche dopo che sia venuto meno tale diritto o persegua una finalità diversa da quella consentita[9].

5. *Il bene giuridico tutelato*

La questione più dibattuta sull'argomento riguarda il bene giuridico oggetto di tutela.

Una prima tesi, fondata sulla collocazione topografica dell'art.615-*ter* e sui lavori preparatori[10], vede la norma come protezione del c.d. "domicilio informatico": l'evoluzione tecnologica e sociale avrebbe fatto assurgere l'elaboratore a luogo virtuale ove

1 Cfr. G. Pica, Diritto penale delle tecnologie informatiche, Torino, 1997, 38.

2 Sui problemi inerenti alla sanzionabilità di tale condotta prima dell'introduzione dell'art. 615-ter cfr. sul tema. G. Corrias Lucente, Informatica e diritto penale: elementi per una comparazione con il diritto statunitense, in "Dir. Inf.", 1987, I parte, 195; P. Galdieri, Teoria e pratica nell'interpretazione del reato informatico, Milano, 1997, 135; E. Giannantonio, L'oggetto giuridico dei reati informatici, in CP, 2001, 2244; F. Sarzana, Note sul diritto penale dell'informatica, in "Giur. Pen.", 1984, I, 28.

3 Camera dei Deputati, XI Legislatura, Disegno di legge n. 2773, Presentazione del Ministro di Grazia e Giustizia (G. Conso), 9.

4 Nella pedissequa riproduzione dell'art. 614 c. il legislatore ha addirittura trasposto nella nuova versione l'aggravante per l'ipotesi in cui il colpevole fosse "palesemente armato".

5 Corte di Cassazione, Sez. Penale, Sezioni Unite, n. 17325 del 2015.

6 C. Parodi, La tutela penale dei sistemi informatici e telematici: le fattispecie penali, Relazione presentata al Convegno Nazionale su "Informatica e riservatezza" del CNUCE - Pisa 26/27 settembre 1998.

7 G. Trapani, Accesso abusivo ad un sistema telematico, in "Studium Iuris", 2001, fasc.6, 724, nota a Cass. pen. Sez V, 6 dicembre 2000, n. 1675.

8 Si è menzionato l'esempio di password di default non sostituite dall'utente inesperto.

9 G. Trapani, cit.

10 Così Camera dei Deputati, XI Legislatura, Disegno di legge N. 2773. presentazione del Ministro di Grazia e Giustizia (G. Conso), 9. In dottrina, nel senso che l'art. 615-ter c. tuteli il domicilio informatico, R. Borruso, La tutela del documento e dei dati, in R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti (a cura di), "Profili penali dell'informatica", Milano, 1994, passim. 28; G. Faggioli, cit., 105; P. Galdieri, La tutela penale del domicilio informatico, in P. Galdieri (a cura di), "Problemi giuridici dell'informatica nel Mec", Milano, 1996, 189 ss.

si svolgono le più intime attività realizzatrici della personalità umana. La dottrina prevalente respinge tale tesi, sottolineando i confini evanescenti di questa nuova dimensione della riservatezza individuale, ed evidenziando la sua incompatibilità con la stessa lettera della norma, che prevede tra le circostanze aggravanti l'eventualità che i fatti "riguardino sistemi informatici o telematici di interesse militare o relativo all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico", estendendo la tutela ben al di là della "area di rispetto pertinente al soggetto interessato"[11].

Altri segnalano il parallelismo con l'art. 637 c.p. che, nell'ambito di una società prevalentemente rurale, proteggeva da ogni possibile turbativa la proprietà fondiaria, come nell'attuale società viene protetto il "bene informatico" dalle intrusioni che ne impediscano l'esclusiva indisturbata fruizione[12].
Ma anche tale posizione non è immune da critiche: nuovamente per l'assimilazione dei sistemi informatici e telematici ad ambiti spaziali reali, incompatibili con la dimensione meramente immateriale, ed anche per la scarsa ragionevolezza di una così grande disparità di trattamento sanzionatorio (una scarsa pena pecuniaria per l'art. 637, la pena detentiva per l'art. 615-*ter* c.p.) per due fattispecie che si assumono così simili, limitate entrambe alla violazione della sfera di signoria dell'interessato, rispettivamente sul proprio fondo o sul proprio elaboratore[13].

6. *Reato di pericolo o reato di danno*

Secondo alcuni si tratterebbe di un reato di pericolo astratto, in quanto incrimina una condotta di per sé innocua per il bene giuridico protetto, a cui secondo l'*id quod plerumque accidit* consegue la lesione. La validità di tale massima di esperienza escluderebbe problemi di legittimità costituzionale rispetto al principio di offensività[14].

Questa interpretazione tuttavia farebbe sorgere notevoli dubbi di costituzionalità in merito al reato-ostacolo di "detenzione e diffusione di codici di accesso" (615-*quater*), che diventerebbe un illecito di "pericolo di pericolo", sanzionando un comportamento troppo distante dall'effettiva lesione del bene giuridico[15].

La soluzione più corretta, che porta ai risultati più coerenti anche sul piano sistematico, è allora quella che vede nell'accesso abusivo un reato di danno, in quanto l'introduzione è essa stessa accesso alla conoscenza di dati e informazioni, lesione effettiva della riservatezza e non un momento distinto, ancorché generalmente prodromico[16].

7. *L'illiceità del mantenimento nel sistema*

Occorre poi ricordare che tale reato viene integrato anche dalla condotta di chi, entrato legittimamente, si mantenga all'interno del sistema per un tempo superiore a quello voluto da colui che ha diritto di escluderlo, o per finalità diverse da quelle per cui il reo era stato inizialmente autorizzato a entrare, come nelle due recenti sentenze sopra analizzate[17].
Una delle prime pronunce in tal senso è la sentenza Cass. SS.UU. 27.10.2011, n. 4694, che si è espressa sulla configurabilità del reato nel caso in cui un soggetto, legittimamente ammesso ad un sistema informatico o telematico, vi operi per conseguire finalità illecite.

Su tale aspetto, che ad oggi appare pacifico, si era in passato registrato un contrasto interpretativo all'interno della giurisprudenza delle sezioni semplici, così motivato dalla Suprema Corte: "Rilevante deve ritenersi, perciò, il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che sostanzialmente non può ritenersi autorizzato ad accedervi ed a permanervi, sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (nozione specificata, da parte della dottrina, con riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro) sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito.

In questi casi, come in quelli sopra visti, è proprio il titolo legittimante l'accesso e la permanenza nel sistema che risulta violato: il soggetto agente opera illegittimamente, in quanto il titolare del sistema medesimo lo ha ammesso solo a ben determinate condizioni, in assenza o attraverso la violazione delle quali le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta". ©

11 C. Pecorella, op.cit., 314.

12 F. Berghella-R. Blaiotta, Diritto penale dell'informatica e beni giuridici, in "Cass. pen.", 1995, fasc. 9, 2333.

13 C. Pecorella *op. cit.*, 316.

14 F.C. Palazzo, Introduzione ai principi del diritto penale, Giappichelli, Torino, 1999, 150.

15 F. Berghella - R. Blaiotta, Diritto penale dell'informatica e beni giuridici, Cass. pen., 1995, fasc. 9, 2333.

16 S. Aterno, Sull'accesso abusivo ad un sistema informatico o telematico, in "Cass. Pen.", 2000, fasc. 11 (nov), 2995, nota a Cass. Pen. Sez. VI 4/11/99 n. 3067.

17 Sia consentito sul punto il rinvio a E. Bassoli, Fondamenti di diritto della comunicazione elettronica, II Ed. Amon, 2018, passim.