ACCESSO ABUSIVO A UN SISTEMA INFORMATICO O TELEMATICO ART. 615 TER C.P.

Dr. Francesco Zaccaria

Sommario: 1) Introduzione; 2) Bene - interesse giuridicamente tutelato; 3) La condotta penalmente rilevante e la struttura del reato; 4) Le condotte tipiche; 5) Le misure di sicurezza del sistema informatico; 6) Compatibilità con il tentativo; 7) Luogo di consumazione del reato.

1) INTRODUZIONE

Come si evince dalla Relazione al disegno di legge n. 2773 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" (11ª legislatura, divenuto legge il 23 dicembre 1993 n. 547) lo sviluppo delle nuove tecnologie informatiche e telematiche ed il loro impatto con la società moderna resero indispensabile una specifica regolazione del fenomeno, affinché fossero introdotte più chiare regole alle quali informare i comportamenti.

Tale esigenza già all'epoca molto sentita è oggi sempre di maggiore attualità soprattutto in considerazione del fatto che taluni settori di rilevante interesse nell'economia nazionale appaiono fortemente dipendenti dalle tecnologie informatiche. Di qui, quindi, nasce e sempre maggiormente si accresce, l'esigenza di positivizzare tutti quei comportamenti, per esempio di intrusione o sabotaggio, che possono provocare danni notevoli, sotto molteplici aspetti, alla vita del Paese.

Si legge nella Relazione sopraindicata che: "È quindi necessario, in relazione a tale stadio di evoluzione tecnologica, individuare adeguate norme che consentano allo Stato e alla società civile di difendersi da comportamenti che, in quanto incidenti su sistemi di vitale rilevanza, rappresentano un gravissimo pericolo per la collettività intera".

Pertanto, proprio al fine di rispondere ad esigenze di tal fatta, viene introdotto nel nostro ordinamento l'articolo 615 ter c.p.. La norma è stata aggiunta all'interno del codice penale italiano dalla legge 23.12.1993, n. 547 anche sulla base delle raccomandazioni provenienti dal Consiglio d'Europa che da tempo sottolineava la necessità di tutelare i consociati da tale nuova forma di aggressione della propria sfera personale oltre ad evidenziare la gravità ed i costi degli abusi informatici.

Prima dell'introduzione nel nostro ordinamento di detta norma, dottrina e giurisprudenza non hanno mancato di proteggere le esigenze di tutela dei sistemi informatici attraverso il ricorso a fattispecie già esistenti nel nostro codice penale. In quest'ottica si sono succedute interpretazioni, per certi aspetti un po' forzate, ad esempio dell'articolo 614 c.p. "Violazione di domicilio", del reato di "Sostituzione di persona" ex articolo 494 c.p.

nonché di quello di intercettazione abusiva di comunicazioni telefoniche e telegrafiche ex articolo 617 c.p.[1].

Ad ogni modo tali interpretazioni sono state dai più abbandonate poiché finiscono per compromettere irreparabilmente principi cardine del nostro ordinamento quali quello di legalità e quello di tassatività[2].

Come detto, il reato di accesso abusivo ad un sistema informatico o telematico è previsto e punito dall'articolo 615 ter del c.p. e si inserisce all'interno del titolo XII del codice, dedicato ai delitti contro la persona, capo III, sezione IV, preposta a sanzionare i delitti contro l'inviolabilità del domicilio.

Con la legge n. 547 del 1993 sono stati introdotti nel corpo del codice penale, fra gli altri, anche gli articoli 615 quater c.p. "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici" e 615 quinquies c.p. "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico".

La introduzione di fattispecie incriminatrici di tal fatta all'interno del nostro sistema giuridico si è resa irrinunciabile soprattutto in considerazione dell'evoluzione e dell'espansione delle reti informatiche che ha, tra l'altro, posto nuovi problemi in materia di riservatezza[3].

In particolare, accanto a nuove forme di aggressione della privacy tradizionale, si pone un interesse di nuova emersione, la cosiddetta privacy informatica. Con tale espressione si sintetizza l'esigenza che l'uso di un sistema informatico avvenga in condizioni di libertà e autonomia tali da lasciare impregiudicate l'integrità e la riservatezza del sistema e dei dati raccolti[4].

2) BENE – INTERESSE GIURIDICAMENTE TUTELATO

Non c'è dubbio che la collocazione sistematica di tale fattispecie si giustifichi in relazione alla specifica oggettività di tutela. Nella relazione al disegno di legge si afferma che i sistemi informatici e telematici rappresentano ormai "una espansione ideale dell'area di rispetto pertinente al soggetto interessato garantita dall'articolo 14 della Costituzione" che, come è noto, assicura la inviolabilità del domicilio. Pertanto il bene-interesse giuridicamente tutelato dall'articolo 615 ter c.p. è simmetricamente costituito dalla pace del cosiddetto domicilio informatico e, cioè, del domicilio elettronico quale estensione virtuale del soggetto titolare di un sistema informatico[5]. Questa conclusione appare perfettamente in linea con la *ratio* di tutela della medesima riservatezza informatica, che non risiede nella esigenza di salvaguardare i dati personali contenuti nel sistema

1 Per un'elencazione completa della casistica Cfr. PICA.
2 Cfr. Wolters Kluwer, *Leggi d'Italia Legale*, Codice penale commentato.
3 SIEBER, *Computerkriminalitat und Informationsstrafrecht*, in Computer und Recht, 1995; SARZANA, *Informatica e diritto penale*, Milano, 1994; PICOTTI, Studi di diritto penale dell'informatica, Verona, 1992.
4 FIANDACA - MUSCO, *Diritto penale*, Parte speciale Volume II, tomo primo, 2007.
5 PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999.

informatico, bensì nella necessità di proteggere lo *ius excludendi* di ciascun soggetto dalla propria sfera privata racchiusa nel domicilio informatico[6].

A ben considerare, infatti, il titolo XII del codice penale, dedicato ai delitti contro la persona, capo III, sezione IV, apre proprio con l'articolo 614 codice penale che sanziona la violazione di domicilio "classica".

Ciò che deve essere preso in considerazione per valutare la condotta prevista e punita ex articolo 615 ter c.p. è la violazione da parte del soggetto agente del diritto di esclusione dalla propria sfera personale che il legislatore riconosce in capo al titolare del sistema informatico o telematico.

In buona sostanza il legislatore ha assicurato la protezione del bene domicilio informatico, inteso sia quale spazio fisico in cui sono contenuti i dati informatici personali, sia quale spazio ideale di pertinenza della sfera individuale e privata[7].

Dibattito dottrinale[8]

Il bene-interesse giuridico individuato nella riservatezza dei dati personalissimi. Alcuni autori riguardo alla collocazione sistematica della norma ritengono che la ratio sottesa all'intervento del legislatore consiste nella esigenza di tutelare i soli dati personalissimi dei sistemi informatici, ovvero quelli attinenti alla vita privata del soggetto. Ciò posto, il bene giuridico protetto dalla norma si specificherebbe nella riservatezza dei dati e dei programmi contenuti in un sistema informatico[9].

L'indisturbata fruizione del sistema da parte del gestore quale oggetto giuridico tutelato. Su un altro fronte, invece, si colloca quella parte della dottrina che ritiene impossibile circoscrivere l'oggettività giuridica del reato sanzionato dall'articolo 615 ter c.p. alla mera tutela del domicilio informatico, inteso quale sfera privata afferente alle private esplicazioni della persona umana, posto che tale profilo personalistico non si configura quale elemento indefettibile della realtà informatica. Sicché la ratio della norma si specificherebbe nell'interesse alla indisturbata fruizione del sistema da parte del gestore[10]. Tale assunto sarebbe confortato dalla circostanza che il legislatore ha configurato lo *jus excludendi alios* dai sistemi informatici indipendentemente dal fatto che il contenuto del sistema abbia o meno carattere personale.

La semplice tutela di un interesse patrimoniale. Secondo altra prospettazione, la norma presiede esclusivamente alla tutela di un interesse patrimoniale, leso dall'eventuale danneggiamento della struttura informatica[11].

[6] FIANDACA - MUSCO, *Diritto penale*, cit..
[7] GAROFOLI, *Compendio di Diritto penale* – Parte speciale.
[8] GAROFOLI, *Compendio di Diritto penale*, cit..
[9] POMANTE – PECORELLA.
[10] SPAGNOLETTI.
[11] MARINI.

3) LA CONDOTTA PENALMENTE RILEVANTE E LA STRUTTURA DEL REATO

Sempre più spesso, nel corso degli ultimi anni, si è verificata l'ipotesi delittuosa sanzionata dall'articolo 615 ter c.p., atteso che sempre maggiori sono i domicili virtuali di una persona. In quest'ottica, infatti, è sufficiente fare riferimento alle caselle di posta elettronica o, ancora, ai profili sui social network.

E' bene, dunque, a questo punto della trattazione, cercare di identificare quali sono in concreto le condotte che integrano il reato di cui all'art. 615 ter c.p..

Al primo comma dell'articolo 615 ter c.p. il legislatore prevede un reato di tipo comune, considerato che sanziona la condotta di chiunque si introduca in maniera abusiva all'interno di un sistema informatico o telematico protetto, sprovvisto della necessaria autorizzazione di chi ha il diritto di escluderlo. Il reato è punito con la reclusione fino a tre anni ed è prevista la procedibilità a querela di parte. Deve, altresì, precisarsi che viene sanzionata una duplice condotta, ovvero sia quella di introduzione abusiva all'interno del sistema informatico o telematico sia quella di mantenimento contro la volontà, espressa o tacita, del titolare all'interno del sistema.

Questa differente modalità di esecuzione della fattispecie rileva anche ai fini della valutazione del *tempus commissi delicti*. Per l'opinione maggiormente diffusa, infatti, il reato di accesso abusivo ex articolo 615 ter c.p. è un reato istantaneo, considerato che si consuma nel momento stesso in cui l'agente non autorizzato si inserisce nello spazio, nel domicilio virtuale, del soggetto titolare del diritto di esclusione. La condotta di mantenimento non autorizzato, invece, costituirebbe un'ipotesi di reato istantaneo ad effetto permanente, atteso che lo stesso perdura per tutto il tempo in cui permane l'accesso non autorizzato.

I commi secondo e terzo dell'articolo 615 ter c.p. si connotano per un maggiore disvalore giuridico-penale e dispongono sanzioni più gravi rispetto a quelle previste dal primo comma del suindicato articolo. In quest'ottica, si giustifica anche la previsione della procedibilità d'ufficio.

In particolare è necessario interrogarsi sul se queste ipotesi siano fattispecie aggravate, opinione minoritaria, oppure se costituiscano autonome fattispecie delittuose[12].

Questa seconda opinione è seguita da parte della dottrina e della giurisprudenza in virtù di molteplici considerazioni.

In primo luogo la circostanza che, per esempio, nel comma secondo n. 1) dell'articolo 615 ter c.p., viene inciso un bene-interesse ulteriore rispetto al domicilio, quale il buon andamento e l'imparzialità della Pubblica amministrazione tutelato dall'articolo 97 della Costituzione.

In secondo luogo, deve considerarsi che l'ipotesi di cui al comma secondo n. 3) del suindicato articolo, prevede anche il verificarsi di un evento quale la distruzione o il danneggiamento del sistema informatico o telematico.

[12] Contra fra gli altri Cfr. FIANDACA - MUSCO, *Diritto penale*, cit..

Infine, in questo senso, depone anche la previsione di un differente sistema di condizioni di procedibilità: a querela per il primo comma dell'articolo 615 ter c.p. e d'ufficio negli altri casi.

Per altri autori, invece, i commi secondo e terzo dell'art. 615 ter c.p. costituirebbero ipotesi aggravate. Più in particolare, detti commi prevedrebbero quattro circostanze aggravanti, alla cui presenza corrisponde, come sottolineato, un notevole inasprimento della pena edittale (alla pena base della reclusione sino a 3 anni si sostituisce la reclusione da 1 a 5 anni)[13].

4) LE CONDOTTE TIPICHE

A lungo si è discusso sulla configurabilità del reato *de quo* nell'ipotesi in cui un soggetto, legittimamente ammesso ad utilizzare ed operare su un dato sistema informatico o telematico, lo utilizzi per finalità illecite o comunque diverse da quelle per le quali è autorizzato.

Il contrasto fra coloro che sostenevano che il reato ex art. 615 ter c.p. si consumasse ogniqualvolta un certo soggetto provvisto di autorizzazione utilizzasse il sistema per finalità diverse da quelle consentite e coloro che ritenevano che, invece, in ipotesi di tal fatta non potesse ravvisarsi alcuna condotta violativa del dettato di cui all'art. 615 ter c.p. è stato risolto in senso favorevole al primo orientamento dalla sentenza Cass. Pen. S.U. 27.10.2011, n. 4694 secondo la quale: "Sussiste il reato di accesso abusivo ad un sistema informatico o telematico protetto di cui all'art. 615 ter c.p. allorché la condotta di accesso o di mantenimento nel sistema posta in essere dal soggetto agente, nonostante a ciò abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema in parola onde delimitarne oggettivamente l'accesso. Ne deriva che, ai fini della configurabilità della citata fattispecie delittuosa, risultano irrilevanti gli scopi e le finalità che soggettivamente hanno indotto e motivato l'ingresso al sistema[14]".

Tale orientamento è stato più di recente confermato dalla Suprema Corte a sezioni semplici, in questi termini, infatti, cfr. Cass. Pen. Sez. V, 05.12.2016, n. 11994 per la quale "In tema di delitti contro la inviolabilità del domicilio, integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter c.p., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, ovvero ponga in essere operazioni di natura ontologicamente diversa da quelle per le quali l'accesso è consentito. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema[15]" e, ancora cfr. anche Cass. Pen. Sez. V, 29.11.2017, n. 1021 secondo la quale "Integra il delitto previsto dall'art. 615-ter, comma 2, n. 1, c.p. la condotta del pubblico ufficiale che, pur non violando

[13] Cfr. Wolters Kluwer, *Leggi d'Italia Legale*, Codice penale commentato.
[14] Cass. Pen. S.U., 27.10.2011, n. 4694.
[15] Cass. Pen. Sez. V, 5.12.2016, n. 11994.

un sistema informatico o telematico protetto, acceda o si mantenga nel sistema per scopi diversi rispetto a quelli per i quali gli è attribuita la facoltà di accesso[16]".

5) LE MISURE DI SICUREZZA DEL SISTEMA INFORMATICO

Come è noto, la norma oggetto di analisi circoscrive la tutela ai soli sistemi protetti da misure di sicurezza. Per la dottrina maggioritaria le misure di sicurezza consistono in dispositivi idonei ad impedire l'accesso al sistema a chi non sia autorizzato. In particolare, secondo i più, è sufficiente qualsiasi misura di protezione, anche banale e facilmente aggirabile, in quanto la pretesa esistenza della misura di sicurezza, **è esclusivamente preordinata a rendere esplicita e non equivoca la volontà di riservare l'accesso solo a determinate persone, ovvero di porre un generale divieto di accesso[17]**. Ne consegue che anche l'adozione di una protezione costituita da una semplice parola-chiave (password), facilmente accessibile o ricostruibile, rappresenta una esplicitazione del divieto di accesso al sistema e legittima la tutela in sede penale[18].

Per altra dottrina che rappresenta, però, una opinione minoritaria, l'utilizzo di una semplice parola chiave o codice d'accesso non sarebbe in grado di integrare il requisito richiesto dalla norma delle "misure di sicurezza"[19].

La giurisprudenza della Suprema Corte aderisce ormai da tempo al primo degli orientamenti riportati. In proposito è sufficiente considerare quanto statuito nella sentenza Cass. Pen., Sez. II, 21.02.2008, n. 36721 (rv. 242084) "Integra il delitto di introduzione abusiva in un sistema informatico o telematico l'accesso ad un sistema che sia protetto da un dispositivo costituito anche soltanto da una parola chiave (cosiddetta "password")"[20].

In buona sostanza, l'opinione predominante, costantemente espressa nel corso degli ultimi anni da parte degli Ermellini, è quella di punire qualsiasi introduzione in un sistema informatico telematico che avvenga contro la volontà dell'avente diritto. In questo senso giova precisare, ancora una volta, che il reato previsto e punito dall'articolo 615 ter c.p. si caratterizza non per la violazione di sistemi protettivi ma per la violazione del delle disposizioni del titolare del diritto di esclusione, così come avviene nell'ipotesi delittuosa di violazione di domicilio ex articolo 614 c.p.. Pertanto, non è necessaria ai fini dell'integrazione del reato *de quo* la violazione delle misure di sicurezza ma è sufficiente che queste ultime siano state predisposte dal titolare del diritto[21].

6) COMPATIBILITÀ CON IL TENTATIVO

Con riferimento alla compatibilità dell'articolo 615 ter c.p. con l'istituto del tentativo non sembrano esserci dubbi di sorta. Infatti, una volta ravvisati gli elementi degli atti idonei,

[16] Cass. Pen. Sez. V, 29.11.2017, n. 1021.
[17] D'AIETTI.
[18] Cfr. Wolters Kluwer, *Leggi d'Italia Legale*, Codice penale commentato; D'AIETTI; PAZIENZA.
[19] Cfr. CECCACCI, *Computer Crimes. La nuova disciplina dei reati informatici*, Milano, 1994, 70.
[20] Cass. Pen., Sez. II, 21.02.2008, n. 36721 (rv. 242084).
[21] Cfr. Cass. Pen., Sez. V, 7.11.2000, n. 12732.

diretti in modo non equivoco, sembra ben possibile configurare e, conseguentemente, punire un tentativo di accesso abusivo ad un sistema informatico o telematico. Il tentativo, quindi, sarà configurabile in tutti i casi in cui l'agente, in presenza di una volontà contraria dell'avente diritto, cerchi di aggirare le protezioni, per esempio digitando più password, e non vi riesca[22].

Per una recente opzione dottrinaria nel reato di accesso abusivo ad un sistema informatico o telematico non sarebbe ammissibile il tentativo. Infatti, considerando quest'ultimo come un'ipotesi di reato di pericolo astratto, non potrebbe a rigore ravvisarsi la configurabilità del tentativo ex art. 56 c.p. perché, altrimenti, vi sarebbe un'eccessiva anticipazione della soglia di punibilità in violazione del principio di offensività[23].

7) LUOGO DI CONSUMAZIONE DEL REATO

Molto problematica si presenta la questione relativa al luogo della consumazione del reato ex articolo 615 ter c.p.. In dottrina e giurisprudenza si contendono il campo più opinioni.

Per un primo orientamento, per vero risalente nel tempo, si dovrebbe fare riferimento al fine di stabilire il luogo della consumazione al server che elabora e controlla le credenziali di autenticazione del cliente. In questi termini cfr. Cass. Pen., Sez. I, 27.5.2013, n. 40303 per la quale: "Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico non è quello in cui vengono inseriti i dati idonei ad entrare nel sistema bensì quello dove materialmente è collocato il server che elabora e controlla le credenziali di autenticazione del cliente[24]".

Per altra opinione, sostenuta da autorevole dottrina, dovrebbe, invece, guardarsi al luogo in cui ha fisicamente sede il sistema oggetto di intrusione e non al luogo in cui si trovi fisicamente l'agente nel momento in cui vengono poste in essere le attività intrusive[25].

Da ultimo si segnala un orientamento, sempre più seguito all'interno della giurisprudenza di legittimità, secondo cui il luogo della consumazione sarebbe quello in cui l'agente materialmente pone in essere la condotta delittuosa di introduzione abusiva o mantenimento illecito. A parere della Suprema Corte, infatti, è proprio quello il luogo in cui il bene interesse protetto dal legislatore finisce per essere compromesso, violato dal soggetto agente. In questi termini cfr. Cass. Pen., S.U., 26.3.2015, n. 17325 secondo la quale : "Il delitto di accesso abusivo ad un sistema informatico o telematico, previsto e punito dall'art. 615-ter c.p., si consuma nel luogo in cui si trova il soggetto che effettua l'introduzione abusiva, ovvero vi si mantiene abusivamente. L'ingresso o l'introduzione abusiva, invero, 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

22 Cfr. Pica, Monaco, Marini.
23 Cfr. Pecorella, Antolisei, Mucciarelli.
24 Cass. Pen. Sez. I, 27.5.2013, n. 40303.
25 Cfr. Parodi, Calice

superamento delle misure di sicurezza apposte dal titolare del sistema, in tal modo realizzando l'accesso alla banca-dati[26]".

[26] Cass. Pen. S.U., 26.03.2015, n. 17325.