Pubblicato in «Telediritto.it: Portale giuridico umbro», Informatica giuridica, dottrina, 2009.

Il reato di accesso abusivo*

SOMMARIO: *1. Premessa —2. L'accesso abusivo – 3. ...segue: le misure di sicurezza – 4. ...segue: il "trattenimento" abusivo nel sistema – 5. ...segue: l'accesso tramite software di controllo remoto – 6. Il portscanning -*

1. La fattispecie prevista e punita dall'articolo 615-ter del codice penale rappresenta probabilmente uno dei reati informatici maggiormente diffusi: l'accesso abusivo ad un sistema informatico rappresenta, infatti, una delle sfide più avvincenti e stimolanti per qualsiasi esperto di sicurezza e spesso l'autore del fatto non avverte in pieno la portata antigiuridica dell'azione commessa, che viene piuttosto vissuta come un gioco od un test delle proprie capacità[1].

Il legislatore, riconosciuto che il domicilio informatico rappresenta uno spazio in cui l'individuo trasferisce ed esercita alcune delle sue facoltà intellettuali, ha ritenuto che lo stesso fosse, come tale, meritevole di una tutela, quantomeno, pari a quella attribuita al domicilio fisico; tale decisione lo ha "praticamente costretto"[2] a garantire al domicilio informatico una tutela piena ed esclusiva espandendo l'area di rispetto garantita all'individuo dall'articolo 14 della Costituzione e dagli articoli 614 e 615 del codice penale[3].

La giurisprudenza e buona parte della dottrina hanno commentato in maniera particolarmente favorevole la norma in esame, spesso plaudendo alla scelta del legislatore[4], ma

* **Emanuele Florindi** avvocato, membro del direttivo AISF (Accademia Internazionale di Scienze Forensi). Professore a contratto del corso di "Bioetica e Diritto" presso la facoltà di Scienze MM.FF.NN., del corso di "Diritto dell'informatica" presso il corso di laurea specialistica in informatica, e di "Informatica giuridica" presso la facoltà di Giurisprudenza dell'Università degli Studi di Perugia.

1 A tal proposito si veda la decisione del Tribunale dei minorenni di Bologna, 07 maggio 2008, n.659: *è noto come l'imputabilità del minore presupponga l'accertamento della capacità di intendere e di volere di costui, la quale si sostanzia nella c.d. "maturità mentale", concetto, questo, a carattere relativo, poiché correlato alle caratteristiche del reato commesso, ed implicante in special modo la capacità del soggetto di percepire il disvalore etico-sociale delle proprie azioni. Tale essendo la premessa è gioco forza concludere che l'indagine sull'imputabilità del minore debba essere condotta con particolare cautela rispetto a reati, come quelli informatici, in cui il comportamento incriminato può essere interpretato più come il sintomo di spiccate e non comuni capacità intellettive dell'agente piuttosto che quale manifestazione di un atteggiamento deviante di costui*.

2 Cass. pen. Sez. 6, sent. 3067 del 14/12/1999.

3 Cfr. Ministero di Grazia e Giustizia, Schema di disegno di legge contenente modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale, in tema di criminalità informatica.

4 R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti, *Profili penali dell'informazione*, Milano, 1994;

Via XX Settembre 131/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

non sono mancate le critiche, anche dure. In particolare si è criticata non soltanto la scelta del legislatore di collocare la norma tra i delitti contro l'inviolabilità del domicilio, ma anche la decisione di punire il semplice accesso.

2. La scelta del legislatore è, ad avviso di chi scrive, pienamente condivisibile in quanto deputata a difendere lo *ius excludendi alios*, elemento essenziale e vera *conditio sine qua non* del principio, costituzionalmente garantito, dell'inviolabilità del domicilio. Il legislatore ha, infatti, positivamente valutato come, nella società moderna, informatizzazione e telematica, abbiano assunto un'importanza ed una diffusione sempre maggiore e come, stante l'intrinseca insicurezza dei sistemi e la sempre più diffusa informatizzazione ed utilizzazione di Internet, sia cresciuta nella società l'esigenza di tutelare la riserva-

M. Mantovani, "I reati informatici in Francia", in *Rivista del diritto dell'informazione e dell'informatica*, Milano, 1990. Si veda poi Cass. pen., Sez. 6, sent. 3067 del 14/12/1999 in cui la Corte ha fornito una precisa e lucida definizione di domicilio informatico osservando:
non risulta che questa Corte abbia avuto occasione di esprimersi in ordine all'oggetto giuridico della tutela approntata dall'art. 615 ter c.p. / Indubbiamente la collocazione sistematica della norma nella sezione IV (concernente i delitti contro l'inviolabilità del domicilio) del capo III del titolo XIII del libro II, riguardante i delitti in particolare, dà ragione dell'intenzione del legislatore - il quale ha preso a parametro il "domicilio fisico" dell'individuo - di assicurare la protezione del "domicilio informatico", quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici), di pertinenza della persona, al quale estendere la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto (art. 14 Cost.), come non manca di notare, del resto, la Relazione al disegno di legge 23 dicembre 1993, n. 547.
La dottrina che si è occupata del problema è, però, divisa sull'estensione da attribuire alla garanzia offerta dal legislatore del 1993 con la norma in argomento, sostenendosi da parte di alcuni (proprio per la collocazione sistematica della norma) che lo scopo avuto di mira dal legislatore sia stato quello di tutelare soltanto i contenuti personalissimi (cioè attinenti al diritto alla riservatezza della vita privata) dei sistemi informatici (teoria alla quale ha evidentemente ritenuto di aderire il tribunale di Lecce, il quale ha ritenuto che, pur essendosi il D. L. introdotto nel sistema informatico "X", non sia stato violato l'ambito di riservatezza individuale di alcuno), mentre v'è chi riconosce che la norma in parola debba estendersi nel senso che essa abbia ad oggetto lo ius excludendi del titolare del sistema informatico, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla propria sfera di pensiero o alla propria attività (lavorativa e non). / Ora, sembra alla Corte che debba preferirsi quest'ultimo indirizzo, per la ragione che esso meglio si attaglia alla lettera e allo scopo della legge: alla lettera, perché la norma non opera distinzioni tra sistemi a seconda dei contenuti (esclusivamente limitandosi ad accordare tutela ai sistemi protetti da misure di sicurezza); alla ratio legis soprattutto, perché la prima interpretazione implicherebbe l'esclusione dalla tutela - irragionevolmente e verosimilmente in senso contrario all'intenzione del legislatore - di aspetti non secondari, quali per esempio, quelli connessi ai profili economico - patrimoniali dei dati (si pensi al diritto dei titolari di banche dati protette da misure di sicurezza di permettere l'eccesso alle informazioni dietro pagamento di un canone), lasciando quindi sforniti di protezione i diritti di enti e persone giuridiche, non tanto per essere incerta l'estensione a tali categorie soggettive della tutela della riservatezza e in genere dei diritti della personalità (per l'estensione delle norme sulla violazione di domicilio alle persone giuridiche, v. per esempio, Cass. sez. II, 6 maggio 1983, Saraceno, rv 161358; Cass. sez. I, 2 febbraio 1979,

Via XX Settembre 13/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

tezza dei dati, delle comunicazioni e più in generale del proprio domicilio informatico.

D'altra parte nessuno di noi sarebbe disponibile a tollerare l'ingresso abusivo e non autorizzato di estranei nella propria abitazione anche nel caso in cui questi non manifestino intenzioni aggressive nei nostri confronti ed agiscano al solo scopo di soddisfare la propria curiosità: il solo fatto che degli sconosciuti si siano introdotti nella nostra abitazione violando ed abbiano violato la nostra riservatezza ci infastidisce senza contare che il sentirci insicuri ed alla mercé di persone sconosciute rende tale fatto ancora più intollerabile.

Allo stesso modo un accesso non autorizzato nel nostro sistema informatico, ma anche, più semplicemente, nel nostro PC domestico genera insicurezza, ansia, paura e rende necessario affrontare gli ulteriori costi legati alla necessità di verificare tutti i dati al fine di verificare eventuali illecite modifiche. Il tutto senza considerare i possibili ulteriori danni.

Il reato di accesso abusivo si caratterizza, quindi, per l'alta potenzialità offensiva senza considerare che vi sono ipotesi in cui lo strumento utilizzato per l'accesso consente all'intruso di disporre del computer della "vittima" come desidera, al limite anche utilizzandolo per commettere illeciti; si rende, comunque, necessario specificare che i "poteri" acquisiti dall'intruso e, di conseguenza le sue capacità offensive, dipendo in massima parte da due elementi: il sistema operativo utilizzato sul computer della "vittima" ed il sistema utilizzato per accedere alla macchina.

Nel caso di un sistema operativo multiutente l'intruso godrà necessariamente solo ed esclusivamente dei "privilegi" propri dell'utente che stava utilizzando il computer al

---

Passalacqua, rv 142131) ma piuttosto perché principalmente fra dette categorie si rinvengono soggetti titolari di sistemi informatici protetti da misure di sicurezza (enti, anche pubblici, grandi società commerciali) per i quali lo ius excludendi è correlato prevalentemente, se non esclusivamente, a diritti di natura economico patrimoniale.

D'altra parte, con il riferimento al "domicilio informatico", sembra che il legislatore abbia voluto individuare il luogo fisico - come sito in cui si può estrinsecarsi la personalità umana nel quale è contenuto l'oggetto della tutela (qualsiasi tipo di dato e non i dati aventi ad oggetto particolari contenuti), per salvaguardarlo da qualsiasi tipo di intrusione (ius exludendi alios), indipendentemente dallo scopo che si propone l'autore dell'abuso. Pare, infatti, che una volta individuato nell'accesso abusivo a sistema informatico un reato contro la libertà individuale, il legislatore sia stato quasi costretto dalla sistematica del codice a quel tipo di collocazione, senza però che con la collocazione stessa si sia voluto anche individuare, in via esclusiva, il bene protetto con riferimento alle norme sulla violazione di domicilio, cioè la pax domestica ovvero la quiete e la riservatezza della vita familiare. / Va, inoltre, considerato che ove il legislatore ha avuto l'intento di tutelare la privacy vi ha espressamente fatto riferimento in modo inequivocabile, sia nella legislazione meno recente (v. la l. 8 aprile 1974, n. 98, il cui art. 1 ha introdotto nel codice penale, sotto la rubrica "interferenze illecite nella vita privata" l'art. 615 bis, sia in quella più vicina (v. la l. 31 dicembre 1996, n. 675, sulla Tutela delle persone o di altri soggetti rispetto al trattamento dei dati personali).

Via XX Settembre 131/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

momento del fatto[5]; in tale ipotesi è evidente che tanto più elevata sarà la posizione dell'utente nella scala gerarchica, tanto maggiori saranno i poteri dell'intruso fino ad ottenere il pieno controllo della macchina nel caso in cui riesca ad accedere come utente *root*[6]: in quest'ultimo caso, come laddove vi siano dei sistemi monoutente, le possibilità dell'intruso saranno limitate soltanto dal sistema utilizzato per accedere al computer.

Senza volerci addentrare in inutili particolari tecnici, è sufficiente qui ricordare come, in estrema sintesi, sia possibile accedere all'intero sistema ovvero soltanto alle sue risorse. Nel primo caso, l'intruso avrà il pieno controllo del sistema, tanto da indurre i commentatori ad utilizzare il termine "amministrazione remota"[7], mentre, nella seconda ipotesi, questi potrà "soltanto" visionare ed, eventualmente, modificare o cancellare, i *file* contenuti nell'hard disk senza, però, poter materialmente utilizzare il computer della vittima[8].

È evidente come, in entrambi i casi, il soggetto che subisce l'aggressione, è esposto al concreto rischio di ricevere dalla stessa notevoli danni.

3. In materia di accesso abusivo una delle questioni più dibattuta in dottrina e giurisprudenza è rappresentata dalla specificazione "*protetto da misure di sicurezza*" fatta dal legislatore.

In particolare si è giunti ad affermare che dette misure dovrebbero essere tali da garantire la sicurezza assoluta del sistema, ritenendo inidonee delle semplici password e giungendo a richiedere la completa sicurezza del sistema e l'assoluta certezza di impe-

---

5 Nel caso in esame si presuppone un accesso da remoto alla macchina compromessa, ma il discorso resta valido anche nel caso di accesso locale. È evidente che, in tal caso, l'intruso si troverà fisicamente alla tastiera del computer ed utilizzerà per accedere allo stesso *l'account* (*login* e *password*) di un utente autorizzato.

6 *Administrator* o *Amministratore* nel caso di sistemi Windows (XP o Vista). È comunque possibile che un intruso che riesca ad accedere ad un computer come utente normale (user) riesca poi ad acquisire maggiori privilegi utilizzando appositi comandi (i.e. "*su*" o "*sudo*" nel caso di sistemi Linux, "*esegui come*" nel caso di Windows XP o Vista).

7 In tale ipotesi l'intruso potrà utilizzare il computer come se si trovasse materialmente alla tastiera dello stesso. Potrà, quindi, non soltanto curiosare la suo interno alla ricerca di dati interessanti (password, numeri di carte di credito etc.), ma anche utilizzare il computer della vittima per navigare o commettere illeciti più gravi (i.e. tentativi di accesso a sistemi governativi o bancari). In tale ipotesi è plausibile che le responsabilità degli illeciti perpetrati dall'intruso ricadano sulla vittima stessa, almeno sino a quando la stessa non dimostrerà che la propria macchina è stata compromessa da un ignoto criminale. Il tutto, sempre e comunque, in relazione ai limiti indicati nelle pagine precedenti.

8 Un classico esempio di accesso da remoto alle sole risorse del sistema è quello che è possibile effettuare sfruttando il protocollo NETBIOS e la disattenzione di molti utenti di Windows che lasciano le proprie cartelle in condivisione mentre navigano in internet. Per un utilizzo illecito, ritenuto erroneamente penalmente non rilevante, di tale tecnica si veda G.U.P. di Roma, sent. 4/04/2000, n. 12005/98 RGNR.

Via XX Settembre 131/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

netrabilità[9].

Non sembra, tuttavia, potersi condividere una simile interpretazione, sia da un punto di vista tecnico (la sicurezza assoluta non può esistere in ambito informatico), sia da un punto di vista strettamente giuridico, stante le varie pronunce della Corte di Cassazione e la lucida analisi di parte della dottrina secondo cui potrebbe trattarsi anche di misure molto semplici e comuni[10].

Non può poi trascurarsi che, se l'illecito fosse stato caratterizzato dall'effrazione di misure di sicurezza, non avrebbe avuto alcuna rilevanza la condotta del soggetto che, dopo essere legittimamente penetrato nel sistema informatico, vi si mantenga contro la volontà, espressa o tacita, del titolare[11]; proprio questa seconda parte dell'articolo, insieme alla sua collocazione, deve farci comprendere appieno come l'interesse del legislatore sia effettivamente quello di garantire il libero accesso di chiunque alle informazioni pubbliche presenti nella Rete, tutelando al tempo stesso il diritto del cittadino di escludere dal proprio sistema le persone a lui non gradite sia in via preventiva, tramite misure di sicurezza, sia in un secondo momento, tramite l'invito a lasciare il sistema.

Allo stesso modo, la stessa inesistenza di misure di sicurezza non potrebbe essere addotta come giustificazione dal soggetto che, consapevolmente, si sia trattenuto in un sistema informatico contro la volontà tacita del proprietario dello stesso, ma non è possibile ignorare che seri dubbi sorgono in relazione agli elementi necessari per individuare tale "volontà tacita di esclusione".

E' opinione di chi scrive che tale volontà non possa essere stabilita aprioristicamente, ma deve essere desunta sulla base delle prassi e delle consuetudini informatiche e, pertanto, dovrà essere oggetto di specifica valutazione da parte del giudice il quale, nella valutazione della fattispecie, terrà conto anche delle specifiche competenze informatiche dell'imputato[12].

In linea di massima può, ad esempio, ritenersi circostanza notoria che assai di rado

---

9 G.U.P. di Roma, sent. 4/04/2000, n. 12005/98 RGNR, *passim*.

10 In particolare si veda Cass.Pen., Sez. VI, sent. 3067 del 14/12/1999; Cass. pen., sez. 5, sent. 12732 del 6/12/2000 in cui la Suprema Corte ha ribadito il concetto illustrato nel 1999 affermando che "la violazione dei dispositivi di protezione del sistema informatico non assume rilevanza di per sé, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone". Si veda poi Cass.Pen., Sez. V, sent.37322 del 08/07/2008 secondo cui "Ai fini della configurabilità del reato previsto dall'art. 615 ter cod. pen. (accesso abusivo ad un sistema informatico o telematico), la protezione del sistema può essere adottata anche con misure di carattere organizzativo, che disciplinino le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo"; Cass.Pen., Sez. II, sent.36721 del 21 febbraio 2008: "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")".

11 In tal senso Cass. Pen, sez. 5, sent. 12732 del 6/12/2000.

12 Ovviamente il giudice dovrà essere messo in condizione di valutare se il soggetto agente sia stato o meno in condizione di comprendere l'errore.

Via XX Settembre 13/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

un soggetto condivide volontariamente l'intero contenuto del proprio sistema garantendo un accesso libero e completo a chiunque, essendo simili situazioni, il più delle volte, riconducibili a meri errori nella configurazione del sistema operativo, ovvero di altri programmi, come, ad esempio quelli di *file sharing*[13] eventualmente utilizzati, ovvero a *bug*[14] presenti negli stessi ad insaputa dell'ignaro utente.

La volontà di escludere, tuttavia, non può essere astrattamente desunta, ma deve essere espressa o comunque intuibile da elementi esterni che siano non compatibili con la volontà di consentire l'accesso[15].

4. Particolarmente complessa è, invece, la questione relativa a quei soggetti che, pur autorizzati ad accedere al sistema per ragioni di servizio vi si trattengano o effettuino ulteriori accessi per motivazioni differenti[16].

La Corte di Cassazione ha avuto modo di occuparsi spesso di questi casi; a tal proposito, di particolare interesse è la decisione del maggio 2008[17]: il procedimento vedeva come imputato un cancelliere in servizio presso un ufficio giudiziario a cui era stato contestato, tra gli altri, il reato di cui all'art. 615 ter c.p., in concorso con quello di rive-

---

[13] Si tratta di programmi che permettono a più soggetti di scambiare tra di loro materiale di vario genere, (mp3, immagini, filmati, programmi…) tramite la condivisione delle cartelle che contengono detto materiale. È evidente che se uno sprovveduto utente condivide l'intero disco rigido ciò è, molto probabilmente, dovuto ad un errore dello stesso ed il soggetto che si trattenga nelle directory condivise oltre il tempo strettamente necessario a comprendere che si trova in una zona riservata del sistema è di fatto paragonabile ad un soggetto che, entrato in un locale pubblico, sia per errore finito in una privata dimora passando attraverso una porta lasciata distrattamente aperta: dovrebbe immediatamente abbandonare detto luogo. In tal senso Cass.Pen., Sez. I, sent. 6844 del 13/06/1994 secondo cui "risponde del reato di violazione di domicilio, chi si introduce o si intrattenga in un esercizio commerciale per minacciare o aggredire o comunque per uno scopo illecito del tutto opposto a quello di usufruire dei servizi offerti dal locale, ritenendosi implicita la contraria volontà del titolare dello *ius prohibendi*".

[14] Si tratta di errori, presenti nel sistema operativo o in altri programmi, che permettono funzioni non conosciute dall'utente e, spesso, non previste nemmeno dagli stessi programmatori. Per esempio alcuni anni fa un noto programma di *file sharing* conteneva un errore di configurazione che impostava di *default* la condivisione dell'intero hard disk permettendo a chiunque di sfogliarne il contenuto utilizzando un normale *browser*.

[15] Cass.Pen., Sez.I, sent. 2831 del 16/03/1978.

[16] Di volta in volta la Giurisprudenza si è occupata di differenti casi similari. Tipicamente si tratta di pubblici dipendenti (forze dell'ordine, addetti alle cancellerie, dipendenti dell'Agenzia delle Entrate...) che avevano utilizzato gli strumenti informatici dell'ufficio per acquisire informazioni di interesse personale proprio o di terzi.

[17] Cass. Pen., sez. V, sent. 26797 del 29 maggio 2008. Per un commento si veda R.Flor, "PERMANENZA NON AUTORIZZATA IN UN SISTEMA INFORMATICO O TELEMATICO, VIOLAZIONE DEL SEGRETO D'UFFICIO E CONCORSO NEL REATO DA PARTE DELL'EXTRANEUS", in *Cass. Pen*. 2009, 4, 1509.

Via XX Settembre 131/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

lazione di segreti di ufficio. All'imputato era contestato un accesso abusivo al sistema informatico dell'ufficio, tramite il quale egli aveva potuto apprendere notizie riservate relative a un fascicolo processuale penale, notizie poi indebitamente rivelate, secondo la prospettazione accusatoria, a un avvocato.

La Corte, rigettava il ricorso avverso la condanna per il reato di rivelazione di segreti di ufficio, ma l'annullava limitatamente al reato di accesso abusivo a un sistema informatico, sulla base della valutazione che l'operatore giudiziario era in effetti autorizzato ad accedere senza limiti, mediante la propria password, al registro informatico dell'ufficio, di guisa che non poteva ritenersi fosse stato effettuato un accesso abusivo: un profilo di rilevanza penale poteva porsi solo limitatamente all'uso dei dati così acquisiti, nella specie autonomamente sanzionabile ex art. 326 c.p.

La Corte, in particolare, osservava che il reato in esame consiste nell'accesso abusivo o nell'indebito (*invito domino*) trattenimento in un sistema informatico. Nel caso in esame appariva pacifico che l'autore dell'interrogazione incriminata aveva, in quanto Cancelliere dell'Ufficio del Giudice delle indagini preliminari del Tribunale di Milano, libero accesso ai registri informatizzati dell'Amministrazione della Giustizia e che l'interrogazione risultava effettuata impiegando la password legittimamente in suo possesso. A ciò doveva aggiungersi che non soltanto non vi era alcuna norma o disposizione interna organizzativa che impediva al cancelliere addetto alla singola sezione di consultare i dati del registro generale e le assegnazioni ai diversi uffici, ma anche laddove vi fosse stata tale inibizione sarebbe stata da considerarsi contraria ad ogni buona regola organizzativa, attese le necessità di consultazione di un ufficio giudiziario.

In conclusione la Corte escludeva sia che l'imputato avesse effettuato un accesso che non gli era consentito sia che si fosse trattenuto nel sistema oltre modi o tempi permessi, in quanto nessuna limitazione di tal genere era prevista per la lettura dei dati ad opera degli utilizzatori del sistema.

In relazione all'utilizzo illecito dei dati così acquisiti i Giudici hanno ritenuto che siffatta violazione non attiene alle modalità che regolano l'accesso al sistema e la consultazione dei dati in esso registrati, in quanto l'uso successivo che di tali dati s'è fatto e l'infedeltà dell'agente ammesso in via privilegiata al sistema viene ad essere assorbito nella condotta di rivelazione di notizie d'ufficio che erano, invece, destinate a rimanere segrete.

La norma in esame garantisce infatti la riservatezza del domicilio informatico quale spazio ideale (ma anche fisico) in cui sono contenuti i dati informatici, per salvaguardarla da qualsiasi tipo di intrusione non autorizzata, indipendentemente dallo scopo che si propone l'autore dell'accesso abusivo[18]; infatti è mediante l'apprestamento dei mezzi di protezione e l'erogazione delle correlate chiavi d'accesso che il titolare dello *ius exlu-*

[18] In tal senso si veda anche Cass. sez. VI, sent. 3067 del 14.12.1999.

Via XX Settembre 131/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

dendi seleziona gli ammessi, il cui dovere di riservatezza è altrove assicurato.

Dunque, al pari di quanto già in precedenza affermato[19], la Corte osservava che "la sussistenza o meno della contraria volontà dell'avente diritto" necessaria alla configurabilità del reato debba essere verificata "solo ed esclusivamente con riferimento al risultato immediato della condotta posta in essere dall'agente con l'accedere al sistema informatico e con il mantenersi al suo interno e non con riferimento a fatti successivi che, pur se già previsti, potranno di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione da parte dell'agente medesimo".

E' evidente che, laddove tali atti integrino autonome violazioni, gli stessi saranno direttamente sanzionabili a seconda degli specifici connotati delle ulteriori condotte criminose realizzate.

In conclusione il legislatore ha previsto un requisito di illiceità speciale, ripetendolo per ciascuna condotta alternativa, rappresentato dall'abusività, che costituisce un elemento essenziale del reato e richiede la valutazione della sussistenza della "mancata autorizzazione".

Proprio per tale ragione è necessario distinguere fra il caso in cui il soggetto sia stato autorizzato all'accesso al sistema, ma vi si sia mantenuto abusando del titolo di legittimazione, ovvero vi abbia svolto attività non attinenti al proprio lavoro e/o per raggiungere finalità completamente diverse da quelle consentite[20] da colui che, svolgendo la propria attività lavorativa ordinaria all'interno di un ente (come nel caso in esame), non osservi disposizioni organizzative interne sulle modalità di consultazione o di trattamento dei dati ovvero acceda per ragioni personali a dati a cui sarebbe comunque legittima-

---

[19] Cass.Pen, Sez. V, sent. 2534 del 20.12.2007.

[20] Si pensi, a titolo di esempio, all'ipotesi di un socio, o di un collaboratore, che acceda al sistema informatico per acquisire l'elenco dei clienti. In tal senso si veda Cass.Pen., sez.5, sent. 37332 del 8/07/2008 secondo cui "l'accesso al sistema è consentito dal titolare per determinate finalità, ovvero il raggiungimento degli scopi aziendali, cosicché se il titolo di legittimazione all'accesso viene dall'agente utilizzato per finalità diverse da quelle consentite non vi è dubbio che si configuri il delitto in discussione, dovendosi ritenere che il permanere nel sistema per scopi diversi da quelli previsti avvenga contro la volontà, che può, per disposizione di legge, anche essere tacita, del titolare del diritto di esclusione. [...OMISSIS...] l'introdursi in un sistema informatico al fine di duplicare i dati ivi esistenti costituisce (come si chiarirà anche meglio in seguito) condotta tipica del delitto di cui all'art. 615 ter c.p., perchè la intrusione informatica può sostanziarsi sia in una semplice lettura dei dati contenuti nel sistema, sia nella copiatura degli stessi". Allo stesso modo si veda Cass. Pen., sez. V, sent. 44362 del 14 ottobre 2003: "Ai fini della configurabilità del delitto di accesso abusivo ad un sistema informatico, la violazione dei dispositivi di sicurezza non rileva di per sè, ma solo come manifestazione di una volontà contraria a quella di chi dispone del sistema; ne consegue che commette il delitto di cui all'art. 615 ter c.p. anche colui che, autorizzato all'accesso per una finalità (controllo della funzionalità del programma informatico), utilizzi il titolo di legittimazione per copiare i dati gestiti da detto programma".

Via XX Settembre 13/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

to ad accedere[21].

Mentre nel primo caso non vi possono essere dubbi sulla contraria volontà del titolare del sistema, avendo egli fornito l'autorizzazione all'accesso ai soli fini di manutenzione, di aggiornamento o di collaborazione, con esclusione di ogni ulteriore attività estranea al rapporto, nel secondo caso, invece, è assai più oneroso provare l'eventuale illecito ed abusivo accesso: la contravvenzione alle disposizioni del titolare si può desumere solo se esiste un parametro "regolamentare" di riferimento, possibilmente scritto o, quanto meno, nella forma di una consuetudine frutto di un comportamento costante ed uniforme nel tempo seguito dal personale con l'assenso del titolare ed osservato nella convinzione che sia obbligatorio.

5. Differente è il discorso in relazione ad alcuni *tool* di controllo remoto che, per le loro caratteristiche intrinseche, possono essere (e spesso vengono) installati ed utilizzati senza che il titolare della macchina compromessa si accorga di nulla. In tale situazione è piuttosto evidente che l'accesso al sistema non potrà mai essere ritenuto in buona fede, salvo espressa autorizzazione dell'avente diritto.

Più complesso è, invece, il caso di programmi di controllo remoto che quando attivi sono visibili all'utente o che possono essere attivati dallo stesso; in un simile caso il Giudice sarà tenuto a valutare le circostanze che hanno portato all'accesso, stabilendo, in base al suo prudente apprezzamento, se il soggetto si sia introdotto e trattenuto nel sistema per errore scusabile (i.e. errore nella digitazione dell'indirizzo IP), ovvero nella consapevolezza di ledere l'altrui diritto.

L'illecito è, infatti, caratterizzato dalla contravvenzione alle disposizioni, espresse o tacite, del titolare esattamente come avviene nel delitto di violazione di domicilio. La giurisprudenza, perché possa configurarsi il reato, richiede, infatti, soltanto che il sistema informatico non sia aperto a tutti, come avviene nel caso delle pagine web ospitate su un server[22].

Il reato, comune ed a forma libera, si perfeziona con l'acceso al sistema informatico, identificabile di fatto con il superamento delle barriere predisposte dal *dominus*, ovvero con il trattenersi all'interno dello stesso nonostante l'avente diritto abbia manifestato, espressamente o tacitamente, la sua contraria volontà in proposito. La specificazione "abusivamente" fatta dal legislatore sembra escludere la punibilità del soggetto agente

[21] Oltre alla sentenza qui in esame si veda Cass. Pen., sez. VI, sent. 39290 del 08 ottobre 2008; Cass. Pen., sez. V, sent. 2534 del 20 dicembre 2007; Cass. Pen., sez. V, sent. 6459 del 04 dicembre 2006.

[22] Tribunale di Milano, sez. III, 19 marzo 2007 "La copia di più pagine HTML da un sito web non protetto da misure di sicurezza ad un altro sito web non integra di per sé né il reato di cui all'art. 615 ter c.p. né quello di cui all'art. 640 ter c.p. La pubblicazione su un sito web di contenuti oggetto di copiatura da altro sito web può costituire, qualora ne ricorrano gli estremi, violazione della l. n. 633 del 1941 sul diritto di autore".

Via XX Settembre 131/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

nelle ipotesi di colpa essendo richiesto il dolo generico consistente nella coscienza e volontà di introdursi o mantenersi in un sistema informatico o telematico contro la volontà del titolare[23].

In merito all'oggetto tutelato dalla norma non sembra potersi accogliere la teoria secondo cui questo sarebbe "la riservatezza delle informazioni" e non l'inviolabilità del "domicilio informatico"[24].

In realtà l'oggetto tutelato è complesso e, se lo stesso può essere visto anche nella riservatezza del titolare, è assai più ampio[25]; sembra, infatti, preferibile la tesi, avallata anche dalla giurisprudenza della Suprema Corte, secondo cui la collocazione della norma ed i termini utilizzati dal legislatore indicano la volontà di quest'ultimo di assicurare una protezione a trecentosessanta gradi del "domicilio informatico", quale spazio ideale (ma anche fisico, in cui sono contenuti i dati informatici) di pertinenza della persona, al quale estendere la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto. Va, infatti, considerato, come la Corte non ha mancato di fare, che laddove il legislatore ha avuto l'intento di tutelare la privacy vi ha espressamente fatto riferimento in modo non equivocabile, sia nella legislazione meno recente[26] sia in quella a noi più vicina[27].

---

[23] Non si ritiene necessaria l'altruità del sistema, laddove costante giurisprudenza ha ammesso che lo *ius excludendi* possa essere esercitato dall'avente diritto anche nei confronti dello stesso proprietario del bene. *Infra multis* si veda Cass. pen., sez. 5, sent. 335 del 18/01/1983.

[24] A tal proposito esemplare è Cass.Pen, sez. V, sent. 46454 del 22 ottobre 2008 da cui viene escluso il trattamento illecito, ma confermato l'accesso abusivo "Il reato di trattamento illecito di dati personali, già previsto dall'art. 35 l. 31 dicembre 1996 n. 675 (ora previsto, in rapporto di continuità normativa, dall'art. 167 d.lg. 30 giugno 2003 n. 196), non è configurabile allorché ricorrano le condizioni di cui alla clausola limitativa introdotta dall'art. 5, comma 3, d.lg. n. 196 del 2003, secondo cui il trattamento di dati personali se effettuato da persone fisiche per fini esclusivamente personali "è soggetto all'applicazione del presente codice (ergo, il codice della privacy) solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione" (da queste premesse, in una fattispecie in cui gli imputati si erano introdotti abusivamente nella rete informatica del gestore telefonico Tim e avevano acquisito i dati del tabulato telefonico di una persona per raccogliere prove da fornire alla committente circa l'infedeltà del marito, la Corte, mentre ha rigettato il ricorso relativamente al reato di cui all'art. 615 ter c.p., ha annullato la condanna limitatamente al reato di cui all'art. 35 l. n. 675 del 1996, apprezzando come nel caso concreto difettasse la destinazione dei dati raccolti alla comunicazione sistematica o alla diffusione, per essere stati questi acquisiti per fini esclusivamente personali della committente)".

[25] In tal senso si veda Cassazione penale, sez. V, sent.11689 del 06 febbraio 2007 secondo cui "L'accesso abusivo a un sistema telematico o informatico si configura con la mera intrusione e non richiede che la condotta comporti una lesione della riservatezza degli utenti né tantomeno che "l'invasione" sia compiuta con l'obiettivo di violare la loro privacy".

[26] Cfr. Legge 8 aprile 1974, n. 98, il cui articolo 1 ha introdotto nel codice penale, sotto la rubrica "interferenze illecite nella vita privata", l'art. 615 bis.

[27] Cfr. Legge 31 dicembre 1996, n. 675, titolata "Tutela delle persone o di altri soggetti rispetto al tratta-

Via XX Settembre 13/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

Il reato è perseguibile a querela della persona offesa[28], ma non bisogna dimenticare che quasi sempre questo fatto è connesso con l'illecita acquisizione del file delle password e tale fatto integra il reato di cui all'art. 615 quater procedibile d'ufficio. Tale circostanza sembrerebbe imporre l'obbligo (almeno ai sistemisti di Enti Pubblici ed ai pubblici ufficiali) di denuncia ai sensi dell'art. 331 c.p.p., obbligo sanzionato penalmente ai sensi degli artt. 361 e 362 c.p. in caso di omissione.

Non sembra, infine, potersi ragionevolmente escludere la punibilità del tentativo, anzi proprio a proposito del tentativo sorgono non pochi problemi.

6. La questione relativa alla possibilità di configurare un tentativo in relazione al reato di cui al 615-ter ha, infatti, sollevato ampie polemiche in dottrina, soprattutto in relazione alle modalità con cui il reato in questione potrebbe essere tentato. In particolare, ci si riferisce qui ad una tecnica piuttosto diffusa, nota con il nome di *port scanning*[29], che consiste nell'utilizzare programmi in grado di verificare se un determinato sistema informatico ha o meno alcuni servizi[30] in ascolto.

---

mento dei dati personali". Si veda oggi il Dlgs 196/03.

[28] Il soggetto legittimato a proporre querela è stato identificato dalla dottrina nel titolare del sistema e non nella parte concretamente danneggiata dall'incursione. Quest'ultima potrà, evidentemente, costituirsi parte civile per ottenere il risarcimento del danno.

[29] Possiamo definire il *port scanning* come quel processo di connessione a porte TCP e UDP appartenenti al sistema in cui si vuole tentare di accedere al fine di determinare quali servizi siano in esecuzione o stato di *listening* (ascolto). L'identificazione delle porte in ascolto è critica al fine di determinare il tipo di sistema operativo utilizzato e, soprattutto, le applicazioni in uso; un aspirante intruso può, infatti, abusare dei servizi presenti sulla macchina, sia in caso di cattiva configurazione, sia nel caso in cui siano presenti servizi non autorizzati (*i.e. trojan horse* o programmi similari). Negli ultimi anni le tecniche per effettuare portscanning hanno subito un notevole miglioramento tenendo presente i diversi obiettivi che un possibile intruso potrebbe voler raggiungere. In tal senso Tribunale di Roma, Ordinanza 1 agosto 2001, Iacorelli Vs Infostrada SpA in cui il Tribunale ha definito tale pratica come "una serie programmata di tentativi di accesso diretti ad evidenziare, in base alle risposte fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo al fine di acquisire gli elementi per una successiva intrusione o esclusivamente di conoscere le caratteristiche dell'altrui sistema o server, adibito all'erogazione di determinati servizi in rete". In alternativa al *port scanning* è possibile effettuare un *net scanning*. Quest'ultimo prende di mira un'intera rete, o una sua porzione, per verificare quali e quanti computer hanno una determinata porta (o alcune determinate porte) in ascolto. Se, per esempio, si volesse verificare quanti, e quali, sono i computer della sottorete 192.168.01.01 infetti dal server di Back Orifice, quindi virtualmente accessibili (a condizione di possedere il relativo programma client), non occorrerebbe fare altro che avviare un programma di port scanning e lanciare la scansione sulla sottorete 192.168.01.* (dove xxx è un numero che si è preferito oscurare) alla porta 33337; allo stesso modo, se si cercasse il server di Net Bus si effettuerebbe una scansione alla ricerca della porta 12345 e via di questo passo.

[30] Con il termine "*servizi*" si indicano i programmi in esecuzione in una determinata macchina identificandoli sulla base delle loro funzioni e del servizio che offrono (*i.e.* server web, server ftp, server di posta …). Per semplificare possiamo paragonare il nostro computer ad un ufficio con tantissimi spor-

Via XX Settembre 13/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

È evidente che, durante la navigazione in internet, non tutti i servizi sono in ascolto e le relative porte sono, pertanto, "chiuse", pronte per essere "aperte" nel momento in cui l'utente decide di utilizzare, o far utilizzare, un determinato servizio. Oltre le porte "standard"[31], vi sono, tuttavia, numerosissime altre porte che vengono utilizzate da specifici programmi. Potrebbe trattarsi di porte utilizzate da programmi di file sharing, da programmi di chat ovvero da un ventaglio pressoché infinito di possibili utilizzi leciti. Tuttavia, accanto ai programmi leciti, troviamo anche dei programmi illeciti, che si attivano ad insaputa dell'utente e permettono ad un terzo di accedere al suo computer. Anche queste porte hanno subito una sorta di standardizzazione, tanto che moltissimi programmi di difesa (in particolare *firewall* e programmi di monitoraggio delle porte) automaticamente identificano come tentativo di accesso ogni contatto a quelle determinate porte.

Proprio questo è il punto nodale della questione: molto spesso il tentativo di accesso segnalato dal *firewall* è, in realtà, soltanto un *port scanning* o, ipotesi più frequente, un *net scanning* spesso effettuato da ragazzini alla ricerca di un computer infetto a cui accedere.

Lo *scanning* in sé e per sé, tuttavia, non può in alcun modo essere ritenuto un accesso abusivo al sistema laddove dottrina e giurisprudenza sono concordi nel ritenere che il reato venga ad esistenza soltanto laddove l'accesso al sistema sia effettivamente avvenuto. È, tuttavia, innegabile che lo stesso possa essere ritenuto un atto prodromico all'accesso vero e proprio in quanto rappresenta il mezzo principale per raccogliere infor-

telli specializzati in determinate funzioni. Ogni sportello è caratterizzato da un numero che lo identifica permettendo al cliente di rivolgersi direttamente allo sportello giusto. Così se ci si vuole collegare ad un sito internet si "busserà" alla porta 80 (in alcuni casi 8080) del server, mentre se si vuole leggere la posta ci si connetterà alla porta 110, alla 25 per inviare messaggi, e via di questo passo. È evidente che si tratta di procedure automatizzate, basate sulla standardizzazione delle porte, ma nulla vieta ad un utente di modificare questi parametri. Possiamo quindi sostenere che, generalmente, ad ogni porta corrisponde un determinato tipo di programma in ascolto che ne permette l'utilizzo da parte di un computer remoto.

[31] Note anche come "*well know ports*" ed individuate da IANA (Internet Assigned Numbers Authority) nelle porte che vanno da 1 a 1023. Queste porte non dovrebbero essere utilizzate senza una registrazione di IANA. La procedura di registrazione è definita nella RFC4340, Sezione 19.9. Accanto alle "*well know ports*" ci sono le "Registered Ports" comprese tra la 1024 e la 49151.

Via XX Settembre 131/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

mazioni essenziali sul computer che si desidera attaccare ovvero, nel caso di *net scanning*, per individuare i possibili bersagli: computer "compromessi" all'interno di una rete.

Il punto nodale della questione è valutare se lo *scanning* sia un atto diretto in maniera non equivoca a violare un sistema informatico e quindi punibile ex articolo 56 del codice penale, ovvero costituisca un atto preparatorio non punibile[32].

Esemplificando, è possibile paragonare un utente che effettua uno *scanning* ad una persona che, a seconda dei casi, verifica la chiusura delle porte e delle finestre di un'abitazione ovvero verifica la chiusura della porta in tutti gli appartamenti di un grosso condominio. Possono tali atti essere ritenuti *idonei* e *diretti in maniera non equivoca* alla commissione del crimine di violazione di domicilio?

La risposta non è affatto semplice, stante l'impossibilità di accedere ad un sistema esclusivamente effettuando uno *scanning*: anche se si individua una falla, è, infatti, necessario che il soggetto in questione possieda gli strumenti adatti per sfruttare tale falla in modo tale da accedere effettivamente al sistema. Chi scrive ritiene che il portscanning debba essere valutato prestando particolare attenzione ai servizi richiesti. La Suprema Corte[33] ha, infatti, a più riprese sottolineato come "gli atti meramente preparatori possono costituire materia di tentativo solamente quando siano idonei e diretti in modo non equivoco alla consumazione di un delitto. Essi, cioè, debbono avere potenzialità causale di produrre l'evento e rivelare, in modo non equivoco, l'intenzione di commettere un delitto".

In merito alla *potenzialità causale* questa è stata individuata come la suscettibilità dell'azione a produrre l'evento che rende consumato il delitto voluto[34]. Appare evidente come il *portscanning*, soprattutto se effettuato su una *subnet* alla ricerca di computer infetti, costituisca un presupposto necessario e sufficiente all'accesso abusivo: una volta individuate le macchine compromesse, infatti, null'altro occorre all'intruso se non indicare il loro indirizzo IP al client del programma[35]. Un *portscanning* mirato ad una porta

[32] Sulla punibilità degli atti preparatori, laddove univocamente diretti alla commissione dell'illecito, si veda, tuttavia, Cass. pen., sez. 2, n. 2791 del 16/03/1992 "anche un atto preparatorio può integrare gli estremi del tentativo, quando sia idoneo e diretto in modo non equivoco alla consumazione di un reato, cioè quando abbia la capacità, valutabile ex ante, di raggiungere il risultato prefisso, in relazione alle circostanze del caso, e sia inoltre univocamente diretto alla consumazione del reato"; Cass. pen., sez. 2, n. 3692 del 20/04/1985 "un atto meramente preparatorio può costituire materia di tentativo punibile, sempre che l'atto stesso risulti idoneo e diretto in modo non equivoco alla commissione di un delitto".

[33] Cass. pen., sez. 2, n. 10496 del 25/10/1988; *conf.* Cass. pen., sez. 2, n. 295 del 26/07/1995.

[34] Cfr. Cass. pen., sez. 1, n. 1915 del 22/02/1982.

[35] Tornando all'esempio fatto in precedenza, immaginiamo che l'aspirante intruso abbia effettuato uno scanning della subnet 192.168.1.* alla porta 33336 (dove troviamo generalmente in ascolto il trojan Back Orifice). Una volta appurato che la macchina che si trova all'indirizzo IP 192.168.1.20 è infetta non dovrà fare altro che lanciare il client di Back Orifice e digitare 192.168.1.20:33336 per accedere

Via XX Settembre 13/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it

generalmente utilizzata da un *trojan* può, quindi, essere ritenuto un atto idoneo diretto in maniera non equivoca a violare il sistema e, pertanto, in esso può ravvisarsi un'ipotesi di delitto tentato.

La *ratio* dell'art. 56 del codice penale è, infatti, di marcare il confine tra atti leciti ed atti illeciti identificando l'inizio dell'attività punibile[36]. Deve, pertanto, ritenersi che il reato *de quo* inizi a perfezionarsi nel momento in cui l'aspirante intruso inizia a saggiare le difese della vittima, ovvero tenta di individuare una facile preda utilizzando particolari strumenti tecnici.

alla macchina in questione. Le uniche possibili incognite sono rappresentate dalla possibilità che il server Back Orifice sia protetto da una password oppure che si tratti di un programma che simula detto server registrando gli attacchi. Al di fuori di tali, remote, ipotesi, l'intruso avrà accesso alla macchina.

[36] In tal senso Cass. pen., sez. 1, n. 10574 del 09/10/1987.

Via XX Settembre 131/h, 06124 Perugia
tel. 075.5716115 - fax 075.5724079
cell. 347.6581799 - 3495738557
ciace.mariacristina@ordineavvocati.perugia.it
florindi.emanuele@ordineavvocati.perugia.it