STUDIO LEGALE CANESTRINI

[ACCESSO ABUSIVO A SISTEMA INFORMATICO

RIFLESSIONI SULL'ART. 615 TER C.P. CON PARTICOLARE RIFERIMENTO ALLE MISURE DI SICUREZZA]

1. Cenni sul funzionamento del World Wide Web ("Internet")

Le informazioni di ogni sito vengono memorizzate su documenti chiamati **pagine web** ed inserite in computer chiamati **web server**.

Quando sul programma che serve per visualizzare le pagine web (browser: es. Chrome, Internet Explorer, ...) viene digitato un indirizzo internet (es. www.canestrinilex.it)[1], esso non fa altro che creare una richiesta della pagina al relativo web server[2]. Quando la richiesta viene accettata dal Server, la pagina viene letta ed interpretata dal browser secondo le istruzioni contenute che generalmente erano in formato html[3] (ora si stanno affermando anche formati diversi, cd. dinamici).

Qualsiasi sito necessita dunque di un **web server**, ovvero di un computer connesso alla rete che possa contenere tutte le pagine web e sia in grado di comunicare con i computer esterni.

Questo web server deve essere dunque necessariamente in comunicazione con il mondo esterno; è possibile (anzi è usuale) che solo alcune parti siano liberamente accessibili mentre altre necessitano di un accesso mediante *password* e *user name* (ad es. per poter caricare sul web server contenuto nuovo - cd. upload - , ...).

2. L'accesso abusivo a sistema telematico e le misure di sicurezza: l'elemento oggettivo

La norma incriminatrice, come noto, punisce chi

> "***abusivamente*** *si introduce in un* ***sistema informatico o telematico protetto da misure di sicurezza*** *ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*"

2 a) Introduzione abusiva

La formulazione letterale è quantomeno infelice, tanto da aver recentemente originato per altra questione di diritto una remissione alle SS.UU. della Corte di Cassazione: Cass. pen., sez. V, ord. 11.2.2011 (dep. 23.3.2011), n. 11714, Pres. Calabrese, Est. Scalera, ric. Casan).

In dottrina e giurisprudenza (v. Cass., sez. 5^, n. 26797/2008) è stato giustamente criticata l'espressione "***abusivamente*** *si introduce*" per la sua forte ambiguità e la conseguente possibilità d'imprevedibili e pericolose dilatazioni della fattispecie penale se non intesa in senso di "accesso non autorizzato", secondo la più corretta espressione di cui alla cd. "lista minima" della Raccomandazione del Consiglio d'Europa (89) 9, attuata in Italia con la L. n. 547 del 1993, e di "accesso senza diritto" (*access ... without right*) impiegata nell'art. 2

[1] Detto anche **U.R.L.**, acronimo *di uniforme resource locator*.
[2] Ciò avviene mediante il protocollo http (che infatti precede l'URL: http://www.canestrinilex.it).
[3] In caso di mancata specificazione della sottopagina si viene indirizzati automaticamente alla pagina index.html, cioè alla pagina di partenza standardizzata: digitando http://www.canestrinilex.it vengo indirizzato a http://www.canestrinilex.it/index.html.

della Convenzione sul cyber crime (cui al quale con la L. n. 48 del 2008 non s'è ritenuto di dare ulteriore attuazione, trattandosi d'ipotesi già disciplinata dall'art. 615 ter cod. pen.).

In ordine a tale punto si è ritenuto (in assenza di risolutive pronunce della Suprema Corte in merito) che "l'avverbio in questione rappresenta un vero e proprio caso di **antigiuridicità speciale** che richiede per la punibilità l'assenza di situazioni scriminanti ulteriori rispetto alle cause di giustificazione codificate; in particolare si è sottolineato come norme primaria di riferimento è quella dettata a tutela della privacy (Commentario Cedam, sub articolo 615ter Cp, p. 2033). Ora, come è noto, le ipotesi di illiceità speciale riguardano quei casi in cui è la stessa norma a prevedere espressamente un fatto commesso "abusivamente", "illegittimamente" "indebitamente" mediante un diretto riferimento a norme extrapenali; secondo gli indirizzi giurisprudenziali prevalenti secondo cui soltanto in presenza di "finalità diverse" o "differenti scopi" potrebbe parlarsi di accesso abusivo (secondo l'equazione finalità diversa/assenza di autorizzazione).

2 b) Il sistema informatico

Per sistema informatico o telematico deve intendersi "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente" (Cass. 3067/1999 riv 214945).

Il sistema informatico, dovendo svolgere una funzione - mediante tecnologie informatiche - è dunque tale se gestisce od elabora dati, mentre tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è "sistema informatico".

La mera copiatura dei contenuti di un sito, realizzata semplicemente a partire dalla visualizzazione del sito senza introduzione nella "memoria interna" del sito o nei programmi che ne consentono il funzionamento, non concreta interazioni con il sistema informatico come definito dalla giurisprudenza; peraltro, si segnala che la norma in questione è stata introdotta al fine di reprimere il fenomeno degli hacker, cosa ben diversa dalla consultazione / visualizzazione / copiatura del contenuto di una pagina web.

2 c) Esistenza di misure di sicurezza

Dirimente ai fini della configurabilità del reato è la presenza o meno delle cd. misure di sicurezza nel sistema informatico / telematico.

Le “misure di sicurezza”, il cui superamento è parte dell’elemento oggettivo del reato, non sono definite dal legislatore; la definizione è comunque ricavabile da migliore dottrina e dall’analisi puntuale delle pronunce giurisprudenziali.

Secondo Natalini[4], il "sistema" di protezione concretamente considerato, per poter essere l'oggetto materiale del reato in discorso, deve essere ulteriormente connotato da un preciso elemento qualificativo: deve risultare protetto da "misure di sicurezza".

Sono tali quelle protezioni (che possono essere apposte sia a livello di apparecchiature (hardware) che di programmi (software) che **integrano quei peculiari meccanismi operativi che impediscono un libero accesso al sistema e, quindi, la presa di cognizione di informazioni e dati ivi rinvenibili) a terzi estranei (ad esempio, codice alfanumerico di accesso, chiave di avviamento, eccetera**) (Ceccacci, "Computer crimes. La nuova disciplina sui reati informatici", Milano, 1994, p. 19).

L'apposizione di siffatte misure protettive del sistema informatico o telematico costituisce infatti l'estrinsecazione della *voluntas excludendi* manifestata dal titolare del relativo *ius*.

L'accesso ad un sistema non protetto, pertanto, risulta atipico e penalmente lecito (ma non anche civilisticamente, dovendosi, a tale riguardo, ulteriormente verificare in concreto un danno ingiusto risarcibile ex articolo 2043 Cc (Nunziata, "La prima applicazione giurisprudenziale del delitto di "accesso abusivo ad un sistema informatico" ex articolo 615ter Cp", in Giurisprudenza di merito, 1998, p. 714)[5].

In giurisprudenza, come è stato acutamente osservato (Cass., Sez. 5^ penale, 16 giugno 2000 - 10 agosto 2000, n. 9002, CED 217734 e Cass., Sez. 5^ penale 7 novembre 2000, Zara e da ultimo Cass., Sez. 2^ penale, 4 maggio 2006 - 14 settembre 2006), la **violazione dei dispositivi di protezione del sistema informatico non assume rilevanza di per sè, perchè non si tratta di un illecito caratterizzato dalla effrazione dei sistemi protettivi, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone**. In effetti l'illecito è caratterizzato dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio e come è testimoniato dalla seconda parte dell'art. 615 ter c.p., comma 1 (Cassazione penale sez. V. 08 luglio 2008, n. 37322)[6].

In sostanza, le misure protettive si atteggiano, in ambiente informatico, a surrogato della perimetrazione muraria o della delimitazione spaziale connaturata al domicilio tradizionale per la tutela di beni giuridici come il patrimonio, la riservatezza, la fede pubblica, l'inviolabilità dei segreti e la libertà individuale. Non si deve, quindi, far riferimento alla manomissione di sistemi protettivi, ma, piuttosto, alla contravvenzione alle disposizioni del titolare, interpretazione, questa, fondata anche su reiterati pronunciamenti della giurisprudenza di merito e di legittimità (v. Tribunale di Torino, 7 febbraio 1998; Cass.

---

[4] Aldo Natalini, ACCESSO A SISTEMI INFORMATICI: L'ILLICEITÀ (SPECIALE) RICHIEDE LESIONE CONCRETA, in Diritto e Giustizia, 2005, 46, 42 ss..

[5] In questo senso, non è mancato però in dottrina chi ha criticato la scelta restrittiva del legislatore, in considerazione del fatto che, se il domicilio informatico va tutelato in quanto estensione della mente e della personalità di ciascuno, tale tutela non può essere condizionata da particolari tecnici del sistema (Pica, "Reati informatici e telematici", in Digesto delle discipline penalistiche, Torino, Aggiornamento 2002, p. 259): il tutto riportato in Natalini, cit.

[6] La giurisprudenza peraltro specifica che le misure di sicurezza, rilevanti come espressione dello *ius excludendi alios*, rilevanti quali misure di protezione del sistema, possono consistere In misure di carattere organizzativo che disciplinino le modalità di accesso ai locali ove il sistema è ubicato ed indichino le persone abilitate all'utilizzo dello stesso (Cassazione penale sez. V. 08 luglio 2008, n. 37322);

penale, Sez. 5, 7 novembre 2000, n. 12732, come confermato da Cassazione penale sez. II, 21 febbraio 2008, n. 36721; cfr. detta pronuncia anche per i rilievi che seguono).

Si ha dunque introduzione in un sistema informatico o telematico protetto allorchè si sono oltrepassate le barriere (logiche e/o fisiche), che presidiano l'accesso alla memoria interna del sistema e si è, quindi, in condizioni di poter richiamare i dati e i programmi che vi sono contenuti.

E' solo in questo momento, infatti, che può dirsi realizzata la situazione di pericolo per la riservatezza dei dati e dei programmi memorizzati dall'elaboratore che giustifica l'intervento della sanzione penale. Il reato si consuma con il semplice accesso ad un sistema informatico o telematico, a prescindere dal fine, purchè il sistema sia protetto da misure di sicurezza.

Nella nozione di misure di sicurezza possono farsi rientrare tutte quelle misure di protezione, al cui superamento è possibile subordinare l'accesso ai dati e ai programmi contenuti nel sistema.

Può trattarsi, ad es., di codici di accesso, alfabetici o numerici, da digitarsi alla tastiera, ovvero memorizzati sulla banda magnetica di una tessera da introdurre in un apposito lettore. Oltre a queste misure cd. logiche, vengono in rilievo anche misure di tipo fisico (ad es. chiavi metalliche per l'accensione dell'elaboratore); in tal caso si fa riferimento a queste misure con l'espressione misure di protezione hardware, per distinguerle da quelle logiche di tipo software.

Sempre Cass. Pen. 36721/2008 cit. chiarisce che è certamente necessario che il sistema non sia aperto a tutti, ma assume rilevanza qualsiasi meccanismo di selezione abilitati all'accesso. Ne consegue che anche l'adozione di una protezione semplice, costituita da una parola chiave (*password*) rappresenta pur sempre un'esplicitazione del divieto di accesso al sistema e legittima la tutela in sede penale[7].

Le misure di sicurezza possono consistere **in dati di accesso personali** (Cassazione penale sez. II, 24 febbraio 2011, n. 9891), o **in apposito codice utente e di una password**, specificando poi che dall'interpretazione sistematica e letterale della norma è evidente che il compito di rendere manifesta la volontà del titolare dello *spatium operandi et deliberandi* di escludere soggetti non autorizzati è affidato alle " misure di sicurezza ", nel caso di specie alle credenziali di autenticazione. Pertanto, in assenza di diverse specifiche disposizioni organizzative o regolamentari (che nel caso di cui ci si occupa non esistevano), esse rimangono gli unici elementi obiettivi che individuano i limiti dell'autorizzazione all'accesso. (G.I.P. Bari, Uff. Indagini preliminari Bari, 11 dicembre 2009)[8], o in

[7] Prosegue la pronuncia citata: “Corretta, pertanto, è la motivazione data sul punto dalla Corte di merito, secondo la quale "l'attribuzione ai dipendenti autorizzati di username, sia pure costituita dalla lettera iniziale del proprio nome seguita dall'intero cognome e di una password composta da sei o otto elementi scelti dall'utente, si configura, senza meno, come una protezione del sistema, operante nei confronti di accessi provenienti dall'esterno". Ed, invero, nel caso di specie, l'accesso al sistema avveniva attraverso l'immissione del proprio username assegnato dalla società e composto dalla prima lettera del nome e dal cognome, quest'ultimo per esteso, oltre che dalla propria chiave di accesso o password composta di sei caratteri a scelta dell'utilizzatore con validità di 140 giorni, scaduti i quali doveva essere rinnovata (Cassazione penale sez. II 21 febbraio 2008, n. 36721).

[8] Richiama la pronuncia quell’orientamento giurisprudenziale secondo il quale la qualificazione di abusività va intesa in senso oggettivo con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza , apprestate al fine di impedire accessi

"impostazioni di protezione del browser" che regolano l'esecuzione automatica di download e contenuti attivi durante la navigazione Internet, permettendo di configurare diversi livelli di protezione, con richiesta o meno di conferma da parte dell'utente e con eventuali barriere automatiche per determinati programmi o contenuti attivi (...) qualificabili misure di protezione, giacché esse attinenti esclusivamente non alla configurazione di Explorer (modalità di fruizione) ma alla maggiore o minore interazione passiva del sistema informatico, connesso al web, dall'esterno verso il suo interno (Corte appello Bologna sez. II, 27 marzo 2008).

Alla stregua delle considerazioni svolte, può affermarsi:

a) il reato di accesso abusivo ad un sistema informatico o telematico sussiste ogni volta che vengano **sorpassati gli ostacoli** che presiedono l'accesso al sistema, non presupponendo necessariamente che l'agente sia in grado di poter richiamare e disporre dei dati e dei programmi contenuti nel computer violato;

b) il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico e, quindi, con l'introduzione di un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'inclusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa;

c) il reato di accesso abusivo ad un sistema informatico si realizza anche mediante la violazione di un dispositivo di protezione del sistema costituito da una parola chiave (password) (Cassazione penale sez. II, 21 febbraio 2008, n. 36721).

3. L'elemento soggettivo

Il dolo richiesto dalla norma incriminatrice è un dolo generico, che consiste nella volontà di introdursi o di mantenersi nella memoria interna di un elaboratore, in assenza del consenso del titolare dello ius excludendi, e con la consapevolezza che quest'ultimo ha predisposto delle misure di protezione per i dati che vi sono memorizzati. E' del tutto irrilevante lo scopo perseguito dall'agente nel commettere l'accesso abusivo (Cassazione penale sez. II 21 febbraio 2008, n. 36721): ma deve pur sempre esserci la consapevolezza delle misure di sicurezza con concretano lo ius excludendi.

Avv. Nicola Canestrini

---

indiscriminati, senza che rivestano rilevanza la finalità che si propone l'autore e l'uso successivo dei dati che se illeciti, integrano eventualmente un diverso titolo di reato. Ha confermato l'accezione in senso restrittivo della formula di "accesso non autorizzato" in linea con la Raccomandazione del Consiglio d'Europa (cfr. supra).