Accesso abusivo ad un sistema informatico o telematico

di: **Bruno Fiammella**

Relazione per il convegno "I reati informatici e la criminalità aziendale", Salone degli industriali, Reggio Calabria, 23 giugno 2001 - Pubblicato anche su: www.filodiritto.com

La realtà economica e sociale in cui viviamo ci consente di asserire con certezza che i sistemi informatici e telematici hanno ormai preso il sopravvento tanto da condizionare "l'organizzazione sociale, lo sviluppo e la crescita delle relazioni interpersonali, della manifestazione e della comunicazione del pensiero"[1].

L'attività finanziaria ed organizzativa ha trovato nei sistemi di comunicazione a distanza, uno strumento ideale, in quanto rapido, efficace e soprattutto economico, per la crescita e lo sviluppo, tanto da rimanerne condizionata.

L'interesse dell'economia e dei fautori dello sviluppo verso le nuove tecnologie comporta, inevitabilmente, una crescita dell'attenzione dell'uso e delle potenzialità di questi sistemi anche da parte di una nuova forma di criminalità: quella informatica. Se potevano ancora esistere "dei dubbi sulla rilevanza - qualitativa ed in prospettiva quantitativa - del fenomeno "criminalità informatica, recenti provvedimenti dell'autorità giudiziaria hanno dimostrato come comportamenti penalmente rilevanti possano frequentemente presentarsi anche nell'ambito di attività imprenditoriali e professionali nei termini descritti dalle fattispecie normative, effetto questo anche della globalizzazione dello strumento informatico come modalità di espressione dell'attività economica"[2].

Nell'ambito quindi delle fattispecie introdotte nel codice penale con la L. 547/93, é indispensabile individuare quelle che rappresentano uno strumento di tutela primaria, immediata ed effettiva dei sistemi informatici e telematici, nonché, soprattutto, degli interessi che attraverso tali sistemi vengono perseguiti.

La salvaguardia dei sistemi informatici dall'accesso abusivo costituisce uno degli aspetti più complessi e delicati della criminologia informatica e trova la sua genesi nel momento in cui l'evoluzione tecnologica ha consentito a più computer o a più sistemi di "dialogare" tra loro.[3]

La possibilità di poter accedere attraverso le normali linee telefoniche ai sistemi informativi, sia dei privati che degli operatori pubblici, ha posto l'opinione pubblica di fronte alla necessità di confrontarsi rispetto ad una nuova esigenza di tutela, quella del proprio domicilio

[1] **Cesare 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.
[2] Ibidem

informatico, questo nuovo spazio virtuale costituito prevalentemente da informazioni, spazio in cui si esplica la personalità del singolo. La necessità di tutelarsi dall'accesso abusivo infatti, implica il riconoscimento dell'esistenza di un nuovo "spazio virtuale" costituito e delimitato non più da elementi di tipo "fisico" quali le mura di un edificio ma da "informazioni".

La libertà informatica, di cui si parlava in precedenza, è quindi strettamente collegata al riconoscimento di un domicilio informatico, intendendo per tale luogo una lettura aggiornata del bene giuridico "domicilio" già costituzionalmente tutelato dall' art. 14 della Costituzione.

Assistiamo quindi ad una evoluzione del tradizionale concetto di domicilio, evoluzione che la giurisprudenza ha pedissequamente accompagnato, arrivando ad inglobare, in questa definizione, oltre alle mura domestiche, anche l'auto, la roulotte, la banca, fino ad arrivare, appunto, alla più recente definizione di domicilio informatico.

Più che di un nuovo bene giuridico si deve quindi parlare di una riformulazione del concetto tradizionale di domicilio che sia idonea a soddisfare le esigenze poste in essere dai luoghi informatici.

L'art. 4 della legge sui reati informatici inserisce, nel codice penale, ben tre nuovi articoli dopo il 615 *bis*, i quali vanno a disciplinare la complessa e dibattuta questione del cosiddetto *domicilio informatico*.[4] Ci soffermiamo con particolare attenzione sul reato di accesso abusivo.

L'art. 615 *ter* c.p., rubricato *"accesso abusivo ad un sistema informatico o telematico"*, punisce chiunque si introduca senza autorizzazione in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantenga contro la volontà esplicita o tacita di chi ha il diritto di escluderlo.

La norma recita testualmente: *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero si mantiene contro la volontà di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni"*.

Ma entriamo nello specifico ad analizzare l'articolo per comprendere come, il comportamento di chi accede ad un sistema sia prodromico rispetto ad altri comportamenti a cui il legislatore ricollega le fattispecie di reato evidenziate dagli art.li successivi, e mi riferisco alla detenzione e diffusione di password, al danneggiamento, alla cancellazione di informazione e dati, ed alla non meno diffusa, ma altrettanto pericolosa condotta di diffusione dei cosiddetti "virus".

---

[3] **Paolo Galdieri** : *Teoria e pratica nell'interpretazione del reato informatico*, Giuffrè, 1997.
[4] **Pica Giorgio** : *Diritto Penale delle tecnologie informatiche*, UTET, 1999.

In pratica cioè, se non accedo ad un sistema (legalmente o illegalmente) non potrò porre in essere altre condotte come quelle previste dalle fattispecie tipiche di cui al 615 *ter* e *quoter*. L'accesso quindi, abusivo o meno, diventa condotta prodromica, in un certo senso, un mezzo per il compimento di successivi reati.

Il comportamento incriminato consiste nell'introdursi abusivamente all'interno di un sistema e nel mantenersi. La prima condotta è evidentemente un antecedente necessario per la seconda. Tuttavia il legislatore ha specificato nella formulazione della fattispecie le due condotte in forma distinta e separata. Questo perché noi potremmo essere autorizzati ad entrare in un sistema, ad esempio per scrivere o leggere alcuni dati, ma potremmo anche, successivamente al compimento dell'attività per la quale siamo stati autorizzati, mantenerci indebitamente all'interno della macchina, del computer e compiere tutta una serie di operazioni per le quali non siamo stati esplicitamente o implicitamente autorizzati.

Questa condotta è facilmente riscontrabile nei luoghi di lavoro dove, l'intervento temporaneo sulla macchina del collega, si rivela uno dei momenti più a rischio per l'integrità del sistema stesso. In molti casi, la curiosità gioca degli scherzi che possono avere delle conseguenze notevolmente dannose, quali l'inopportuna cancellazione di alcuni file o, peggio, il danneggiamento di alcuni comandi fondamentali per il funzionamento del sistema stesso.

Tutto ciò fa parte, ovviamente, di una cultura della sicurezza aziendale che oggi non sussiste all'interno delle nostre imprese, ma che è già in forte crescita al di là dei nostri confini nazionali.

La sicurezza infatti non è solo un problema di prodotto da vendere o da acquistare ma è, innanzitutto, una cultura da acquisire.

La sicurezza richiede progettualità, integrazione con i processi aziendali, consapevolezza, e necessità di una continua verifica a causa del fatto che lo stato dell'evoluzione è esso stesso, per sua natura, in continuo fermento.

La condotta commissiva dell'accesso abusivo è dovuta al fatto che la norma è costruita sul volontario mantenimento dell'accesso nonostante il divieto espresso o tacito del titolare.[5]

La fattispecie penale in questione restringe tuttavia il suo campo di azione ai soli casi di accesso ad un sistema informatico o telematico che sia protetto da "misure di sicurezza".

L'intenzione del legislatore, è quella cioè di punire soltanto ove il titolare del sistema abbia dimostrato, attraverso l'inserimento di una misura di sicurezza, il cosidedetto "*ius excludendi alios*" cioè la volontà di riservare l'accesso solo a persone da lui autorizzate. E' importante

[5] **Pica Giorgio** : *Diritto Penale delle tecnologie informatiche*, UTET, 1999.

sottolineare come non è la qualità dei contenuti che giustifica il diritto alla riservatezza, ma è il fatto che comunque si tratti di contenuti inseriti all'interno di un'area riservata. Altrimenti l'analisi per stabilire se una violazione è meritevole o meno diventerebbe opinabile e non più accertabile secondo precisi criteri di valutazione.

Innanzitutto chiariamo che quando si parla di misure di sicurezza si fa riferimento a diversi tipi di strumenti: possiamo avere delle misure fisiche (come la vigilanza), logiche (password), biometriche (lettura dell'iride o dell'impronta digitale). Su questo punto, quello delle misure di sicurezza vi è tuttavia una importante elemento da sottolineare : la scelta del legislatore di indirizzare la tutela penale solo per i sistemi dotati di misure di protezione. Tale scelta, male viene accolta da chi considera ingiustificata la distinzione dei vari domicili informatici. Si verrebbero cioè a creare sistemi protetti (di serie A) e sistemi non protetti (di serie B).

L'accesso al sistema diventa quindi abusivo ed illegittimo solo in presenza di un *quid pluris* che ci allerta sulla presenza di una *voluntas excludendi* da parte del titolare, una volontà di sbarramento manifestata in modo non equivoco.[6]

Recente giurisprudenza[7], asserisce che qualora il sistema non sia protetto da misure di sicurezza, la condotta normativa non viene in essere poiché il legislatore, con l'introduzione della norma di cui all'art. 615 *ter* ha inteso tutelare non la *privacy* di un qualsiasi "domicilio informatico", ma soltanto quella di sistemi protetti da misure di sicurezza contro il pericolo di accessi da parte di persone non autorizzate.

Considerato quindi che l'esistenza di idonei mezzi efficaci di protezione è elemento costitutivo della fattispecie incriminatrice di cui all'art. 615 ter c.p., stante il principio di tassatività del nostro diritto penale, in carenza di adeguate ed aggiornate misure di sicurezza non avremo il configurarsi del reato.

E' chiaro come questa norma ponga seri problemi alle attività aziendali, statuendo una necessità di continuo e costante aggiornamento della tecnologia e degli strumenti utilizzati.

Questa prima impostazione è stata modificata, e meglio specificata, da una ancora più recente sentenza della Corte di Cassazione.[8] Il supremo collegio ha ritenuto che ciò che sia determinante per la configurazione del reato, non è tanto la presenza di misure di protezione

---

[6] **Pica Giorgio** : *Diritto Penale delle tecnologie informatiche*, UTET, 1999.

[7] **Trib. Pen. di Roma,** Uff. GIP, Sez. 8a, Sent. 21 aprile 2000 n. 6677/99 R.G.G.I.P.

[8] **Corte di Cassazione**, Sez. V Pen., Sent. 7 nov. - 6 dicembre 2000, n. 1675. Vedi anche : **Corte di Cass.**, Sez.VI Pen. Sent. 4 ott. - 14 dic. 1999, n. 3067.

interne o esterne al sistema, quanto l'aver agito contro la volontà contraria di chi dispone legittimamente del sistema.

Ed infatti, un sistema dovrebbe essere giuridicamente tutelato sempre, non soltanto quando il titolare lo ha dotato di misure di sicurezza.

Esistono infatti una serie di informazioni all'interno dei nostri computer che, sebbene prive di adeguate misure di protezione, il titolare può avere interesse a celare ed a mantenere riservate, anche solo per una tutela della propria *privacy*.

L'esistenza quindi di una violazione e di un illecito dovrebbe essere ricondotta principalmente all'elemento soggettivo della fattispecie di reato e cioè l'elemento psicologico di chi agisce. La semplice altruità del sistema, l'appartenenza, in sostanza, della macchina al proprietario, implica la necessità di un suo consenso per qualunque tipo di disposizione e gestione di dati.

Oltretutto, così formulata la legge impone un notevole aggravio di costi per l'attività imprenditoriale in quanto costringe le aziende ad un continuo aggiornamento dei propri sistemi di sicurezza al fine, appunto, di ricadere all'interno della previsione normativa.

Inoltre, tutelare soltanto i sistemi protetti potrebbe essere sintomo di una discriminazione poiché creerebbe una disparità di tutela tra il singolo utente, le piccole aziende e le grandi, poiché ciascuna di queste categorie troverà delle difficoltà diverse, proporzionate al reddito o al fatturato per trovare i mezzi necessari per dotare i propri computer o terminali delle indispensabili misure.

Infine, altro aspetto interessante della norma è il problema relativo alla identificazione del luogo in cui si consuma il reato.

Il problema sorge in relazione all'accesso perpetrato per via telematica, quando cioè tra la postazione di chi compie l'azione ed il luogo in cui si trova il sistema od il terminale su cui si concretizza, siano distanti tra loro ed il collegamento avvenga tramite modem.

Il reato di accesso abusivo deve ritenersi formalmente perpetrato nel luogo in cui si trova il sistema che subisce l'attacco.[9] E' chiaro che questo pone e porrà sempre dei delicati problemi all'esplicarsi ed all'efficacia dell'azione penale.

Da un lato sussiste la difficoltà pratica di risalire in termini probatori all'autore del fatto di reato, in quanto la disponibilità di un *account* non implica necessariamente l'uso in esclusiva dello stesso. In sostanza, l'abbonamento al *provider* stipulato a nome del capo famiglia o del direttore di una azienda, non identifica l'effettivo utilizzatore dello stesso, che di volta in volta potrà essere un familiare o un dipendente; inoltre, altro aspetto non meno rilevante, la postazione da cui agisce il soggetto può appartenere ad uno Stato diverso da quello in cui si

trova il sistema oggetto dell'azione, con comprensibili e rilevanti conseguenze sul piano della attività di ricerca probatoria prima e giurisdizionale poi.

Certo, in questa materia le certezze sono ancora poche ed i dubbi molti, ma è proprio questo, a mio avviso, che ci deve spingere ad un continuo confronto, proprio perché il prossimo futuro vedrà sempre più vicine le figure del legale e dell'esperto di tecnologie informatiche, lasciando a ciascuno il relativo campo di competenza, ma anche creando una nuova ed indispensabile sinergia tra le due figure professionali.

Reggio Calabria, 23.06.2001

[9] **Pica Giorgio** : *Diritto Penale delle tecnologie informatiche*, UTET, 1999.