

## **DETEZIONE E DIFFUSIONE ABUSIVA DI CODICI D'ACCESSO**

L'art. 615-*quater* punisce l'abusiva acquisizione in qualunque modo (anche mediante autonoma elaborazione, come precisa la relazione introduttiva alla legge) e diffusione di "codici di accesso" ai sistemi informatici o telematici protetti da misure di sicurezza, oltre all'indicazioni di qualunque istruzione idonea al predetto scopo.

La norma in questione si pone come naturale completamento della tutela prevista dall'art. 615-*ter*, che punisce ogni accesso abusivo ad un sistema informatico o telematico. Infatti, l'acquisizione o la diffusione dei cc.dd. codici di accesso è preordinata alla commissione di un accesso abusivo.

Nella stessa relazione alla legge si evidenzia che *"la previsione è, per un certo verso, analoga a quella di cui al terzo comma dell'articolo 9 della legge 8 aprile 1974, n. 98"*, relativa alla messa in circolazione di apparecchi o strumenti idonei alla commissione dei delitti previsti dagli artt. 615-*bis* (Interferenze illecite nella vita privata) e 617-*quater* (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche).

Il primo comma statuendo che è punibile chiunque *"abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole*

*chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo"* chiarisce le modalità della condotta e l'oggetto che la norma intende tutelare.

Quanto all'oggetto di tutela, esso è costituito da tutti i mezzi idonei all'accesso ad un sistema informatico o telematico. Come è stato giustamente osservato<sup>1</sup> i mezzi idonei all'accesso, di cui parla la norma, possono distinguersi in tre grandi categorie:

- mezzi di accesso fisici
- mezzi di accesso memorizzati dall'utente legittimo
- sistemi biometrici

I mezzi di accesso della prima categoria posseggono il requisito della fisicità e sono costituiti da chiavi meccaniche o da tesserini magnetizzati di riconoscimento (ad esempio badge, carte di credito, Bancomat ecc.).

Tali mezzi sono consegnati al legittimo utilizzatore dal gestore del sistema e costituiscono, pertanto, una forma di legittimazione e di accesso controllato.

---

<sup>1</sup> Borruso-D'Aiotti AA.VV. *op. cit.*, pag. 78.

Il livello di sicurezza da essi assicurato non è molto elevato poiché possono essere sottratti o ceduti, oltre che facilmente contraffatti e duplicati. Proprio per tale motivo, il più delle volte, la sicurezza viene accresciuta combinandoli ad una sequenza di elementi numerici, alfabetici o simbolici.

Dette sequenze appartengono alla seconda categoria di mezzi di accesso e costituiscono sicuramente il metodo più diffuso per tutelare o limitare l'ingresso ad un sistema. Il *personal identification number* (indicato con l'acronimo P.I.N.) e la password (letteralmente, parola chiave) sono i casi più comuni di sequenze di elementi assegnati dal gestore del sistema in via esclusiva all'utilizzatore.

Il P.I.N., usualmente utilizzato per carte di credito e Bancomat, consiste in una serie di numeri; le password sono, invece, una sequenza alfanumerica (cioè un insieme di lettere o di numeri e lettere).

Sia P.I.N. che password devono essere comunicate, normalmente dopo l'utilizzo dei mezzi di accesso fisici, al sistema informatico o telematico.

Nonostante tali mezzi di difesa siano usati dai circuiti bancari internazionali per rendere possibile il c.d. trasferimento elettronico dei

fondi<sup>2</sup>, non rappresentano l'*optimum* in tema di sicurezza. Infatti, i sistemi più affidabili sono quelli biometrici, che raffrontano alcune caratteristiche fisiche dell'utente con quelle precedentemente memorizzate dal sistema. Attualmente, i sistemi biometrici più diffusi sono quelli relativi alle impronte digitali, al riconoscimento vocale, al reticolo venoso della retina dell'occhio ed al controllo dinamico della firma<sup>3</sup>.

In relazione ai diversi mezzi idonei all'accesso varia il tipo di condotta che la norma ha inteso reprimere.

La nuova figura di reato contempla due differenti ipotesi: la prima relativa alla nozioni di detenzione e diffusione<sup>4</sup>; la seconda alla fornitura a terzi di indicazioni o istruzioni idonee al compimento dello scopo cui mirano le condotte ricomprese nella prima ipotesi.

Più dettagliatamente, la fattispecie di cui alla prima ipotesi può essere realizzata con varie modalità: con il procurarsi, riprodurre, diffondere, comunicare o consegnare codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico.

---

<sup>2</sup> Il *trasferimento elettronico dei fondi*, realizzato dagli istituti di credito secondo procedure uniformi, consente la circolazione del denaro e lo scambio di informazioni, relative alle transazioni commerciali, fra gli istituti stessi.

<sup>3</sup> Borruso-D'Aietti AA.VV. *op. cit.*, pag. 80.

<sup>4</sup> Cfr. Relazioni introduttiva alla legge

Le varie espressioni non sono del tutto equivalenti. Infatti, con i termini diffondere, comunicare o consegnare si fa riferimento a qualsiasi forma di divulgazione dei codici o delle parole chiave, e può riguardare sia l'attività di chi le procuri abusivamente, sia quella del legittimo titolare del codice o della parola chiave che abusivamente le comunichi. È da notare che solo l'operatore del sistema può comunicare abusivamente (ossia fuori dei poteri attribuitigli) detti mezzi di accesso, in quanto la comunicazione presuppone la detenzione degli stessi. In tal ultimo caso il delitto è aggravato ai sensi dell'ultimo comma della norma in questione (che rimanda alla circostanza aggravante di cui al numero 1 del quarto comma dell'art. 617-quater).

Con il termine procurarsi, invece, viene punita l'attività dell'agente, finalizzata all'ottenimento dei mezzi di accesso, che precede cronologicamente quella di diffusione e detenzione: *“tale condotta può concorrere con quella di chi li comunica o li cede (i codici), ma potrebbe essere attuata senza cooperazione di altre condotte criminose.”*<sup>5</sup>

Secondo taluni, *“va notato che nella nozione di «procurarsi» va ricompresa anche la mera detenzione (attività criminosa indicata nella*

---

<sup>5</sup> Borruso-D'Aiotti AA.VV. *op. cit.*, pag. 80.

*rubrica della norma, ma non riprodotta all'interno della disposizione).*"<sup>6</sup>

Tale tesi, però, confligge contro il principio di stretta legalità che delimita la punibilità ai soli fatti sufficientemente descritti dal legislatore all'interno delle condotte tipiche.

Invero, il fatto che il legislatore abbia ommesso di citare all'interno delle condotte punibili quella di detenzione è una scelta ampiamente giustificabile. Infatti, l'illecito in esame è configurato come reato di pericolo in quanto la punibilità non è subordinata alla realizzazione di alcun evento.

Ora è chiaro che le condotte cui alludono i termini "*procura, riproduce, diffonde, comunica o consegna*" rivestono un maggior disvalore, oltre che essere indici di una maggiore pericolosità dell'agente, rispetto alla semplice detenzione; pertanto, ben si può ritenere che non concorrono la meritevolezza e l'opportunità di punire per la mera detenzione di codici di accesso.

La riproduzione, infine, è l'attività consistente nella moltiplicazione, non autorizzata, di un qualsiasi mezzo di accesso.

---

<sup>6</sup> Borruso-D'Aietti AA.VV. *op. cit.*, pag. 80.

Quanto alla seconda ipotesi, contemplata nel primo comma della norma in parola, è da dire che è sanzionabile il comportamento di chi “*fornisce indicazioni o istruzioni idonee al predetto scopo*”.

Il delitto si sostanzia nella fornitura di informazioni tecniche che rendano possibile la ricostruzione del codice di accesso o il superamento delle misure di protezione del sistema informatico o telematico.

La norma, per la configurabilità del delitto in esame, impone che l'agente si prefigga lo scopo di “*procurare a sé o ad altri un profitto o di arrecare ad altri un danno*”, richiedendo con ciò un dolo specifico.

Da ultimo, è da evidenziare che il legislatore ha usato l'avverbio “abusivamente”, in relazione alle modalità della condotta, introducendo una nota di antigiuridicità speciale. “*Si tratta di un richiamo che rimanda a situazioni scriminanti ulteriori rispetto alle cause di giustificazione codificate.*”<sup>7</sup>

---

<sup>7</sup> Antolisei “*Diritto penale, parte speciale, I*” a cura di L. Conti, Milano, 1994, pagg. 202-204.