RATIO QUOTIDIANO
Il commento e la critica delle più importanti notizie del momento

DIRITTO

di GIOVANNI ALIBRANDI

L'accesso abusivo a un sistema informatico o telematico

Anche in presenza di autorizzazione a operare, rimane penalmente rilevante la condotta di chi esorbita dai limiti.

L'evolversi dei sistemi informatici e telematici, se per un verso ha il pregio di semplificare la vita di cittadini e imprese, per altro verso comporta **problemi di sicurezza informatica, telematica** e in materia di **trattamento di dati personali** . Si pensi, per esempio, alla gestione degli archivi informatici aziendali, alla trasmissione telematica di dichiarazioni fiscali e comunicazioni varie all'Amministrazione Finanziaria, alla banca dati da questa utilizzata per la raccolta e l'elaborazione dei dati relativi alla fiscalità dei contribuenti (anagrafe tributaria). Tutti sistemi che contengono dati sensibili e riservati, da proteggere in modo adeguato, disciplinando gli accessi attraverso **specifiche " *autorizzazioni* "**, oppure autorizzandone l'accesso mediante il rilascio di **credenziali** a soggetti individuati e individuabili.

L'**art.615- *ter*c.p.** , peraltro reato presupposto della responsabilità degli enti, punisce con la reclusione fino a 3 anni la condotta di chi abusivamente accede a un sistema informatico o telematico. Se la condotta è posta in essere da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso di potere o violazione dei doveri inerenti alla funzione o al servizio, oppure con abuso della qualità di operatore del sistema, la pena è fino a 5 anni di reclusione.

Nel rilascio delle credenziali di accesso, il titolare del sistema ovviamente deve tener conto dei compiti che il soggetto ricevente è chiamato a svolgere. Qualora l'accesso avvenga per **motivi estranei** allo svolgimento di tali compiti, pur in presenza di abilitazione, scatterà il reato di accesso abusivo.

Al riguardo, le Sezioni Unite della Corte di Cassazione, fin dal 2011, hanno sancito il seguente principio: " *integra il delitto previsto dall'art. 615-ter c.p. la condotta di colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto* ***violando le condizioni ed i limiti*** *risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema* ".

Il principio è ribadito nella sentenza n. 25944/2020 della Suprema Corte, che tratta il caso di un **sottufficiale della Guardia di Finanza** che per reperire informazioni riguardanti un soggetto controparte contrattuale di un proprio familiare, si introduceva abusivamente nel sistema in uso alle forze di polizia in 2 distinte occasioni.

In commento ai contenuti della norma penale, anche sulla base di precedenti giurisprudenziali, la citata sentenza argomenta che ha rilievo penale non solo la condotta di chi utilizza il sistema per **finalità diverse da quelle consentite** (raccolta di dati protetti per finalità estranee alle ragioni di istituto e agli scopi sottostanti alla protezione dell'archivio informatico), ma anche la condotta di **abusiva permanenza** ne sistema contro la volontà di chi ha il diritto di escluderla, soprattutto se la legittimazione all'accesso è utilizzata per finalità diverse da quelle consentite.

A prescindere dal caso del pubblico ufficiale, è opportuno sottolineare che il tema dell'accesso abusivo a sistema informatico o telematico riguarda molto da vicino le imprese che ne sono dotate. In merito, è assolutamente consigliato informare adeguatamente il personale interessato circa la rilevanza penale di talune condotte, a salvaguardia della stessa impresa, sia per il suo futuro, sia per evitare possibili contestazioni di violazione della privacy da parte di terzi.