I LIMITI DELLA PUNIBILITÀ DEL REATO DI ACCESSO ABUSIVO A UN SISTEMA INFORMATICO IN CASO DI "DIVULGAZIONE RESPONSABILE"

Andrea Fux

G.I.P. di Catania, decreto 15 luglio 2019

Con il decreto di archiviazione in oggetto il Giudice per le indagini preliminari presso il Tribunale di Catania ha preso posizione sulla tematica riguardante la cd. divulgazione responsabile.

In fatto, il procedimento traeva origine dalla querela presentata dal legale rappresentante di una società di sviluppo *software* che aveva portato a un'incolpazione per i reati di accesso abusivo a un sistema informatico e diffamazione.

L'indagato, dopo aver ricevuto dettagliate informazioni dall'azienda circa il prodotto offerto e aver effettuato un accesso non consentito al suo sistema informatico, aveva inviato diverse segnalazioni alla società querelante in relazione alla vulnerabilità del sistema; solo un mese dopo, in conseguenza dell'inerzia di quest'ultima, l'*hacker* decideva di rendere noto, con finalità di tutela dei consumatori, la presenza dei suddetti difetti.

Ciò premesso, il G.i.p., richiamando il concetto di divulgazione responsabile e riconoscendo congruo – considerate gravità e complessità della vulnerabilità – il tempo intercorso tra la prima segnalazione e l'atto divulgativo, riteneva non integrato il delitto *ex* art. 615-*ter* c.p. Allo stesso modo decideva per l'insussistenza dell'ulteriore fattispecie di diffamazione per via dell'operatività scriminante del diritto di critica di cui all'art. 51 c.p., tenuto conto del nucleo di veridicità della notizia diffusa.

La cd. *responsible disclosure* (o *vulnerability disclosure*) è uno strumento importante di prevenzione e di contrasto agli attacchi informatici, e, più in generale, di garanzia della sicurezza dei sistemi, soprattutto in considerazione della tendenza degli sviluppatori a tacere su eventuali vulnerabilità o di aver subito attacchi di questo tipo, principalmente per motivi di immagine e reputazione sul mercato. Si tratta, in particolare, di un modello di divulgazione dei problemi di sicurezza che prevede un periodo di tempo prima che queste vengano comunicate, così da consentirne la correzione (elemento questo ritenuto fondamentale nella motivazione del decreto). In ciò la divulgazione responsabile si differenzia dalla cd. *full disclosure*, nella quale la pubblicazione avviene immediatamente dopo la scoperta della vulnerabilità e/o senza darne comunicazione al gestore del servizio, non concedendo quindi al venditore alcuna opportunità di risolvere l'anomalia. Negli ultimi anni si è registrata comunque un'inversione di tendenza, e le aziende hanno cominciato a puntare sugli *hacker* etici (anche detti "*white hats*"), anche commissionando *penetration tests* per colmare eventuali problemi di sicurezza.

Nel merito, la motivazione del decreto non consente di comprendere a pieno come la condotta posteriore di divulgazione responsabile (identificata solo come "prassi consolidata") sia entrata nella struttura del reato, elidendone l'integrazione. Invero, la fattispecie di accesso abusivo di cui all'art. 615-*ter* si punisce chi "abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza": sia il

dolo specifico che la successiva operazione di diffusione cadono quindi fuori dalla fattispecie, che deve ritenersi già perfezionata al momento della violazione del sistema informatico dell'azienda; eventualmente, i citati elementi potrebbero rilevare ai soli fini del riconoscimento dell'attenuante *ex* art. 62, comma 1, n. 1 c.p.

Diversamente concludendo si dovrebbe considerare la violazione come elemento di un'unica condotta volta alla segnalazione della "falla", facoltizzata dall'ordinamento; ma così non può ritenersi: l'incoerenza di una simile ricostruzione risiede nel fatto che l'Italia, come la quasi totalità dei Paesi dell'Unione Europea, non è dotata di un quadro normativo che riconosca e disciplini la divulgazione responsabile (adottato solo da Olanda, Francia e Lituania).