Il Ddl cyber security inasprisce le pene agli hacker, ma è solo un elemento transitorio

Il 25 gennaio, durante la seduta del Consiglio dei Ministri, è stato deliberato il disegno ormai già noto come **Ddl cyber security**, un provvedimento che si propone di fornire linee guida aggiornate utili a contrastare il cybercrimine. Malgrado l'evidente rilevanza di tale iniziativa nel contesto di una società sempre più digitalizzata, emerge fra le righe un'osservazione critica riguardante la sfida delle istituzioni nel promuovere un adeguamento sistemico della cybersicurezza, con lo Stato che piuttosto tende per il **rafforzamento delle pene** contro coloro che vengono colti in flagrante reato.

Il disegno di legge oggetto di discussione in seno al Consiglio dei Ministri ha posto infatti particolare enfasi sull'incremento delle **detenzioni legate ai reati informatici**. L'atto di accesso illecito alle banche dati di aziende o istituzioni potrebbe ora comportare pene che vanno **dai cinque ai dieci anni**, un approccio punitivo che raddoppia la durata delle sanzioni attualmente previste. Coloro che creano o distribuiscono software volti a danneggiare sistemi informatici potrebbero a loro volta essere condannati fino a due anni di reclusione, oltre a essere soggetti a una multa che potrà toccare i 10.329€. L'obiettivo è esplicitamente quello di adottare una strategia di deterrenza che disincentivi i singoli dall'abbracciare la via del cybercrimine e, al contempo, induca i colpevoli a cooperare con le autorità al fine di ottenere fino a due terzi di riduzione della pena. «Tutti questi reati rientrano nella disciplina dei reati di criminalità organizzata», ha fatto notare il **sottosegretario Alfredo Mantovano**, Autorità delegata per la sicurezza, «quindi permettono non soltanto l'utilizzo di strumenti più efficaci di indagine e di accertamento, ma anche quel coordinamento che passa attraverso le direzioni distrettuali antimafia e la procura nazionale antimafia».

L'evoluzione delineata appare sotto molti aspetti più securitaria che rivoluzionaria; tuttavia, il disegno di Ddl cyber security affronta approfonditamente anche un aspetto di rilevanza straordinaria, ossia le numerose lacune informatiche presenti attualmente all'interno della **Pubblica Amministrazione** (PA). Dopo un periodo di anni in cui si è economizzato su fondi e risorse destinate alle strategie di cybersicurezza, dopo una lunga serie di importanti violazioni agli archivi di informazioni pubblici, vengono finalmente affrontate le carenze della PA e le istituzioni saranno costrette ad adeguarsi a molti degli obblighi già imposti alle imprese. In particolare, le istituzioni dovranno **notificare tempestivamente qualsiasi attacco** subito dai loro server all'Agenzia per la Cybersicurezza Nazionale (ACN) e dovranno farlo entro 24 ore dalla scoperta del perpetrato reato. La mancata segnalazione comporterà un richiamo, il quale, in caso di recidiva nell'omissione, potrà tradursi in sanzioni pecuniarie comprese tra i 25.000€ e i 125.000€.

Ai Comuni con una popolazione superiore a 100.000 abitanti, alle Aziende Sanitarie Locali (ASL), ai capoluoghi di Regione e alle aziende di trasporto pubblico locale viene inoltre

richiesto di **istituire un ufficio dedicato alla cybersicurezza**. Questa evoluzione sarà parzialmente tutelata dal meccanismo di "raffreddamento" delle carriere degli esperti del settore. Secondo l'articolo 16 del disegno di legge, i dipendenti "che abbiano partecipato, nell'interesse e a spese dell'Agenzia, a specifici percorsi formativi di specializzazione" non potranno trasferirsi al settore privato per un periodo di due anni dalla conclusione del corso. L'idea è quella di prevenire una "fuga di cervelli" assicurandosi che i costi di formazione sostenuti dalle entità pubbliche non finiscano semplicemente a beneficiare il più attrattivo settore aziendale.

In generale, le norme attualmente in discussione sembrano rappresentare più che altro una **fase transitoria** volta a colmare le lacune di un sistema giuridico che, da un lato, si trova in difficoltà nell'affrontare il complesso panorama della criminalità digitale e, dall'altro, è costretto ad attendere l'elaborazione da parte dell'Unione Europea di una serie di pacchetti normativi destinati a impattare significativamente sull'industria tecnologica, soprattutto in relazione al campo delle intelligenze artificiali.

[di Walter Ferri]