CORRIERE DELLA SERA – 17 DICEMBRE 2024

Cybercrime, la difesa è la formazione

di Gerardo Villanacci

Le cronache e le inchieste di questi ultimi tempi sui crimini informatici confermano l'umana e irrefrenabile tendenza a sbirciare nelle vite degli altri.
Curiosità che accresce notevolmente se gli ascoltati sono conosciuti oppure vi è un interesse a conoscere le lore cose. Le conversazioni carpite in treno, ovviamente non nelle costose carrozze silenziose, oppure nei locali pubblici come nelle file di attesa, hanno non poco contribuito al successo letterario del genere «guardare - ascoltare di nascosto».
Già a partire dai primi anni dell'Ottocento, grandi autori come Honoré de Balzac (Papà Goriot), Emile Zola (Pot-Bouille) avevano colto il diffuso interesse indagatore. Un'attenzione che nel tempo non ha mai perso attualità come comprovano anche opere più recenti da quella di Carlo Emilio Gadda (Quer pasticciaccio brutto de Via Merulana) oppure Yasmina Reza (Il Dio del massacro) fino a Muriel Barbery (L'eleganza del riccio).
Si può ben comprendere, quindi, che ci troviamo di fronte ad una sorta di retaggio culturale che è difficile, per non dire impossibile, debellare. Non di meno siamo ormai giunti nella fase in cui il fenomeno, evoluto in problema, è diventato insostenibile.
Non c'è dubbio che lo sviluppo delle tecnologie informatiche abbia non poco contribuito positivamente ai cambiamenti in tutti i settori della nostra vita, fornendo nuove ed importanti opportunità sul piano lavorativo ma anche sociale ed economico. Ma è parimenti evidente che l'altro lato della medaglia è rappresentato da una nuova criminalità il cui contrasto effettivo richiede una alta competenza tecnologica.
Piaccia o meno tutti sono esposti al rischio del cybercrime, dal cittadino che naviga su internet alle grandi multinazionali il cui funzionamento è in larga parte dovuto all'utilizzo di sistemi informatici.
Purtroppo, c'è da aggiungere che il nostro Paese si posiziona nei primi posti, dopo Stati Uniti, Giappone e India, tra quelli che subiscono il maggiore numero di attacchi e, in una posizione ancora più avanzata, per quanto concerne l'incremento degli stessi.
Senza dubbio la crisi sanitaria e quella economica, conseguente al Covid 19, ha notevolmente contribuito all'incremento della problematica determinando la decuplicazione dei reati (65% in più tra il 2022 e il 2023) rispetto alla media mondiale (12% in più).

Tra le varie cause il ritardo legislativo ha avuto un peso considerevole e, per altri versi, esprime la sottovalutazione di un pericolo che si insinua negli interstizi delle fragilità delle persone, dalla pedopornografia, al cyberbullismo, e di quelle della rete e dei dati.
È anche vero che a livello europeo la legislazione dei reati informatici è risalente all'ormai lontano settembre del 1989 quando il Consiglio d'Europa emanò la «raccomandazione sulla criminalità informatica» alla quale in larga misura si è ispirata la prima normativa italiana in materia, nel dicembre del 1993 con la modifica di alcune norme dei codici penali e di procedura penale relative alla criminalità informatica. In ultimo lo scorso 17 luglio è entrato in vigore il disegno di legge volto a rafforzare le emergenze cibernetiche per la pubblica amministrazione, le imprese e i cittadini.
Tuttavia è un dato accertato che la promulgazione di nuove e più severe regole non ha ridotto i crimini informatici che anzi ad oggi risultano aumentati e rappresentano un vero business.
Certo, è illusorio pensare di poter completamente azzerare il pericolo di attacchi, così come prevenire le attività illecite di dipendenti infedeli, ma una strada possibile che merita di essere seriamente percorsa è quella della formazione delle persone.
Una formazione che deve essere adeguata e corrispondente a quella degli hacker, pronta a controbattere le novità del rischio cyber e che consenta di riconoscere tempestivamente le insidie degli spioni soprattutto nei settori più esposti tra i quali la sanità e la finanza.