CYBERSECURITY E 231: IL RACCORDO TRA EVENTI E NORME

Ranieri Razzante, Docente di Legislazione Antiriciclaggio nell'Università di Bologna

Nell'analisi del tema, ampiamente dibattuto e innovativo, della cd. «*cybersecurity*», ci si trova difronte ad un *mare magnum* di interpretazioni e definizioni, soprattutto di *species* del *genus*, per cui risulta assai difficile fornire un inquadramento sistematico delle stesse. Se a ciò si aggiunge un quadro internazionale di regole ancora in via di definizione e, vieppiù, di uniformazione, si rischia di non occuparsi adeguatamente di una delle minacce più attuali e invasive agli ordinamenti economici e informatici degli Stati avanzati. Crimini che non conoscono confini perimetrabili, data la vastità incommensurabile del *web*, per definizione lo spazio territoriale più aperto ad oggi rilevabile «in natura». Le imprese italiane sono risultate, da recenti studi e da rilevazioni sul campo, assai indietro nella gestione dei rischi *cyber*. Ciò a motivo del fatto, soprattutto, che non si è compreso adeguatamente che detti rischi non sono confinabili all'area IT e, specie in quelle di grandi dimensioni, essi sono assolutamente trasversali a tutti i comparti e settori dove ci si serva di strutture informatiche per lo svolgimento degli affari. Si è rimasti legati, in seconda battuta, alla mera definizione, nei MOG, dei reati informatici di cui al nostro codice penale, senza adeguatamente considerare le varie declinazioni che essi oggi possono assumere, e che non sono completamente comprimibili e mitigabili, come rischi, con le tradizionali misure previste nei protocolli *privacy* e Gdpr.

Premessa

Con il d.l. 14 giugno 2021, n. 82, convertito in l. 4 agosto 2021, n. 10, si è data attuazione alle «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale».

Il tutto, a sua volta, in esecuzione di delega del d.lgs. 18 giugno 2018, 65, che aveva recepito la Direttiva UE 2016/1148, 6 luglio 2016, cd. «NIS» (*Network and Information Security*), ove erano stati disegnati quadro e strumenti per le difese nazionali delle infrastrutture critiche e informatiche dei Paesi europei.

Le disposizioni italiane contengono una serie di novità di non poco momento per l'ordinamento giuridico del nostro Paese.

Innanzitutto, la delimitazione degli oggetti di tutela: reti, sistemi informativi, servizi informatici, comunicazioni elettroniche, al fine di assicurarne – recita l'art. 1 – «la disponibilità, la confidenzialità, l'integrità, la resilienza».

Beni comuni, tra pubblico e privato, in una concettualizzazione chiarificatrice che il decreto fa delle minacce e degli strumenti di contrasto. Una considerazione innovativa dell'attacco non convenzionale, fino ad oggi affidata solo agli esperti delle