Privacy

Il cybersecurity act: i vantaggi del nuovo regolamento europeo di certificazione della cyber-sicurezza per le tecnologie dell'informazione e della comunicazione

di **Marta Cogode, Martina Petrucci**

Il pervasivo utilizzo delle tecnologie digitali offre a cittadini, istituzioni e imprese, nuove opportunità di connessione, favorendo la diffusione delle informazioni e lo sviluppo di nuovi modelli di business. Tutto ciò è certo come lo è la conseguente esposizione a pesanti rischi. I così detti "*cyber* criminali", come noto, tentano quotidianamente di sottrarre dati e compromettere il funzionamento dei sistemi transnazionali di comunicazione che, essendo altamente connessi, risultano particolarmente vulnerabili. L'attenzione nei confronti della *cybersecurity*[1] è cresciuta perché correlata alla prosperità e alla sicurezza di cittadini e imprese.

Si pensi che solo nel 2016, all'interno dell'Unione Europea, sono stati registrati più di 4000 attacchi *ransomware*[2] al giorno e l'80%[3] delle imprese ha subito almeno un incidente di *cybersecurity*. Negli ultimi quattro anni l'impatto economico della *cyber* criminalità è quintuplicato[4].

Il *Cybersecurity Act*, Regolamento UE 2019/881 (in seguito anche "*Regolamento*"), in vigore dallo scorso 27 giugno 2019, ha lo scopo precipuo di creare un quadro unico per l'introduzione di un sistema europeo di certificazione per la sicurezza informatica dei prodotti e dei servizi digitali. Essendo un regolamento, una volta entrato in vigore, diviene immediatamente applicabile in tutti gli Stati membri, fatte salve alcune limitate disposizioni, ad esempio quelle in materia di sanzioni.

Il Regolamento, al fine di rafforzarne le funzioni, ha affidato un mandato permanente all'Agenzia dell'UE per la *cybersecurity*[5] (in seguito, "*ENISA*" o "Agenzia"), da un lato, ridefinendo i poteri alla stessa attribuiti, dall'altro, razionalizzandone gli aspetti organizzativi.

Rinviando alle norme di riferimento per un più opportuno approfondimento, ci pare in questa sede sufficiente far notare come l'ENISA sarà la protagonista indiscussa nel contrasto alle *cyber*-minacce, qualificandosi quale centro d'informazione, di sensibilizzazione e di consulenza per istituzioni, organi dell'Unione e Stati membri sulle esigenze e le priorità in materia di ricerca nel campo della cyber-sicurezza, godendo anche di poteri di analisi, raccolta e condivisione delle *best practices* per la *cybersecurity*.

Con il Regolamento è istituito il quadro europeo di certificazione della cyber-sicurezza,

finalizzato ad aumentare la resilienza agli attacchi *cyber* di prodotti, servizi e processi TIC commercializzati all'interno dell'Unione, rendendo possibile, attraverso un processo di armonizzazione in questo senso, la creazione di un mercato unico digitale. Come disposto dal Considerando 70, infatti, "*il quadro europeo di certificazione dovrebbe essere istituito in modo uniforme in tutti gli Stati membri, in modo da evitare la scelta della certificazione più vantaggiosa in base ai diversi livelli di rigore nei vari Stati membri*". La *ratio* sottesa è semplice: molti degli schemi di certificazione esistenti, che non sono di certo una novità, spesso non trovano reciproco riconoscimento tra i diversi Stati membri, obbligando le imprese a ottenere plurime certificazioni per operare a livello transnazionale. Viceversa, i certificati europei di cyber-sicurezza, essendo documenti rilasciati secondo le regole dettate dal Regolamento, attestano che un determinato prodotto, servizio o processo TIC è stato oggetto di una valutazione di conformità secondo i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione, ricevendo, quindi, automatico riconoscimento in tutti gli Stati membri.

Si badi che il Regolamento non istituisce schemi di certificazione immediatamente operativi quanto, piuttosto, traccia le regole da seguire per l'elaborazione degli stessi. In particolare, sarà l'ENISA, sulla base del programma di lavoro progressivo dell'Unione per la certificazione europea redatto dalla Commissione o a seguito di una proposta specifica proveniente da quest'ultima, a preparare, istituendo un gruppo di lavoro *ad hoc*, una proposta di sistema che soddisfi i requisiti di cui agli articoli 51, 52 e 54 del Regolamento. Con il *Cybersecurity Act* è istituito anche il gruppo europeo per la certificazione della cyber-sicurezza (ECCG), che ha lo specifico compito, tra gli altri, di adottare pareri sulle proposte di sistemi preparate dall'ENISA. La Commissione, sulla base della proposta dell'ENISA, potrà adottare, poi, atti di esecuzione.

I sistemi europei di certificazione della cyber-sicurezza possono specificare per i prodotti, i servizi e i processi TIC un livello di affidabilità ("di base", "sostanziale" o "elevato"), commisurato al livello del rischio associato al previsto uso del prodotto, in termini di probabilità e impatto di un incidente. Per i prodotti, servizi e processi TIC che, secondo il sistema europeo di certificazione, presentano un livello di affidabilità di base è consentita un'autovalutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore degli stessi, il quale rilascia, a sua discrezione, una dichiarazione UE di conformità all'autorità nazionale di certificazione della cyber-sicurezza, con la quale afferma che è stato dimostrato il rispetto dei requisiti previsti nel sistema. Per i prodotti che presentano un livello di affidabilità sostanziale o elevato, invece, una volta adottato uno schema europeo di certificazione da parte della Commissione, coloro che sono interessati, e dunque volontariamente e non obbligatoriamente, potranno presentare domanda di certificazione dei propri prodotti o servizi a specifici organismi accreditati.

Con la nuova normativa i sistemi nazionali di certificazione della cyber-sicurezza coperti da un sistema europeo cesseranno di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato; quelli non coperti, invece, resteranno in vigore.

Appare evidente che sono plurimi i vantaggi derivanti dalla normativa in commento. Da un lato, le imprese saranno fortemente agevolate nella commercializzazione transfrontaliera dei

propri prodotti, stimolando, con ciò, una positiva concorrenza tra fornitori a livello europeo, che porterà alla commercializzazione di beni e servizi migliori e a un migliore rapporto qualità-prezzo.[6]; dall'altro, sarà possibile per i consumatori finali comprendere meglio le caratteristiche di sicurezza del prodotto o del servizio acquistato.

In particolare, a trarne vantaggio saranno le PMI e le *start-up,* che, solitamente, incontrano non poche difficoltà a stabilizzarsi sul mercato. In altre parole, il *Cybersecurity Act* contribuirà a ridurre gli ostacoli all'accesso sul mercato per le PMI e per le nuove imprese, rendendo loro possibile concorrere a livello europeo.

[1]La *cybersecurity* è definita all'art. 2 del Regolamento UE 2019/881 come *l'insieme* delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche.

[2] Un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione. Ad esempio alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

[3]Si veda. http://www.confindustria.eu/documentDownload?id=10050&ext=pdf&name=Lente+sull%27UE+n.+58+-+Cyber+security.

[4]Si veda http://www.confindustria.eu/documentDownload?id=10050&ext=pdf&name=Lente+sull%27UE+n.+58+-+Cyber+security.

[5]Cfr. art. 1, *Cyber securtiy Act*.

[6]Cfr. http://europa.eu/rapid/press-release_QANDA-19-3369_it.htm.