L’Unione europea sotto (cyber)attacco: strategie e prospettive in tema di ciberresilienza e cibersicurezza

written by Francesco Gatta

“L’Europa deve guidare la transizione verso un nuovo mondo digitale”, così si esprimeva Ursula von Der Leyen nella propria agenda politica per il quinquennio di Commissione 2019-2024. Tre anni più tardi, a metà del proprio mandato, e in occasione del discorso sullo stato sull’Unione del 2022, la Commissione ha annunciato una proposta di regolamento in tema di c.d. ciberresilienza. La proposta individua una serie di misure volte a proteggere i consumatori e le imprese mediante l’introduzione di requisiti obbligatori in materia di cibersicurezza per i prodotti hardware e software con elementi digitali. L’iniziativa della Commissione arriva in un contesto delicato e problematico, in cui gli attacchi cibernetici (c.d. *cyber-attacks*) si moltiplicano, mettendo a repentaglio la sicurezza dei governi e dei cittadini.

Il contesto: tra attacchi ibridi ed attacchi cibernetici

Le misure proposte dalla Commissione, facenti parte di una più ampia strategia dell’Unione per la cibersicurezza, giungono in un contesto storico-politico in cui l’Unione europea è sotto costante minaccia di subire attacchi cibernetici. In effetti, diverse minacce hanno colpito in vario modo la regione europea, sotto forma di incursioni nei sistemi informatici, interferenze, fake news, furto di dati, e via dicendo: veri e propri attacchi, idonei a destabilizzare il funzionamento degli apparati informatici statali e ad incidere sulla fornitura di servizi essenziali per i cittadini.

Un caso emblematico è quello dell’Ucraina. Il conflitto provocato dalla Russia è iniziato ben prima del 24 febbraio 2022: l’invasione militare, infatti, è stata preceduta da una strategia mirata e ben pianificata di attacchi in forma cibernetica, con interferenze su larga scala, con le quali abili hacker russi hanno penetrato e paralizzato le infrastrutture informatiche ucraine (servizi bancari e

finanziari, amministrazioni pubbliche, siti governativi, in particolare di difesa e *intelligence*, e financo quello del parlamento, come riportano alcuni media). Si è trattato, insomma, di un disegno preciso, premeditato e ben calcolato, antecedente e strumentale al vero e proprio attacco armato della Russia ai danni dell'Ucraina (sul ricorso agli attacchi informatici da parte della Russia nel contesto del diritto internazionale si veda Stiano).

Ancora, alle porte dell'Ue, attacchi cibernetici hanno recentemente colpito un altro Paese candidato all'adesione: a luglio, e poi ancora a settembre, l'Albania ha subito massicce infiltrazioni nei propri sistemi informatici della polizia e delle forze dell'ordine, questa volta ad opera di hacker operanti dall'Iran. Il governo di Tirana ha reagito interrompendo con effetto immediato le relazioni diplomatiche con l'Iran, intimando a tutto il personale diplomatico iraniano di lasciare il territorio albanese entro 24 ore. È il primo caso mai registrato in cui si verifica una simile reazione da parte di uno Stato di fronte a un attacco cibernetico. In questo senso, il Premier albanese, Edi Rama, ha affermato che l'attacco subito dal proprio Paese "*was not an individual operation or a concerted action by independent criminal groups, but a State-sponsored aggression*". L'Unione europea ha preso le difese dell'Albania, condannando l'accaduto nelle parole della dichiarazione resa l'8 settembre dall'Alto Rappresentante Joseph Borrell.

Attacchi cibernetici e interferenze nei sistemi informatici si verificano, poi, anche presso i confini degli Stati membri, dove le frontiere esterne dell'Unione sono sottoposte a continui rischi per la sicurezza. Lo certifica l'Agenzia Frontex che, nell'analisi strategica dei rischi per il 2022 (*Strategic Risk Analysis 2022*), dà conto di crescenti minacce ibride, sempre più frequenti e sofisticate, che prendono la forma di "*cyber-attacks against border infrastructure, artificial creation of migratory routes or weapons smuggling for terrorist purposes*". La recente "guerra ibrida" lanciata dalla Bielorussia contro le frontiere dei Paesi membri dell'Ue ad essa confinanti (su cui si veda il contributo di Di Pascale) rappresenta un ulteriore esempio di impiego di "armi cibernetiche".

Infine, nemmeno a Strasburgo, nel cuore dell'Europa, è possibile dirsi sicuri, come dimostra l'attacco cibernetico diretto contro la Corte europea dei diritti dell'uomo a fine 2020. Il 22 e 23 dicembre, infatti, il sito web della Corte era stato vittima di un attacco che lo aveva reso inaccessibile ed inutilizzabile. La Corte aveva quindi rilasciato una dichiarazionein cui condannava severamente il "*large-scale cyberattack*" nei suoi confronti. Collegava, inoltre, tale "*serious incident*" alla

pronuncia, il 22 dicembre 2020, della sentenza nel caso *Selahattin Demirtas c. Turchia (No. 2),* in cui la Grande Camera aveva riscontrato numerose violazioni della CEDU in riferimento all'arresto e alla detenzione del leader turco del Partito dei Lavoratori del Kurdistan (PKK) in base ad accuse di terrorismo (per un commento si veda qui e qui; la sentenza, inoltre, è stata anche oggetto di una risoluzione del Parlamento europeo). Sebbene nello stesso giorno fossero state emesse anche una serie di decisioni nei confronti della Russia (*Usmanov c. Russia*; *Plokhovy c. Russia*; *Panovy c. Russia*), pochi giorni più tardi, in effetti, l'attacco cibernetico era stato rivendicato da un collettivo di hacker turchi,proprio in ragione della sentenza resa dalla Corte nel caso *Demirtaş*.

La vicenda è grave in quanto segna il primo attacco cibernetico perpetrato nei confronti un'istituzione europea: un precedente pericoloso ed inquietante, che dimostra come anche le strutture informatiche di un'organizzazione internazionale come il Consiglio d'Europa non possano ormai considerarsi immuni a tali moderne minacce. Sebbene l'attacco, di per sé, non sembra aver determinato significative conseguenze, l'impatto resta serio da un punto di vista simbolico: attaccare l'istituzione più rappresentativa nella tutela dei diritti umani in Europa convoglia un chiaro messaggio di minaccia per i valori e i principi comuni all'esperienza di integrazione europea.

La strategia digitale e la nuova proposta sulla ciberresilienza: contenuti e prospettive

È nel descritto contesto di minaccia che si inserisce la proposta della Commissione per una nuova normativa in tema di ciberresilienza, intesa quale misura per incrementare la cibersicurezza europea. Si tratta di un tema, a ben vedere, che è ormai presente da tempo tra gli obiettivi dell'agenda politica dell'Ue. Limitandosi al periodo più recente, si può ricordare come già sotto la Commissione Barroso II, nel 2013, era stata presentata una Strategia dell'Unione europea per la cibersicurezza, la quale, tra l'altro, menzionava la ciberresilienza quale mezzo per proteggere il corretto funzionamento del mercato interno e rafforzare la sicurezza interna dell'Ue. In seguito, anche la Commissione a guida Juncker aveva insistito sul tema, con una serie di proposte, tra cui quella per l'istituzione di un'agenzia europea per la cibersicurezza. Con il passaggio di testimone all'attuale Commissione, il tema digitale e della cibersicurezza è divenuto ancor più prioritario. Lo testimonia, ad esempio, l'istituzione di uno specifico portafoglio per "un'Europa pronta per l'era digitale", attribuito dalla Presidente Von der Leyen alla danese Margrethe

Vestager, Vice-Presidente Esecutivo della Commissione europea.

Su queste basi, nel dicembre 2020 la Commissione aveva presentato la Strategia dell'Ue per la cibersicurezza, con l'obiettivo di garantire che, in Europa, chiunque possa "condurre una vita digitale in sicurezza" grazie a strumenti di connettività sicuri ed affidabili. La strategia configurava un ventaglio di misure relative a una varietà di settori, tra cui quello della resilienza di beni e servizi digitali. A marzo 2021, quindi, il Consiglio aveva adottato le conclusioni sulla strategia in materia di cibersicurezza, sottolineandone l'importanza per creare "un'Europa resiliente, verde e digitale". Infine, in occasione del discorso sullo stato dell'Unione del 2021, la Presidente Von der Leyen aveva preannunciato la proposta per un nuovo regolamento sulla ciberresilienza, concepito come componente essenziale della politica europea di ciberdifesa.

All'esito di questo percorso, la proposta di regolamento presentata dalla Commissione il 15 settembre 2022 si pone essenzialmente due obiettivi di fondo. Da un lato, mira a ridurre la vulnerabilità nei prodotti digitali, introducendo requisiti comuni di cibersicurezza in riferimento alla produzione e allo sviluppo dei c.d. prodotti intelligenti e connessi. Dall'altro, intende operare sul profilo della trasparenza e dell'informazione verso i consumatori, rendendoli più consapevoli e tutelati nell'acquisto di un prodotto avente determinate caratteristiche di cibersicurezza e capacità di risposta verso attacchi cibernetici. A questo fine, dal primo punto di vista e dal lato del produttore, il regolamento intende introdurre una serie di specifici requisiti obbligatori (c.d. *cybersecurity requirements*, dettagliati in un allegato alla proposta di regolamento), il cui rispetto è condizione necessaria per l'introduzione del prodotto nel mercato. Quanto al secondo profilo, relativo al consumatore, si prevede la fornitura di servizi di informazione ed assistenza, nonché regolari aggiornamenti dell'apparecchio acquistato per migliorarne il grado di cibersicurezza.

Gli obblighi così configurati interessano i vari operatori coinvolti lungo le diverse tappe del ciclo economico del prodotto digitale: dagli sviluppatori ai produttori, fino al distributore. Solo una volta accertata correttamente la sussistenza dei prescritti requisiti, il prodotto potrà ottenere una dichiarazione di conformità europea ed essere finalmente immesso nel mercato. La proposta prevede anche una serie di conseguenze negative in caso di inottemperanza con i requisiti di ciberresilienza, tra cui sanzioni economiche e il ritiro del prodotto dal mercato.

In definitiva, la normativa sulla ciberresilienza viene presentata dalla Commissione come una misura in grado di produrre diversi vantaggi: per le stesse aziende, che saranno in grado di fornire prodotti più sicuri ed affidabili, così evitando anche danni reputazionali legati a uno scarso livello di sicurezza; per i consumatori, che beneficeranno di prodotti più sicuri, nonché di una maggior consapevolezza in tema di cibersicurezza; per l'Ue nel suo complesso, e per il suo mercato, che sarà maggiormente protetto. La proposta, infine, si spinge oltre, affermando che essa ha "*the potential to become an international point of reference*" e che gli standard europei di ciberresilienza potrebbero giocare un ruolo determinante, venendo "esportati" in modo tale da influenzare "*the cybersecurity industry in global markets*".

La parola ora passa al legislatore europeo. La proposta, se approvata, rappresenterebbe, in effetti, la prima normativa di questo tipo a livello dell'Unione. Solo il tempo ci dirà se essa vedrà la luce e sarà in grado di determinare l' "effetto Bruxelles" anche nel settore della cibersicurezza mondiale.