Cibersicurezza:

La strategia dell'Unione europea

Audizione presso la Commissione I "Bilancio, Affari generali ed istituzionali"

Sessione europea 2023

29 marzo 2023

Giovanni Zaccaroni (Università di Milano-Bicocca)

Indice

1. Strategia UE per la cibersicurezza
2. Dichiarazione Europea sui diritti e principi del digitale
3. Quadro giuridico in vigore (1) *ENISA* (2019)
4. Quadro giuridico in vigore (2) *Direttiva NIS 2*
5. Quadro giuridico in vigore (3) *Direttiva sulla resilienza dei soggetti critici*
6. Proposte legislative in corso
7. Accademia per le competenze in materia di cibersicurezza (punto 38)
8. Skills sulla cibersicurezza

Strategia UE per la cibersicurezza

La Comunicazione congiunta su La strategia dell'UE in materia di cibersicurezza per il decennio digitale,(2020) pone 5 obiettivi:

1. Promuore un'infrastruttura resiliente e servizi critici: aumentare il livello di **ciberresilienza** di tutti i settori pertinenti, pubblici e privati, che svolgono una funzione importante per l'economia e la società

2. Creare un **ciberscudo europeo**: una rete di centri operativi per la sicurezza all'interno dell'UE e stanziare oltre 300 milioni di EUR a sostegno della cooperazione pubblico-privata e transfrontaliera al fine di creare reti nazionali e settoriali

3. Rendere sicura la prossima generazione di reti mobili a banda larga

4. Rendere più sicuro sia il web che l'IoT (Internet of Things)

5. **Aumentare le competenze in materia di cibersicurezza** della forza lavoro

Dichiarazione europea sui diritti e i principi digitali per il decennio digitale

Dichiarazione europea sui diritti e principi digitali per il decennio digitale

Che valore ha?

Meramente programmatico (*soft law*) → come il Pilastro Europeo dei Diritti Sociali

Tuttavia, molti di questi diritti e principi sono in realtà già parte della giurisprudenza della Corte di Giustizia UE e dalle Costituzioni degli Stati UE.

Punto 16, Dichiarazione su diritti e principi digitali

La Dichiarazione contiene un passaggio rilevante per questa analisi, al punto 16.

Un ambiente digitale sicuro, protetto e tutelato

16. Ogni persona dovrebbe avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione, traducendosi in un elevato livello di riservatezza, integrità, disponibilità e autenticità delle informazioni trattate.

Punto 16, Dichiarazione su diritti e principi digitali

Ci impegniamo a: […]

b) proteggere gli interessi delle persone, delle imprese e delle istituzioni pubbliche dai rischi di cibersicurezza e dalla criminalità informatica, anche per quanto riguarda le violazioni dei dati e i furti o le manipolazioni dell'identità, il che comprende requisiti di cibersicurezza per i prodotti connessi immessi sul mercato unico;

c) contrastare coloro che cercano di compromettere, all'interno dell'UE, la sicurezza online e l'integrità dell'ambiente digitale o che promuovono la violenza e l'odio attraverso strumenti digitali, e chiamarli a rispondere delle loro azioni.

Quadro giuridico in vigore (1)

Regolamento (UE) 2019/881 del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, («regolamento sulla cibersicurezza»)

- Estende il mandato a tempo indeterminato e aumenta i poteri dell'agenzia della cibersicurezza
- Introduce una certificazione europea in materia di cibersicurezza, di cui ENISA è responsabile
- Consolida il ruolo di ENISA come punto di riferimento per l'adozione di linee guida e buone pratiche in materia di cibersicurezza (ENISA avrà un ruolo nell'adozione dell'atto sull'accademia in materia di cibersicurezza)

Quadro giuridico in vigore (2)

Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, (Direttiva NIS 2)

Recepimento: entro 27 ottobre 2024

Mira a mitigare le minacce ai sistemi informatici e di rete utilizzati per fornire servizi definiti come “essenziali” ed “important” in settori chiave e a garantire la continuità di tali servizi.

Introduce, per esempio, un sistema di notifica alle autorità competenti di qualunque «incidente significativo» che avvenga ai fornitori di tali servizi.

Quadro giuridico in vigore (3)

Direttiva (UE) 2022/2557 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa alla resilienza dei soggetti critici

Recepimento: entro 17 ottobre 2024

Ha uno scopo più specifico della precedente, e cioè aumentare il livello di sicurezza per i soggetti «critici», che «svolgono un ruolo indispensabile per il mantenimento di funzioni vitali della società o di attività economiche»

Proposte legislative in corso

Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014 COM(2020) 595 final (c.d. regolamento DORA – Digital Operational Resiliency Act)

Il compromesso c.d. politico (post triloghi) è già stato approvato ma deve ancora essere pubblicata in Gazzetta Ufficiale per problemi relativi alla traduzione.

Proposte legislative in corso

Punto 39 dell'allegato II del Programma di Lavoro della Commissione Europea → Proposte Prioritarie

Proposta di Regolamento del Parlamento Europeo e Del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali [Cyber resilience act] con 2 obiettivi:

- Sviluppo di "prodotti sicuri con elementi digitali" garantendo che i prodotti hardware e software siano immessi sul mercato con minori vulnerabilità e garantire che i fabbricanti prendano sul serio la sicurezza durante l'intero ciclo di vita di un prodotto

- Tenere conto della cibersicurezza nella selezione e nell'utilizzo di "prodotti con elementi digitali".

Proposte legislative in corso (2)

Obiettivi più specifici del Cybersecurity Resilience Act:

1. garantire che i fabbricanti migliorino la sicurezza dei prodotti con elementi digitali dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita;
2. garantire un quadro coerente in materia di cibersicurezza, facilitando la conformità per i produttori di hardware e software;
3. migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali, e
4. consentire alle imprese e ai consumatori di utilizzare prodotti con elementi digitali in modo sicuro.

Accademia per le competenze in materia di cibersicurezza

Punto 38 del Programma di lavoro della Commissione europea:

Fondazione dell' "Accademia per le competenze in materia di cibersicurezza"

- Iniziativa di carattere non legislativo (regolamento di esecuzione adottato dalla Commissione)
- Prevista per: 3° trimestre 2023 (entro la fine dell'anno)
- Sviluppa le competenze in materia di cibersicurezza già individuate da ENISA

Skills sulla Cibersicurezza (ENISA)

The European Cybersecurity Skills Framework (ECSF) is a practical tool to support the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals.

The ECSF summarises all cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies. It provides a common understanding of the relevant roles, competencies, skills and knowledge required, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programmes.

12 figure professionali

Fonte: sito web ENISA

Conclusioni

- Il quadro giuridico è molto recente.
- Due direttive molto importanti dovranno essere recepite entro ottobre 2024: quale ruolo per le Regioni?
- L'iniziativa che riguarda l'Accademia delle competenze in materia di cibersicurezza sarà pubblicata nella seconda metà del 2023, ma non è chiaro ancora quale atto sceglierà la Commissione (è necessario attendere la pubblicazione del testo).
- La tecnologia si muove molto più velocemente del regolatore: il tempo è il fattore fondamentale.

Legislazione citata

Comunicazione Congiunta al Parlamento Europeo e al Consiglio, La strategia dell'UE in materia di cibersicurezza per il decennio digitale JOIN(2020) 18 final, 16.12.2020

Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01)

Regolamento (UE) 2019/881 del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, («regolamento sulla cibersicurezza»)

Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

Direttiva (UE) 2022/2557 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio

Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali [Cyber Resilience Act]

GRAZIE!

Giovanni Zaccaroni

Ricercatore in Diritto dell'Unione europea
Università di Milano-Bicocca
Dipartimento di Giurisprudenza

per ogni evenienza

giovanni.zaccaroni@unimib.it