Image

Articolo Divulgativo

IL DDL SULLA CYBERSICUREZZA E GLI SVILUPPI EUROPEI IN TEMA CYBERSECURITY

Per affrontare le crescenti minacce cibernetiche e garantire un livello elevato di sicurezza informatica, l'Unione Europea ha agito attraverso direttive e regolamenti. La Direttiva NIS (Network and Information Security), il Regolamento Generale sulla Protezione dei Dati (GDPR) o il nuovo Cyber Resilince Act, rappresentano importanti disposizioni che impongono agli Stati membri e alle organizzazioni private e pubbliche obblighi in termini di prevenzione, gestione e reazione agli incidenti di sicurezza informatica. L'obiettivo della ricerca consiste nell'esaminare gli strumenti normativi principali, verificare la loro influenza nella sicurezza delle reti e dei sistemi informativi e comprendere le sfide associate alla loro esecuzione in un contesto di rapidi progressi tecnologici.

di **Federica Mercurio**
IUS/14 - DIRITTO DELL'UNIONE EUROPEA
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Martedì 2 Luglio 2024

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

To address growing cyber threats and ensure a high level of cybersecurity, the European Union has acted through directives and regulations. The NIS (Network and Information Security) Directive, the General Data Protection Regulation (GDPR) or the new Cyber Resilience Act, represent important provisions that impose obligations on Member States and private and public organizations in terms of prevention, management and reaction to cybersecurity incidents. The objective of the research is to examine the main regulatory tools, verify their influence in the security of networks and information systems and understand the challenges associated with their implementation in a context of rapid technological advances.

Sommario: 1. Il DDL sulla cybersicurezza in Italia; 2. Gli sviluppi europei sulla cybersecurity; 3. Conclusioni.

1. Il DDL sulla cybersicurezza in Italia

La legislazione italiana sulla cybersicurezza è in continua evoluzione per rispondere alle crescenti minacce cibernetiche e conformarsi ai regolamenti dell'Unione Europea. Un esempio importante in tal senso, è dato dal recente disegno di legge (DDL) sulla cybersicurezza, il quale rappresenta un passo significativo verso il rafforzamento delle misure di sicurezza informatica in Italia. Il 16 febbraio del 2024 è stato presentato alla Camera dei deputati il nuovo DDL sulla cyber sicurezza, attualmente in fase di analisi dal parlamento. Lo scopo di quest'ultimo è quello di incrementare la normativa relativa alla Cyber sicurezza nazionale e anche rafforzare la tutela in materia di reati informatici[1].

Gli obiettivi per tale intervento sono molteplici, difatti vi è la volontà di incrementare e modernizzare le disposizioni attualmente vigenti sulla sicurezza digitale e soprattutto, costruire le fondamenta solide di una struttura interna che possa rappresentare le esigenze attuali e future in tema di Security nazionale. Inoltre, vi saranno una serie di azioni, tali da legittimare in modo tempestivo le capacità di risposta della ACN, Agenzia Nazionale per la Cybersicurezza, che gestirà le politiche di sicurezza informatica, il monitoraggio delle minacce cibernetiche e la risposta agli incidenti di sicurezza, garantendo anche il coinvolgendo con le altre autorità nazionali. In modo da garantire una rapida risposta e mitigazione delle minacce, il DDL impone alle aziende operanti nei settori critici l'obbligo di segnalare gli incidenti di sicurezza informatica. Proprio per questo sono state previste una serie di modifiche al Codice penale, al fine di ampliare il regime sanzionatorio previsto per i reati informatici. Infatti, l'articolo 11 del DDL, rubricato: modifiche al Codice penale, reca una serie di disposizioni volte sia a segnalare che a bloccare la

CamminoDiritto.it
ISSN 2421-7123

commissione di reati informatici. Queste modifiche sono essenziali per adeguare il sistema giuridico alle nuove sfide che derivano dall'uso crescente delle tecnologie digitali

I cambiamenti posti alla base della normativa già vigente mirano ad un innalzamento delle pene edittali, rispetto alla loro attuale formulazione, includendo anche altre circostanze aggravanti, individuando le circostanze attenuanti nei casi di lieve entità e instituendo un'estensione del dolo specifico per determinate fattispecie criminose[2]. L'architettura della sicurezza cibernetica in Italia e le relazioni tra gli attori del sistema sono state profondamente modificate dal DDL in oggetto. La possibilità per i rappresentanti della Banca d'Italia e della Direzione nazionale antimafia e antiterrorismo di partecipare alle riunioni del Nucleo per la cybersicurezza su questioni specifiche è tra le principali disposizioni.

Il DDL ha aggiunto nuovi reati riguardanti gli attacchi informatici alle infrastrutture critiche. Nello specifico, in riferimento ai servizi essenziali come l'energia, l'acqua e i trasporti, i quali sono considerati essenziali per la sicurezza nazionale e il benessere generale. Inoltre, è previsto che per garantire una risposta più rapida ed efficace agli incidenti di sicurezza informatica, le imprese, le istituzioni pubbliche e le autorità competenti, come la Polizia Postale e delle Comunicazioni, lavoreranno insieme.

Nel caso in cui i servizi di sicurezza della Repubblica lo informino, il Presidente del Consiglio potrà anche posticipare le responsabilità informative e le azioni dell'Agenzia per la cybersicurezza nazionale, ma solo se ritenuto strettamente necessario. In aggiunta, è stata disposta l'estensione della speciale disciplina delle intercettazioni per la criminalità organizzata ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo. Le aziende sono tenute a segnalare gli incidenti alle autorità competenti in modo rapido. L'inasprimento delle pene, l'inserimento di nuovi reati specifici e il rafforzamento delle misure preventive e di collaborazione con le autorità dimostrano l'impegno del legislatore italiano nel combattere in modo efficace le minacce cibernetiche[3].

La stipula del DDL in oggetto non è stata solo spinta da evidenti motivi pratici[4], cioè per esigenze di risposta ad un fenomeno sempre più crescente nel nostro territorio, ma soprattutto per motivi di armonizzazione rispetto ad un sistema sovranazionale, che già da tempo si è mosso a prevenzione e tutela di attacchi informatici. A tal proposito l'Italia, già due anni fa, con il decreto legislativo del 3 agosto 2022 n. 123, recepì il regolamento europeo 2019/881, relativo all'ENISA, di cui si parlerà in seguito e alla certificazione sulla cybersicurezza per le tecnologie dell'informazione e della comunicazione, che abrogava il precedente regolamento 526/2013 (regolamento sulla cybersicurezza).

CamminoDiritto.it
ISSN 2421-7123

Di conseguenza, con il presente DDL, l'ordinamento italiano tende ancor più ad allacciarsi ad un progetto europeo, che con il Cyber Resilince Act[5], rappresenterà la conclusione di un piano coeso verso il sostegno reciproco contro gli abusi informatici. Lo scopo del presente DDL è certamente quello di prevenire la commissione di reati informatici, agendo a monte sulla protezione dei sistemi nazionali e sulla prevenzione contro gli accessi illeciti sulle piattaforme informatiche. In linea con le direttive e i regolamenti dell'Unione, il disegno di legge sulla cybersicurezza in Italia rappresenta un passo significativo verso il miglioramento della sicurezza informatica del paese.

La legislazione italiana è stata fortemente influenzata dalla legislazione europea, che ha spinto verso un approccio più coordinato e integrato alla lotta alle minacce cibernetiche. A tal proposito, l'Italia si prepara a proteggere meglio le sue infrastrutture e i dati personali dei suoi cittadini in un panorama digitale in continua evoluzione adottando misure più rigorose e creando nuove strutture dedicate alla cybersicurezza.

2. Gli sviluppi europei sulla cybersecurity

La cybersicurezza e la digitalizzazione rappresentano due facce di una stessa medaglia, queste furono le parole utilizzate dalla Presidente della Commissione Europea Ursula von der Leyen nel suo discorso annuale del 2019[6]. Difatti, si reputa che lo stretto rapporto tra digitalizzazione e sicurezza rappresenti il frutto di un ineluttabile sviluppo ed implementazione di queste stesse tecnologie. Questo riferimento è cardinale per comprendere il motivo per cui l'Unione ha lavorato tanto, negli ultimi decenni, in tema di cybersicurezza e di protezione dei dati.

Dietro questo assunto ci sono due principali riflessioni, vi è l'implicita accettazione di quanto possa essere oscuro e quindi non sicuro, il mondo digitale, ed in secondo luogo, vi è l'assunto che, fortunatamente, la sicurezza informatica si sia ormai normalizzata nella politica digitale dell'UE[7].

La normativa europea sulla cybersicurezza ha portato a un ambiente digitale più sicuro e resiliente, imponendo standard rigorosi e incentivando la collaborazione tra gli Stati membri. Nello specifico, il Cyber Resilince Act, già citato in precedenza, ha già avuto l'approvazione del Parlamento europeo nel marzo 2024 e mira a stabilire una maggior protezione delle imprese e dei consumatori che si interfacciano, ormai quotidianamente, con prodotti e servizi informatici, incidendo non solo sulla sicurezza globale degli stessi prodotti e merci immessi nell'Unione ma anche sul mercato dei software in generale. Questo atto rappresenta uno degli ultimi, ma non il solo, strumento disposto dall'Unione, che insieme a tanti altri quali GDPR, regolamento UE 2016/679, in merito alla protezione dei dati personali o la direttiva NIS2, a cui dopo vi faremo un breve cenno, o anche il

CamminoDiritto.it
ISSN 2421-7123

Medical Device Regulation, regolamento 745 del 2017, mirano a completare e integrare, nei vari settori di riferimento, la disciplina in materia di sicurezza informatica[8].

Per comprendere la portata degli interventi europei in materia di cybersicurezza, è opportuno fare riferimento al nuovo cybersecurity act, regolamento UE 2019/881[9]. Difatti, attraverso quest'ultimo, l'Unione ha incrementato i compiti della agenzia UE per la sicurezza informatica, adottando un quadro di certificazione di servizi e di prodotti che possa stabilire delle regole uniformi e attribuendo più forza all'ENISA.

Il piano di certificazione rappresenta uno degli strumenti adottati dall'Unione, volti a far sì che le imprese possano ottenere una certificazione dei prodotti, servizi e TIC (tecnologia dell'informazione della comunicazione), una sola volta, in modo che, quella stessa attestazione conforme, venga identificata e accettata da parte dell'Unione[10]. Infatti, questo piano rappresenterà una nuova svolta nell'ambito della circolazione dei prodotti nell'UE, sia in termini di affidamento, rispetto alla divulgazione dei servizi, che sono essenziali per il mondo digitale, sia in termini di sicurezza degli stessi[11]. Inoltre, il generale piano di certificazione fornisce un sistema di attestazione a livello dell'UE attraverso l'affermazione di regole complete, requisiti tecnici, standard e procedure[12].

Al fine di chiarire le novità del presente atto è necessario citare brevemente il ruolo dell'ENISA. L'agenzia nazionale sulla cybersicurezza informatica ENISA venne stipulata nel 2004 e le sue attuali funzioni sono state stabilizzate e potenziate dal regolamento UE 2019/881 sulla sicurezza informatica[13]. Il suo ruolo è contribuire nella definizione delle politiche europee sulla sicurezza informatica, perfezionando l'attendibilità dei prodotti, dei servizi e dei processi TIC, attraverso appositi programmi di certificazione. Grazie alla diffusione delle conoscenze, l'agenzia collabora con gli Stati membri, per instituire un canale di collegamento, specialmente nei settori economici, basato sulla fiducia reciproca e sull'utilizzo di sistemi che siano veramente garanti della protezione e della sicurezza digitale per i cittadini europei. Inoltre, è disposto che l'ENISA partecipi con la ECCG durante i suoi lavori, quale gruppo europeo di certificazione della cybersicurezza, e si occupi di assolvere al ruolo di segretariato del gruppo dei portatori di interessi per la certificazione della cybersicurezza SCCG[14]. Il gruppo europeo di certificazione della sicurezza informatica (ECCG) è stato istituito per contribuire a garantire l'attuazione e l'applicazione coerenti della legge sulla sicurezza informatica. È composto da rappresentanti delle autorità nazionali di certificazione della cibersicurezza o da rappresentanti di altre autorità nazionali competenti. L'ECCG è determinante per la preparazione dello schema di certificazione candidato e per l'implementazione generale del quadro di certificazione. Il compito affidato all'agenzia, nell'assolvimento del ruolo di segretariato in risposta agli incidenti sulla sicurezza informatica (CSIRT), fu stabilito già nel 2016, grazie alla direttiva 2016/1148 NIS[15].

CamminoDiritto.it
ISSN 2421-7123

Le disposizioni in materia di sicurezza informatica risalenti al 2016, definito appunto dalla direttiva NIS, sono state così aggiornate e riformate dalla direttiva NIS2 del 2022[11]. Anche in questo caso si assiste ad un processo di sviluppo rispetto alla normativa passata in materia di sicurezza informatica, estendendo le previgenti regole a nuovi settori e ambiti, al fine di rendere più competenti e pronte le autorità addette nell'Unione Europea.

La direttiva NIS2 contempla una serie di azioni che possono essere adottate dagli Stati membri al fine di tutelare la sicurezza, in tutto il territorio dell'Unione Europea. Ad esempio, una delle attività previste corrisponde nella creazione di gruppi, composti dagli stessi Stati membri, che possa non solo incidere e migliorare lo scambio comunicativo tra di essi ma anche rendere più semplice la loro collaborazione nella definizione delle varie strategie di intervento[16]. Inoltre, viene chiesto a tutti gli Stati membri di informarsi e di adeguarsi rispetto alle nuove politiche e strumenti di sicurezza informatica anche attraverso l'utilizzo di nuovi strumenti, quali ad esempio un computer security incident response team o anche un'autorità che sia competente nella gestione della rete, dei servizi di informazione e dei rischi di cybersicurezza[17].

In vista dei crescenti episodi che hanno non da poco colpito le strutture importanti dell'ordinamento a tutela di interessi pubblici fondamentali, quali ad esempio la sanità pubblica, l'economia, il sistema di trasporti e delle banche, lo scopo finale è quello di favorire la crescita di una cultura informatica che possa coinvolgere tutti gli Stati membri dell'unione e fornire dei servizi che siano forti e qualitativamente idonei a gestire e prevenire eventuali attacchi informatici[18].

3. Conclusioni

Alla luce di quanto fin qui esposto, è possibile trarre l'attualità e necessità dell'argomento trattato. Sono svariati i tentativi determinati dagli stati e dall'Unione Europea, adottati per tutelare i cittadini dai possibili risvolti negativi, che il mondo dell'informatica possa comportare. Il fine di questa ricerca è mettere in luce i nuovi mezzi messi a disposizione dell'UE, per combattere i crimini informatici e per tutelare i cittadini. La Direttiva NIS e il GDPR sono esempi significativi di come l'UE stia affrontando i problemi di sicurezza e protezione dei dati informatici.

Tuttavia, a causa delle continue minacce cibernetiche, le normative esistenti dovranno comunque essere costantemente aggiornate e rafforzate. Per affrontare le sfide future, è fondamentale che ci sia una cooperazione internazionale, l'adozione di nuove tecnologie di sicurezza e soprattutto educare gli utenti.

CamminoDiritto.it
ISSN 2421-7123

Per concludere, l'Unione Europea deve continuare a vigilare costantemente e ad adottare nuove strategie per proteggere efficacemente i suoi cittadini, nonostante ad oggi la cybersicurezza in Europa abbia stabilito basi solide.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] Senato della repubblica e Camera dei deputati, dossier XIX esima Legislatura, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, A.C. n. 1717 1, Progetti di legge n. 266.

[2] Ibidem, Articolo 11, Modifiche al Codice penale, pp.34-64.

[3] Camera dei deputati, XIX legislatura, PROVVEDIMENTO: Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, 19 Giugno 2024

[4] Difatti, si è assistito nel 2023, ad incremento dei reati informatici pari circa al 7% rispetto all'anno 2022, così come dimostrano i risultati apportati dalla polizia postale italiana, sono stati infatti rilevati i seguenti dati: 9.433 reati informatici commessi nel 2023 contro la persona: stalking, diffamazione, minacce, revenge porn, molestie, trattamento illecito dei dati e linguaggio d'odio i più diffusi. Ministero dell'Interno, Piazza del Viminale, Il report 2023 dell'attività della Polizia Postale nel contrasto ai crimini informatici, 2 gennaio 2024.

[5] European Parliament legislative resolution of 12 March 2024 on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)

[6] T. Liebetrau, "Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice", Introduction, JCMS 2024 Volume 62. Number 3. pp. 705–724.

[7] Ibidem.

[8] C. Telmon, "Cyber Resilience Act, il Parlamento UE approva: perimetro di applicabilità e impatti", Cybersecurity Nazionale, Network-digital-360, 12 marzo 2024.

[9] Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio 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, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»

[10] European Union, European Union. cybersecurity-act , 18 aprile 2023, inoltre si veda Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 al punto 66, 70 e il Titolo III, Quadro di certificazione della cibersicurezza.

[11]European Union, cybersecurity-certification-framework, The EU cybersecurity certification framework, 7 febbraio 2024.

[12] Ibidem.

[13] European Union Agency for Cybersecurity, Informazioni sull'Agenzia dell'Unione europea per la cibersicurezza (ENISA), Verso un'Europa affidabile e sicura dal punto di vista informatico, per ulteriori approfondimenti si veda Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019, al punto 48, 53, 59.

[14] nello specifico, l'SCCG ha il compito di consigliare la Commissione e l'ENISA su questioni strategiche riguardanti la certificazione della cibersicurezza e di assistere la Commissione nella preparazione del programma di lavoro aperto dell'Unione.

[15] European Union, {https/URL}(UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[16] 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).

CamminoDiritto.it
ISSN 2421-7123

[17] Ibidem, Capo III Cooperazione a Livello dell'Unione e Internazionale, articolo 14, Gruppo di cooperazione.

[18] Ibidem, si veda ad esempio l'articolo 21, Misure di gestione dei rischi di cibersicurezza.

[19] European Union, .eu/policies/nis2-directive.

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=10607