DOI: 10.26314/GARR-Conf23-proceedings 14

Cyber Resilience Act and Open Source: problemi aperti e prospettive future

Nadina Foggetti

Consiglio Nazionale delle Ricerche IBIOM - Bari

Abstract. L'Unione Europea ha recentemente innovato la normativa in materia di cyber security, introducendo diverse norme volte a definire un nuovo quadro giuridico di riferimento per gli Stati membri dell'UE in questo settore. In particolare il Regolamento Il Cyber Resilience Act (RCA) si inserisce nel contesto della trasformazione digitale avviata dall'Europa e da attuarsi entro il 2030, ponendosi in maniera complementare al Regolamento 2019/881 relativo all'ENISA, attraverso il quale è stato introdotto nell'ordinamento comunitario un quadro comune di certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione ("TIC"). Obiettivo principale del Regolamento è quello di definire degli standard comuni di sicurezza informatica per i prodotti digitali connessi in rete (cd. "IoT") e per i relativi servizi al fine di proteggere i consumatori e il mercato dagli incidenti informatici, salvaguardando le imprese e gli utenti che acquistano o utilizzano prodotti, o software, con componenti digitali. All'interno dell'ambito di applicazione della nuova normativa rientrano anche i prodotti e alle tecnologie open source soprattutto all'interno di Servizi ICT a supporto delle infrastrutture di ricerca. In questo lavoro si analizzeranno le principali novità introdotte della nuova disciplina europea ed il loro impatto con lo tutela dei principi fondamentali, quali la libera circolazione nel mercato dei prodotti digitali, i principi dell'open Science e dell'Open Source

1. Il nuovo quadro giuridico di riferimento

All'interno della legislazione europea nel contesto della cyber security, nel 2013 è entrata in vigore la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, che armonizza la criminalizzazione e le sanzioni per i reati contro i sistemi di informazione. In seguito è stata adottata la direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS), primo strumento legislativo europeo sulla cibersicurezza. La proposta di Regolamento relativo ai requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, il Cyber Resilience Act (CRA), e che si inserisce nel contesto della trasformazione digitale avviata dall'Europa ha permesso la definizione, nell'ordinamento europeo, di un quadro comune di certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione ("TIC"). La nuova disciplina mira a garantire il miglioramento della sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita, mediante la definizione di un quadro coerente in materia di cibersicurezza che faciliti la compliance per i produttori di hardware e software. Pone, inoltre, le basi per migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali e consentire alle imprese e ai consumatori di utilizzarli in modo sicuro.

Al fine di raggiungere questi obiettivi la nuova disciplina impone degli obblighi per le a-

Conferenza GARR 2023 - Saperi interconnessi - Selected Papers
Firenze, 14-16 giugno 2023 - ISBN: 978-88-946629-2-4 - Creative Commons CC-BY

ziende che producono strumenti digitali, o che li acquisiscono mediante supply chain.

2. Ambito di applicazione della disciplina

In merito all'applicazione ratione materie, il Considerando 11 del CRA stabilisce che lo stesso "non dovrebbe disciplinare il software libero e open source sviluppato o fornito al di fuori di un'attività commerciale". Nell'ambito del software Open Source (OSS), spesso l'accesso al servizio di assistenza, la fornitura di una piattaforma software o l'uso di dati personali contenuti in database è regolato dal pagamento di un prezzo.

Sotto il profilo dell'applicazione ratione personae, il Regolamento stabilisce che può essere considerato "Fabbricante" qualsiasi persona fisica o giuridica che sviluppi o faccia progettare prodotti e li commercializzi con il proprio nome o marchio, a titolo oneroso o gratuito. A questa particolare categoria sono attribuiti obblighi quali la redazione di una valutazione dei rischi di cybersecurity, nonché l'impegno a gestire le vulnerabilità e ad adottare le misure di sicurezza correttive (ivi compreso l'eventuale ritiro del prodotto dal mercato) e l'onere di procedere all'informazione e alla comunicazione all'autorità competente. Similari oneri ricadono, ai sensi del CRA sui distributori di prodotti digitali. Rientra in questa categoria qualsiasi persona fisica o giuridica nella catena di approvvigionamento, diversa dal fabbricante o dall'importatore, che mette a disposizione un prodotto con elementi digitali sul mercato dell'Unione senza modificarne le proprietà. In particolare i distributori sono tenuti ad uno specifico obbligo di verifica rispetto alla presenza del marchio UE sulla cyber security.

L'articolo 3 comma 18, inoltre, prevede l'applicazione degli obblighi a coloro che producono software a titolo gratuito e l'articolo 16 del Regolamento, rubricato "Altri casi in cui si applicano gli obblighi dei fabbricanti", ne estende la portata a qualsiasi persona fisica o giuridica che apporta una sostanziale modifica al prodotto con elementi digitali. In questa prospettiva qualsiasi programmatore, che contribuisce allo sviluppo di un software il cui uso è regolato da licenze libere diventa, giuridicamente, un produttore.

Inoltre, tra gli obblighi dei fabbricanti, vi è quello di segnalare al soggetto che si occupa della manutenzione, una vulnerabilità anche quando si tratta di un componente OS integrato nel prodotto con elementi digitali.

Sulla base di quanto emerge dobbiamo concludere che la disciplina trovi applicazione anche nei confronti del software e della tecnologia OS.

Se si amplia lo studio del legal framework alla proposta di direttiva sulla responsabilità per danno da prodotti difettosi (2022/0302(COD), è possibile notare che l'articolo 4 stabilisce che per "prodotto" si intende anche il software; e che "fabbricante" identifica chi sviluppa, produce o fabbrica un prodotto per uso proprio, allineando di fatto l'ambito di applicazione a quello definito nel CRA.

La questione non è meramente tuzioristica, poiché influisce in modo significativo, non solo sugli obblighi del produttore (sviluppatore), ma anche sulle eventuali responsabilità in cui potrebbe incorrere in caso di mancata compliance con i requisiti prescritti.

3. L'applicazione alla tecnologia open source del CRA

Un primo aspetto rilevante, in termini di ricadute sull'OSS è quello che attiene alla di-

stinzione, operata all'interno del Regolamento, tra software finito e software non ancora rilasciato (versione beta). Il considerando 21 del Regolamento, stabilisce che è possibile condividere la versione beta a condizione che sia messa a disposizione solo per il tempo necessario a testarla e a raccogliere riscontri. In questa ipotesi, i fabbricanti dovrebbero provvedere affinché il software messo a disposizione a tali condizioni sia rilasciato solo a seguito di una valutazione dei rischi e sia conforme ai requisiti di sicurezza relativi alle proprietà dei prodotti con elementi digitali imposti dal CRA.
Una delle caratteristiche dell'OSS è l'innovazione, che si concretizza nella possibilità di garantire una grande flessibilità e libertà nel poter cambiare elementi senza eccessiva restrizione.
In ambiente OSS è difficile distinguere tra versioni Beta e versioni definitive, proprio perché il software è in continua evoluzione ed in continuo cambiamento, per questo è qualificazione dello status dello stesso, ai fini dell'applicazione delle norme in materia di cybersecurity, è particolarmente complessa. Partendo dall'assunto che l'OSS è, altresì in continua evoluzione, il rispetto degli obblighi di documentazione, diverrebbe particolarmente oneroso, anche nella prospettiva del continuo aggiornamento della stessa rispetto alle diverse versioni.
Una caratteristica che contraddistingue l'OSS è la continua produzione di lavoro creativo sui software stessi, operato dalla community di sviluppatori. Questo rende particolarmente difficile tenere traccia degli apporti creativi e pone l'annoso problema, più volte discusso della dottrina, della disciplina giuridica da applicare alle parti aggiunte in seguito al primo sviluppo del software. Si discute se debba essere qualificato come opera collaborativa, creata da più autori, oppure se il software sviluppato di volta in volta rappresenti un'opera derivata da quella originale. Quando si opera in un contesto transnazionale, quale è quello della ricerca scientifica e tecnologica, occorre tenere conto delle differenze che ci sono tra gli ordinamenti giuridici che compongono il legal framwork di riferimento. In particolare, all'interno dei sistemi di common law, l'OSS si qualifica come opere derivata, mentre negli ordinamenti di civil law, si parla di elaborazioni creative. La distinzione è necessaria ai fini dell'attribuzione dei diritti morali d'autore sull'opera, ma anche per individuare la titolarità degli obblighi previsti dal Regolamento.
Inoltre, l'applicazione di obblighi e responsabilità nei confronti dello sviluppatore del software è in grado di determinare un conflitto con le disposizioni contrattuali inserite all'interno della licenza d'uso dell'OSS.
Queste ultime contengono espressi esoneri di responsabilità, in ragione del fatto che gli sviluppatori non percepiscono un compenso per il lavoro di sviluppo. Questa disposizione contrattuale, non esclude in nessun caso la responsabilità per dolo o colpa grave, ma potrebbe non comprende quella per prodotti difettosi come richiesto dalla nuova disciplina in corso di approvazione.
L'applicazione del nuovo quadro giuridico europeo in materia di cyber security avrebbe, sulla base di quanto evidenziato, un impatto significativo sull'ecosistema open source. I soggetti destinatari degli obblighi e delle relative sanzioni previste dal CRA comprendono a pieno titolo gli sviluppatori di software open source, sebbene l'attività svolta dagli stessi sia a titolo gratuito. L'applicazione delle norme in parola è in grado di ridurre

in modo determinante il numero dei potenziali sviluppatori di software OS, in ragione delle importanti sanzioni eventualmente applicabili in caso di violazione. La circostanza, infatti, che gli sviluppatori contribuiscano con il proprio codice, permette l'inserimento degli stessi tra le categorie a cui la nuova disciplina europea attribuisce obblighi specifici e responsabilità.

La produzione di software OS potrebbe subire una significativa riduzione, in ragione degli eccessivi costi di compliance che risulterebbero essere gravosi e demotivanti per i singoli sviluppatori che intendono contribuire a progetti OS.

In secondo luogo vi sarebbe una limitazione alla circolazione del software open source a livello internazionale, dato il legal gap definito dalla differenza di regime giuridico tra le parti di codice che sono sviluppate ed utilizzate all'interno dell'UE e quelle sviluppate al di fuori dello spazio giuridico europeo. Questo gap potrà avere delle ricadute negative sulle dinamiche di interazione tra sviluppatori provenienti da diversi Paesi.

A fronte di queste criticità di impatto della normativa, le principali associazioni di software libero sono intervenute con una lettera aperta rivolta alle istituzioni dell'Unione Europea al fine di poter contribuire al dialogo teso all'elaborazione del testo definitivo del CRA. L'obiettivo è quello di garantire che le caratteristiche uniche del software open source siano considerate a livello normativo e che il Cyber Resilience Act non danneggi involontariamente l'ecosistema open source. Nella lettera si auspica l'apertura di un canale di dialogo, durante il processo di colegislazione, al fine di assicurare che qualsiasi evoluzione dettata dal CRA, tenga conto della diversità delle pratiche di sviluppo di software open source, aperte e trasparenti, e che lo stesso divenga un meccanismo istituzionale di collaborazione fra le istituzioni europee e la community open-source, per garantire che le future decisioni legislative e politiche siano fondate su informazioni corrette. (https://elettronica-plus.it/lettera-aperta-per-il-cyber-resilience-act_128149/)

Bibliografia

Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013 , relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, GU L 218 del 14.8.2013, pag. 8

Direttiva (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

GU L 194 del 19.7.2016, pag. 1.

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), GU L 333, del 27.12.2022, pag. 80.

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"), GU L 151 del

7.6.2019, pag. 15.
Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, COM/2022/454 final, disponibile alla seguente URL: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52022PC0454#footnote4 (ultima consultazione 25 settembre 2023).
Proposta di direttiva on liability for defective products, Procedure 2022/0302/COD, disponibile alla seguente URL: https://eur-lex.europa.eu/procedure/EN/2022_302 (ultima consultazione 25 settembre 2023).

Dell'aversana F., Quale copyright per il mondo del file sharing? Il caso dei social network, in Informatica e diritto, XLIII annata, Vol. XXVI, 2017, n. 1-2, pp. 519-538.

Heim T N, Wessel R A, The Global Regulation of Cybersecurity: A Fragmentation of Actors, Definitions and Norms, in Lucía Millán Moro and Gloria Fer- nández Arribas (eds.), Ciberataques y Ciberseguridad en la Escena Internacional, 2020.

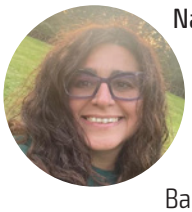
Kasper A, Antonov A, Towards Con- ceptualizing EU Cybersecurity Law, ZEI, 2019.

Markopoulou D, Papakon- stantinou V, De Hert P, "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", Computer Law and Security Review, Vol. 35 Issue 6, Novem- ber 2019.

McGowan D., Legal Implications of Open-Source Software, Symposium: Intellectual Property Challenges in the Next Century, in University of Illinois Law Review, Vol. 2001, pp. 241-304.

Papakonstantinou V., Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?, in Computer Law & Security Review Volume 44, 2022, p. 44 ss.

Biografia



Nadina Foggetti

Tecnologo CNR – IBIOM Bari, già Assegnista di ricerca Senior INFN Bari. Laurea in Giurisprudenza, Master in diritto comunitario e transnazionale -UniTN, Corso avanzato in Data Protection e Data Governance presso e in Coding per Avvocati e Legal Tech -Unimi. Dottore di ricerca in diritto internazionale e dell'Unione europea presso l'Università degli studi di Bari A. Moro. Avvocato e mediatore. Membro SIDI. dal 2005 collabora ad importanti progetti di ricerca nazionali e internazionali nei settori del cybercrime, cybersecurity, data privacy, diritto informatico e cloud computing. Docente di diritto internazionale e diritto della cybersecurity Corso di Laurea in Scienze della Mediazione Linguistica. Autore di diverse pubblicazioni nel settore. Attualmente collabora al progetto ELIXIRxNextGenIT sui temi dell'Open Science, Fair, Open Access.