RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0146 • articolo sottoposto a peer review • pubblicato in anteprima il 17 mag. 2024

FEDERICA CASAROSA

L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2

L'Autrice è tecnologa di ricerca presso la Scuola Universitaria Superiore Sant'Anna e professore presso l'Istituto Universitario Europeo

La ricerca è stata svolta nell'ambito del Progetto PNRR "*SoBigData.it: Strengthening the Italian RI for Social Mining and Big Data Analytics* (CUP B53C22001760006), finanziato dall'Unione europea - Next Generation EU

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

1. Cybersecurity per la pubblica amministrazione

La sicurezza informatica è stata oggetto dell'attenzione del legislatore italiano sin dai primi anni del 2000, riconoscendo la necessità di un intervento di protezione delle infrastrutture e dei cittadini, ancor prima della c.d. *wake up call* operata a livello europeo dal caso *Wannacry*. Sin dai primi interventi, fra cui il d.lgs. 7 marzo 2005, n. 82 sul codice dell'amministrazione digitale, il legislatore ha mostrato come uno dei primi obiettivi da raggiungere sia l'adeguamento del quadro normativo per il settore pubblico. Anche il DDL Cybersicurezza si pone in questa prospettiva andando a definire strumenti e regole finalizzati a proteggere i soggetti della Pubblica amministrazione che, secondo la recente relazione dell'Agenzia per la Cybersicurezza Nazionale (ACN), sono appunto quelli che hanno subito nel corso del 2023 il numero maggiore di attacchi informatici.

Peraltro, il DDL Cybersicurezza si trova ad intervenire in un momento di transizione, in cui il quadro normativo delineato dal d.lgs. 18 maggio 2018, n. 65, che ha implementato la normativa europea di armonizzazione sulla sicurezza delle reti e dei sistemi informativi (Direttiva n. 2016/1148, c.d. Direttiva NIS) deve essere aggiornato alle nuove regole previste dalla Direttiva 2022/2055, c.d. Direttiva NIS 2. La proposta oggetto dell'analisi, quindi, potrebbe rappresentare un intervento che anticipa alcuni aspetti che saranno poi oggetto della normativa di implementazione della Direttiva NIS 2 e consentire alla Pubblica amministrazione di modificare e adattare le proprie strutture organizzative in tempi adeguati rispetto ai procedimenti interni. Al momento, tuttavia, alcune delle norme previste nella proposta di legge non adottano questa prospettiva, e piuttosto individuano modifiche organizzative che, nel breve periodo, potrebbero a loro volta essere oggetto di ulteriore revisione per allinearsi con le norme previste dalla Direttiva NIS 2.

Uno degli elementi di frizione, su cui si concentra il presente contributo, è relativo agli obblighi di notifica previsti per le Pubbliche amministrazioni in caso di incidente informatico, delineati nell'articolo 1 del DDL Cybersicurezza.

2. Il ruolo degli obblighi informativi nell'attuale quadro normativo

Uno dei pilastri della normativa sulla sicurezza informatica, delineato nella normativa di matrice europea e confluito nella normativa italiana, è quello del rafforzamento della cooperazione strategica fra gli Stati Membri e lo scambio di informazioni attraverso la creazione di un gruppo di cooperazione e di una rete di c.d. "squadre di risposta agli incidenti di sicurezza informatica"(c.d. *Computer Security Incident Response Team* – CSIRT). Tali organismi, predisposti a livello nazionale, hanno il compito di monitorare gli incidenti, fornire un allarme tempestivo in caso di impatto oltre il confine nazionale, avvisare e informare le parti interessate sui rischi e sugli incidenti in corso o avvenuti, rispondere agli incidenti, fornire un'analisi dinamica per aumentare la consapevolezza di tutti gli operatori del mercato. In Italia, questo ruolo viene svolto dall'ACN.

Le informazioni relative agli incidenti sono fornite appunto dagli stessi operatori: gli operatori di servizi essenziali (OSE) sono tenuti a notificare, senza indebito ritardo, gli incidenti che hanno un impatto significativo, rispettivamente sulla continuità e sulla fornitura del servizio, allo CSIRT. Per identificare gli incidenti significativi, gli elementi da valutare sono i seguenti:

- il numero di utenti interessati dall'interruzione di un servizio essenziale;
- l'intervallo di tempo durante il quale il servizio essenziale non è stato operativo;
- l'estensione geografica dell'area interessata dall'incidente.

Il presupposto su cui si basa questo scambio informativo, previsto per la prima volta dalla Direttiva NIS, è il fatto che gli OSE utilizzino sistemi di sicurezza informatica simili nel quadro della loro attività e fornitura di servizi. Ciò significa che l'acquisizione di informazioni relative ad un incidente potrebbe aiutare a scoprire altri incidenti (potenziali o in corso) che coinvolgono altri soggetti che operano nel settore. Dunque, l'analisi degli incidenti potrebbe rivelare vulnerabilità condivise. Questo dimostra che la segnalazione degli incidenti ha un duplice obiettivo: nel breve periodo, mira alla scoperta di attacchi su larga scala e all'identificazione delle vulnerabilità sottostanti al fine di consentire una risposta coordinata agli incidenti, mentre nel lungo periodo, mira ad un miglioramento del livello di sicurezza e di preparazione informatica.

È da sottolineare, tuttavia, che la Direttiva NIS, fa riferimento ad una indicazione temporale indefinita per quanto riguarda i tempi di notifica, poiché richiede l'invio della segnalazione "senza indebito ritardo". Questa generica indicazione è stata poi tradotta in un procedimento ben delineato nel d.P.C.M. 14 aprile 2021, n. 81 che prevede una differenziazione sulla base dell'impatto degli incidenti relativi alla sicurezza informatica sugli *asset* ICT degli enti inclusi nel c.d. Perimetro di Sicurezza Nazionale Cibernetico (PSNC - definito con il d.l. 21 settembre 2019, n. 105, DL Perimetro). La tassonomia prevista distingue due tipologie di incidenti sulla base della gravità dello stesso: la Tabella 1 dell'Allegato A contiene gli incidenti meno gravi (e.g. infezione, guasto, installazione, movimenti laterali, azioni sugli obiettivi) e la Tabella 2 quelli più gravi (e.g. azioni sugli obiettivi e disservizio). Questa classificazione è funzionale alle diverse tempistiche necessarie per una risposta efficace. Pertanto, gli OSE dovranno riferire al CSIRT italiano entro un'ora nel caso di un incidente identificato nella Tabella 2 e sei ore nel caso di un incidente rientrante nella Tabella 1. Tali termini decorrono dal momento in cui l'ente viene a conoscenza dell'incidente, ad esempio attraverso le attività di monitoraggio, test e controllo svolte sulla base delle misure di *cybersecurity* previste dallo stesso decreto.

Se l'ente viene a conoscenza di nuovi elementi significativi, tra cui specifiche vulnerabilità sfruttate o, più in generale, la rilevazione di eventi in qualche modo correlati all'incidente, la notifica deve essere modificata senza indebito ritardo dal momento in cui se ne viene a conoscenza, a meno che l'autorità giudiziaria non abbia precedentemente richiesto specifiche esigenze di segretezza delle indagini (si veda l'art. 3(5) d.P.C.M. 81/2021). Inoltre, su richiesta del CSIRT, l'ente che ha notificato un incidente è tenuto, entro sei ore dalla richiesta, ad aggiornare la notifica, ad eccezione dei casi in cui sussistano specifiche esigenze di segreto investigativo.

Ai precedenti obblighi sono aggiunti quelli previsti per gli incidenti che hanno un impatto su reti, sistemi informativi e servizi informatici che si trovano al di fuori del PNSC (diversi quindi dai menzionati asset ICT) ma che sono di pertinenza

di soggetti inclusi nel PNSC (previsti dal novellato art. 1(3-*bis*) del DL Perimetro, così come introdotto dall'art. 37-*quater* (1) d.l. 9 agosto 2022, n. 115, convertito, con modificazioni, in legge 21 settembre 2022). Tali obblighi hanno un termine di notifica di 72 ore; pertanto, meno stringente rispetto a quelli previsti per i beni Perimetro, ma che per limitare eventuali duplicazioni prevede una tassonomia degli incidenti equivalente a quella prevista nelle Tabelle A e B del d.P.C.M. 81/2021 e modalità di notifica in linea con quelle già esistenti.

3. Le novità che emergono dalla Direttiva NIS 2

La Direttiva NIS 2 cerca di superare alcuni dei limiti che erano emersi dall'implementazione della precedente Direttiva NIS. In particolare, sono modificati i criteri per l'identificazione dei soggetti inclusi nel campo di applicazione, passando dalla distinzione fra OSE e fornitori di servizi digitali alla distinzione tra i cosiddetti enti essenziali (*essential entities* - EE) ed importanti (*important entities* - IE). La distinzione non è giustificata da un diverso insieme di requisiti e obblighi di notifica, come accadeva nella direttiva NIS, ma riguarda soltanto il tipo di meccanismi di sorveglianza applicati. Inoltre, la direttiva estende lo scopo di applicazione agli enti della Pubblica amministrazione, prevedendo un obbligo per le strutture centrali e lasciando un livello di discrezionalità agli Stati membri su quella locale (art. 2(f) Direttiva NIS 2). È da sottolineare che le pubbliche amministrazioni non erano escluse dallo scopo di applicazione della Direttiva NIS; tuttavia, rientravano soltanto quelle identificate come OSE dai singoli Stati Membri (considerando (45) Direttiva NIS).

Anche gli obblighi di notifica sono oggetto di modifica e la Direttiva NIS 2 distingue due fasi per la segnalazione degli incidenti. Durante la prima fase, l'entità interessata deve informare, con un rapporto iniziale, lo CSIRT entro ventiquattro ore da quando venga a conoscenza di un incidente. Successivamente, lo stesso soggetto fornirà un rapporto completo entro settantadue ore da quando sia venuto a conoscenza dell'incidente. La seconda fase riguarda il ripristino completo del problema, con la presentazione di un rapporto finale ad un mese dopo il rapporto iniziale.

Si noti che la segnalazione di incidenti cd. significativi è obbligatoria, mentre per qualsiasi altro incidente di livello inferiore non è necessaria la notifica. Tuttavia, al fine di acquisire un quadro completo del panorama delle minacce, la normativa europea fornisce una base giuridica per le notifiche volontarie di incidenti significativi, minacce informatiche e quasi incidenti da parte di entità che non rientrano nell'ambito di applicazione, lasciando agli Stati membri la scelta di dare priorità al trattamento delle notifiche obbligatorie rispetto a quelle volontarie (art. 29 Direttiva NIS 2).

4. Gli obblighi informativi nel DDL Cybersicurezza

Gli obblighi di segnalazione previsti dal DDL Cybersicurezza mostrano una netta differenza dalle norme previste dal d.P.C.M. 81/2021 e una parziale convergenza con le norme previste dalla Direttiva NIS 2. Ai sensi dell'art. 1, le pubbliche amministrazioni sono tenute a segnalare gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici previsti nella tassonomia indicata dall'art. 1 (3-*bis*) d.l. 105/2019. La segnalazione deve essere effettuata entro ventiquattro ore dal momento in cui i soggetti sono venuti a conoscenza dell'evento, cui segue una successiva notifica di tutti gli elementi disponibili entro settantadue ore.

Se approvato secondo il testo attuale, le pubbliche amministrazioni potrebbero trovarsi - nelle more dell'implementazione della Direttiva NIS 2 – a dover valutare se ricadano in una delle seguenti ipotesi. In un primo caso, la Pubblica amministrazione potrebbe essere inclusa nel PNSC e dunque sottoposta al regime previsto dal d.P.C.M. 81/2021. Nel caso in cui l'incidente abbia ad oggetto gli *asset* ICT, la Pubblica amministrazione è tenuta a notificare l'incidente entro un'ora o sei ore dal momento in cui è venuta a conoscenza dell'evento; invece, laddove l'incidente ha ad oggetto reti, sistemi informativi e servizi informatici di pertinenza delle Pubbliche amministrazioni, i tempi si allungano fino a settantadue ore dal momento in cui sono venuti a conoscenza dell'evento. In un secondo caso, la Pubblica amministrazione non è inclusa nel PNSC, ma ricade nelle categorie previste dall'art. 1(1) DDL Cybersicurezza. In caso di incidente che abbia ad oggetto reti, sistemi informativi e servizi informatici (equivalenti ai sopramenzionati *asset* ICT), la Pubblica amministrazione è tenuta a segnalare l'incidente entro ventiquattro ore ed a fornire tutti gli elementi disponibili entro

settantadue ore. Sia nella prima che nella seconda ipotesi, la Pubblica amministrazione non è tenuta a successivi aggiornamenti in merito alla risoluzione dell'incidente.

Indipendentemente dal fatto l'inclusione nel PNSC è segreto di stato, appare evidente che i termini per la segnalazione sono variegati e portano ad una frammentazione che influisce negativamente sull'obiettivo di una rapida e coordinata risposta rispetto ad un eventuale incidente. Da un lato, dal combinato disposto emerge la necessità di un intervento di armonizzazione che permetta alle amministrazioni di rispondere con celerità agli incidenti semplificando il meccanismo di segnalazione in linea con i termini previsti con la Direttiva NIS 2. Dall'altro lato, la mera comunicazione dell'incidente senza una successiva fase di verifica del contenimento e della risoluzione dell'attacco informatico non permette di raggiungere l'obiettivo di una maggiore consapevolezza circa i rischi e le buone pratiche che possono portare al miglioramento del livello di sicurezza a livello generale. Questo passaggio ulteriore è già previsto dalla Direttiva NIS 2, che richiede una seconda fase di aggiornamento ad un mese dalla prima segnalazione. In questo senso, potrebbe essere auspicabile dunque una revisione del testo attuale in cui sia previsto tale ulteriore indicazione, che anticiperebbe l'implementazione della normativa europea e porterebbe ad incrementare i livelli di sicurezza attraverso un maggiore scambio di informazioni.

Riferimenti bibliografici

Agenzia per la Cybersicurezza Nazionale (2023), *Relazione Annuale al Parlamento*, 2023

F. Casarosa, G. Comandé (2024), *Aspettando la NIS2: ovvero il diritto privato della cybersecurity*, in "Diritto dell'informazione e dell'informatica", 2024, n. 1

E. Longo (2024), *Audizione informale per il disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)*, in "Rivista italiana di informatica e diritto", 2024, n. 1

S. Rossa (2023), *Cyber attacchi e incidenti nella pubblica amministrazione, fra organizzazione amministrativa e condotta del funzionario*, in "Vergentis: revista de investigación de la Cátedra Internacional conjunta Inocencio III", 2023, n. 17

S. Schmitz-Berndt (2023), *Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive*, in "Journal of Cybersecurity", vol. 9, 2023, n. 1