NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

La nuova direttiva europea per la cybersicurezza e un ulteriore ampliamento del diritto all'oblio digitale*

di Flavia Zorzi Giustiniani**

Il **14 dicembre** scorso è stata infine adottata, dopo essere stata approvata a larghissima maggioranza dal Parlamento europeo, la nuova direttiva per la cybersicurezza europea (*Network and Information security directive*, cd. direttiva NIS2, concernente l'adozione di misure volte a garantire un livello comune elevato di *cybersecurity* nell'Unione europea)[1]. La direttiva NIS2 è volta a sostituire la precedente direttiva 2016/1148 (cd. NIS1)[2] con una disciplina dotata di maggiore incisività e di un campo di applicazione più ampio. L'obiettiva necessità di procedere a un aggiornamento e nel contempo a un approfondimento della disciplina unionale in materia si è dimostrata ancor più impellente nell'ultimo anno a causa del moltiplicarsi degli attacchi informatici avvenuti in connessione con la pandemia e poi con la guerra russo-ucraina.

L'ambito di applicazione è stato esteso, rispetto alla direttiva NIS1, per quanto concerne sia i destinatari che i settori interessati. Quanto ai primi, essi si identificano nelle medie imprese e in quelle imprese che, indipendentemente dalla dimensione, sono qualificate dalla stessa NIS2 come "soggetti essenziali" o "importanti". Tra i soggetti essenziali sono inclusi: i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che possano considerarsi medie imprese di cui all'art. 2, par. 1, dell'allegato della raccomandazione 2003/361/CE[3]; i prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché i prestatori di servizi DNS, indipendentemente dalle loro dimensioni[4]. Per le due tipologie di enti sono previsti regimi differenziati di vigilanza. In

*Contributo sottoposto a *peer review*.

** Professoressa associata di Diritto dell'Unione europea – Università degli Studi "Link Campus University" di Roma.

[1] Cfr. Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza 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).

[2] La direttiva NIS1, recepita in Italia con il D. Lgs. N. 65/2018, prevede che le società rientranti nel suo ambito di applicazione debbano adottare misure tecniche ed organizzative adeguate e proporzionate rispetto alla gestione dei rischi cibernetici.

[3] Cfr. art. 3.1 a) della direttiva NIS2.

[4] Cfr. art. 3.1 b) della direttiva NIS2.

ISSN 2279-7238

particolare, agli enti essenziali si applicherà un rigoroso regime di vigilanza ex ante, agli enti importanti invece una vigilanza ex post nei soli casi di rilievi o segnalazioni di non conformità. Per quanto concerne i nuovi settori coperti dalla direttiva, vi figurano *inter alia* i servizi digitali (quali *cloud computing*, *data centre*, servizi di comunicazione elettronica e di reti di comunicazione elettronica), i servizi sanitari (società farmaceutiche, produttori di dispositivi medici, healthcare providers ecc.) e i servizi di produzione, trasformazione e distribuzione di cibo, ivi comprese le imprese della grande distribuzione. L'appartenenza al novero dei destinatari della direttiva sarà valutata dai singoli Stati membri sulla base delle informazioni che ogni società sarà tenuta a fornire in base alla nuova disciplina.

I destinatari della direttiva NIS2 dovranno adottare alcune misure minime di gestione della cybersicurezza e di prevenzione delle relative minacce, anche con riguardo alle catene di approvigionamento. Al fine di ovviare alla disomogeneità di soluzioni approntate dai singoli Stati membri nel quadro della direttiva NIS1, il nuovo atto fornisce un elenco di "misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza dei sistemi di rete e di informazione che [i soggetti interessati] utilizzano per le loro operazioni o per la fornitura dei loro servizi e per prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi"[5]. In particolare, gli Stati membri dovranno far sì che le società che rientrano nel campo di applicazione della NIS2 applichino quanto meno misure che comprendono i seguenti elementi:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
b) gestione degli incidenti;
c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;
d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;
g) pratiche di igiene informatica di base e formazione in materia di cybersicurezza;
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso[6].

[5] Cfr. art. 21.1 della direttiva NIS2.
[6] Cfr. art. 21.2 della direttiva NIS2.

Il secondo caposaldo della direttiva è poi costituito dagli obblighi di segnalazione. In particolare, si dispone che i soggetti essenziali e importanti debbano notificare senza indebito ritardo al team nazionale di risposta agli incidenti di sicurezza informatica (CSIRT- *Computer Security Incident Response Team*) o alle autorità competenti eventuali incidenti che abbiano un impatto significativo sulla fornitura dei loro servizi[7]. La nozione di incidente è più ampia rispetto a quella di cui alla NIS1 giacché vi rientrano anche eventi che comportano un danno potenziale. La definizione di "incidente significativo" è peraltro fornita dalla stessa direttiva, che la limita a quegli incidenti che: a) hanno o sono in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) si sono ripercossi o sono in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli[8].

Inoltre, se opportuno, la segnalazione deve essere indirizzata anche ai destinatari del servizio oggetto dell'attacco cibernetico e indicare qualsiasi misura o azione correttiva che tali destinatari sono in grado di adottare in risposta a tale minaccia[9]. La segnalazione, come specificato dalla stessa direttiva, deve avvenire entro ventiquattro ore dalla conoscenza e deve essere seguita da una ulteriore notifica di analisi dettagliata dell'incidente entro settantadue ore dalla conoscenza dello stesso. Nel complesso, gli obblighi di notifica sono stati ridotti al duplice fine di focalizzare l'attenzione sugli incidenti di maggiore rilievo e di non oberare eccessivamente i soggetti interessati.

Più in generale, la direttiva mira a rafforzare la cooperazione tra Stati membri istituendo un gruppo di coordinamento interstatale volto a rafforzare la condivisione di informazioni e richiedendo la creazione di una strategia nazionale sulla cybersicurezza come pure di apposite autorità nazionali di controllo e CSIRT per sviluppare pratiche coordinate di *vulnerability disclosures*. Inoltre, al fine di garantire una gestione coordinata degli incidenti di *cybersecurity* su larga scala, si prevede l'istituzione di un'apposita rete europea delle organizzazioni di collegamento per le crisi informatiche, denominata Eu-Cyclone (European Cyber Crises Liaison Organisation Network).

Agli obblighi previsti si accompagna un apparato sanzionatorio che, in conformità alla prassi dell'Unione in materia di servizi digitali, è modellato su quello del GDPR. Gli Stati membri dovranno prevedere, in particolare, in caso di violazioni dell'art. 21 (recante Misure di gestione dei rischi di cybersicurezza) o 23 (recante Obblighi di segnalazione), sanzioni pecuniarie amministrative fino a 10 fino a 10 milioni di euro o al 2 % del fatturato mondiale totale di impresa per gli enti essenziali e fino a 7 milioni di euro o all'1,4% del fatturato per gli enti importanti[10].

Gli Stati membri avranno 21 mesi di tempo dall'entrata in vigore della direttiva per recepirne le disposizioni nel loro diritto interno. Sforzi ulteriori e particolarmente significativi, considerato il grado di dettaglio del nuovo quadro normativo, dovranno poi essere fatti, auspicabilmente senza una dilatazione eccessiva dei tempi di attuazione, dalle singole imprese interessate.

Un secondo sviluppo di rilievo nel periodo in rassegna si deve alla Corte di Giustizia

[7] Cfr. art. 23.1 della direttiva NIS2.
[8] Cfr. art. 23.3 della direttiva NIS2.
[9] Cfr. art. 23.2 della direttiva NIS2.
[10] Cfr. art. 34, par. 4-5 della direttiva NIS2.

dell'Unione europea (CGUE), che nel caso *TU and RE v. Google LLC* (C-460/20) ha avuto modo di affinare la sua giurisprudenza sul tema del diritto all'oblio digitale[11]. La sentenza, pronunciata l'8 dicembre 2022 nella formazione della Grande Sezione, ha origine dalla vicenda di una coppia di professionisti tedeschi che erano stati presi di mira, in alcuni articoli del 2015, da un sito web statunitense con l'accusa di proporre investimenti con modalità ricattatorie e di essersi conseguentemente arricchiti, come evidenziato dalle immagini di anteprima (cd. *thumbnails* – miniature) allegate che li raffiguravano su mezzi di lusso. A seguito del rifiuto di Google di procedere alla deindicizzazione degli articoli e dei media contestati, la coppia si era risolta ad adire la magistratura tedesca. Il caso è giunto sino alla Corte Federale, che ha deciso di sospendere il procedimento investendo nel contempo la CGUE di due questioni pregiudiziali, che possono così riassumersi. In primo luogo, come dovrebbero essere risolte dalle corti le richieste di deindicizzazione nei casi in cui i ricorrenti contestano l'esattezza delle informazioni riportate da una testata giornalistica e la legalità della pubblicazione dipende dal carattere veritiero delle affermazioni ivi contenute? In secondo luogo, i titolari del trattamento di un servizio di ricerca su Internet sono obbligati ad eliminare le miniature dai risultati di una ricerca nominativa, anche se i risultati contengono un collegamento alla fonte originale?

Nel rispondere al primo quesito, la Grande Sezione, dopo aver ribadito che il trattamento dei dati personali effettuato dal motore di ricerca va distinto da quello compiuto dagli editori di siti web, ricorda che il diritto alla cancellazione ex art. 17 GDPR (che, giova ricordarlo, è rubricato seppur impropriamente diritto all'oblio) deve essere bilanciato con il diritto fondamentale alla libertà di informazione codificato all'art. 11 della Carta dei diritti fondamentali dell'Unione europea. Ricorda poi che, sebbene "di regola", secondo costante giurisprudenza, i diritti dell'interessato ex artt. 7 e 8 della Carta prevalgono "sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso all'informazione in questione, tale equilibrio può nondimeno dipendere dalle circostanze rilevanti di ciascun caso, in particolare dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata dell'interessato, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica"[12].

Per quanto concerne poi la richiesta di deindicizzazione per inesattezza del contenuto indicizzato, la Grande Sezione afferma che tale richiesta, in mancanza di una decisione giudiziaria che accerti l'errore nelle informazioni riportate dall'editore del sito, deve essere accolta dal gestore del motore di ricerca soltanto allorché la persona interessata "apporti elementi di prova pertinenti e sufficienti, idonei a suffragare la sua richiesta e atti a dimostrare il carattere manifestamente inesatto delle informazioni incluse nel contenuto indicizzato o, quantomeno, di una parte di tali informazioni che non abbia un carattere secondario rispetto alla totalità di tale contenuto"[13]. Quanto agli obblighi e responsabilità incombenti sul gestore del motore di ricerca, quest'ultimo

[11] Sulla giurisprudenza europea relativa al diritto all'oblio digitale sia consentito rinviare alla precedente rassegna Cronache sul cyberspazio n. 3/2019 e *amplius* a F. ZORZI GIUSTINIANI, *Il diritto all'oblio nella rete e i suoi limiti nell'attuale contesto europeo*, in G. CAGGIANO - F. MARTINES (a cura di), *Temi e questioni di diritto dell'Unione europea – Scritti offerti a Claudia Morviducci*, Bari, Cacucci, 2019.

[12] Cfr. il par. 62 della sentenza.

[13] Cfr. il par. 72 della sentenza.

nel valutare la richiesta di deindicizzazione "deve fondarsi sull'insieme dei diritti e degli interessi in gioco nonché su tutte le circostanze del caso di specie"[14]. Tuttavia, sottolinea la CGUE, esso "non può essere tenuto a svolgere un ruolo attivo nella ricerca di elementi di fatto che non sono suffragati dalla richiesta di cancellazione, al fine di determinare la fondatezza di tale richiesta"[15]. Nel caso in cui l'inesattezza delle informazioni non appaia in modo manifesto il richiedente potrà sempre rivolgersi all'autorità di controllo o all'autorità giudiziaria per le verifiche necessarie.

Con riferimento al secondo quesito, relativo alla visualizzazione delle foto in forma di miniature a seguito di una ricerca nominativa, la Grande Sezione afferma che detta visualizzazione è idonea a costituire una ingerenza particolarmente significativa nei diritti alla tutela della vita privata e dei dati personali di tale persona[16]. La Corte aggiunge poi che nel valutare una richiesta di deindicizzazione riguardante foto visualizzate sotto forma di miniature il gestore di un motore di ricerca deve procedere ad un distinto bilanciamento dei diritti fondamentali contrapposti. È pertanto necessario tenere in considerazione il valore informativo delle foto in questione "indipendentemente dal contesto della loro pubblicazione nella pagina Internet da cui sono state tratte, prendendo però in considerazione qualsiasi elemento testuale che accompagna direttamente la visualizzazione di tali fotografie nei risultati della ricerca e che può apportare chiarimenti riguardo al loro valore informativo"[17].

La sentenza, che ha in larga parte fatto propria l'opinione espressa dall'Avvocato Generale Petruzzella nelle sue conclusioni, facilita ulteriormente rispetto al passato l'esercizio del diritto all'oblio senza porre oneri eccessivi a carico del gestore. La previa predisposizione da parte dei ricorrenti delle prove a sostegno della falsità delle informazioni diffuse dovrebbe impedire, come sostenuto da Petruzzella, di "trasformare Google nel «giudice della verità» o di realizzare una sorta di censura privata dell'informazione sulla rete"[18]. Rimane tuttavia una criticità di fondo che appare difficilmente risolvibile "a diritto invariato", e che consiste nell'affidare ad un gestore privato, in una situazione peraltro di quasi monopolio, la valutazione della veridicità delle informazioni presenti nel web[19].

[14] Cfr. il par. 69 della sentenza.
[15] Cfr. il par. 70 della sentenza.
[16] Cfr. il par. 93 della sentenza.
[17] Cfr. il par. 108 della sentenza.
[18] Cfr. Conclusioni dell'Avvocato Generale Giovanni Pitruzzella presentate Il 7 Aprile 2022, Causa C-460/20, *TU, RE contro Google LLC*, par. 49 delle conclusioni dell'Avvocato Generale, par. 49.
[19] Per un commento alla sentenza si veda per tutti O.J. GSTREIN, *The Right to be Forgotten in 2022 Luxembourg judges keep surfing the legislative void*, in *Verfassungsblog*, 2022, che così conclude: "While the judgment might be seen as a logical and consistent step in enhancing the jurisprudence of the CJEU on the matter, the history of the right to be forgotten in the EU and beyond also highlights the lack of a shared societal vision on how datafication should manifest in European and Western democracies".