NOMOS
Le attualità nel diritto

Quadrimestrale di Teoria generale,
Diritto pubblico comparato e Storia costituzionale

FLAVIA ZORZI GIUSTINIANI*

IL *CYBER SOLIDARITY ACT* E LA SENTENZA C-154/21 DELLA CORTE DI GIUSTIZIA UE**

SOMMARIO: 1. Il *Cyber Solidarity Act*. – 2. La sentenza C-154/21 della Corte di Giustizia UE nel caso RW c. *Österreichische Post*.

1. Il *Cyber Solidarity Act*

Nel periodo in rassegna deve segnalarsi anzitutto la nuova proposta di Regolamento «volto a stabilire misure per rafforzare la solidarietà e le capacità dell'Unione di individuare, prepararsi e rispondere alle minacce e agli incidenti di cibersicurezza» (cd. *Cyber Solidarity Act*, di seguito CSA), presentata lo scorso 18 aprile dalla Commissione europea[1]. Il disposto normativo trae origine dalla crescente vulnerabilità, riscontrata in particolare nel contesto del conflitto russo-ucraino, di infrastrutture, servizi essenziali ed entità critiche ad attacchi e minacce cibernetiche. Il CSA ha infatti come scopo precipuo quello di rafforzare la solidarietà e le capacità dell'Unione per individuare e rispondere tempestivamente a minacce e incidenti informatici di una certa entità.

Il piano prevede lo stanziamento di 1,1 miliardi di euro, che saranno finanziati per due terzi direttamente dal bilancio dell'Unione attraverso il programma Europa Digitale. Il CSA prospetta in primo luogo la creazione di uno Scudo informatico europeo, ovvero un'infrastruttura paneuropea composta da una serie di centri operativi di sicurezza (*Security Operation Centres* - SOCs) interconnessi, nazionali e transfrontalieri, ubicati in tutta l'Unione europea[2]. Una volta operativi i SOCs, con l'ausilio di tecnologie di avanguardia quali sistemi di intelligenza artificiale e analisi avanzata dei dati, avranno il compito di rilevare e condividere avvisi tempestivi su minacce e incidenti informatici a livello transfrontaliero. Ciò dovrebbe consentire nel breve termine di ridurre a poche ore il tempo necessario per

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

** Contributo sottoposto a *peer review*.

[1] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM(2023) 209 final, Strasburgo, 18 aprile 2023.

[2] Allo Scudo informatico europeo é dedicato il capitolo II della proposta di CSA.

ISSN 2279-7238

rilevare un attacco informatico complesso e, nel lungo periodo, di rilevare un attacco *cyber* prima che questo venga messo in atto.

Tra le misure proposte vi è poi l'istituzione di un Meccanismo di emergenza informatica (*Cyber Emergency Mechanism*), con il quale si intende ad un tempo aumentare la preparazione e rafforzare le capacità di risposta e ripresa agli incidenti informatici su larga scala nel territorio dell'Unione[3]. Il supporto fornito dal Meccanismo è concepito per essere complementare sia alle risorse e alle capacità nazionali che ad altre forme di aiuto disponibili a livello UE. Si dovrebbero predisporre in particolare azioni di preparazione a potenziali vulnerabilità individuate in base a scenari e metodologie di rischio comuni e con specifica attenzione a settori altamente critici (*inter alia* sanità, trasporti ed energia). Il Meccanismo proposto comprende al suo interno un'apposita riserva europea di cybersicurezza basata su molteplici servizi di risposta agli attacchi da parte di fornitori selezionati, i quali saranno pronti ad intervenire in caso di incidenti significativi o su larga scala, su richiesta di uno Stato membro, di istituzioni o di organismi e agenzie della UE. Nell'ambito del Meccanismo è inoltre previsto un sostegno finanziario per l'assistenza reciproca tra Stati membri in caso di emergenza informatica.

Il CSA prevede infine l'introduzione di un sistema di rianalisi degli incidenti cibernetici (cd. *Cybersecurity Incident Review Mechanism*) volto ad esaminare gli attacchi più rilevanti o su larga scala per sviluppare ulteriormente la protezione dell'UE contro le minacce future[4]. L'attività di *review* è assegnata, su richiesta volta volta della Commissione europea, della Rete di Organizzazioni di Collegamento per la Crisi Informatica (EU-CyCLONe) o della Rete delle Squadre di Risposta agli incidenti informatici (CSIRTs), all'agenzia europea per la sicurezza informatica (ENISA). Quest'ultima dovrebbe quindi realizzare un'apposita relazione di revisione dell'incidente da presentare a EU CyCLONe, alla rete CSIRTs nonché alla Commissione europea. Nella suddetta relazione ENISA, anche sulla scorta delle informazioni fornite dai *service providers* e dalle altre entità coinvolte (quali in particolare rappresentanti del settore privato, degli Stati membri e della Commissione), dovrebbe mettere in luce le cause dell'incidente e le criticità maggiori riscontrate, dar conto dell'esito dell'analisi e avanzare se del caso proposte volte a ottimizzare le capacità di risposta dell'UE in ambito cibernetico.

2. La sentenza C-154/21 della Corte di Giustizia UE nel caso RW c. *Österreichische Post.*

Un secondo sviluppo degno di nota si deve alla Corte di Giustizia dell'Unione europea (CGUE), che nella sentenza C-154/2021 resa in via pregiudiziale il 12 gennaio 2023 si è pronunciata in merito agli obblighi del titolare del trattamento nei confronti degli interessati che esercitano il diritto di accesso. Nel caso di specie il cittadino austriaco RW aveva chiesto

[3] Cfr. il capitolo III della proposta di CSA.
[4] Cfr. il capitolo IV della proposta di CSA.

a *Österreichische Post* (le poste austriache) di conoscere a chi erano stati trasmessi i suoi dati personali. *Österreichische Post* si era limitata ad indicare che il trattamento era effettuato nel rispetto della legge e che i dati erano forniti ai partner commerciali a fini di marketing. In primo grado e in appello i giudici avevano respinto il ricorso con la motivazione che l'art. 15 par. 1 lett. c) del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (Regolamento generale sulla protezione dei dati, cd. GDPR), laddove si riferisce a «destinatari o categorie di destinatari» permetterebbe al titolare del trattamento di indicare all'interessato soltanto le categorie di destinatari e non anche gli specifici destinatari dei suoi dati personali. In ultima istanza, la Corte suprema austriaca (Oberster Gerichtshof) ha invece deciso di interpellare la CGUE in merito alla portata del diritto dell'interessato di ottenere informazioni circa i destinatari dei suoi dati personali. In altri termini, il giudice del rinvio ha chiesto ai giudici di Lussemburgo se l'art. 15 par. 1 lett. c) del GDPR imponga o meno al titolare del trattamento dei dati di comunicare all'interessato l'identità concreta dei destinatari dei suoi dati.

La risposta della CGUE è stata netta. A suo avviso l'art. 15 par. 1 lett. c) del GDPR deve essere interpretato nel senso che «il diritto di accesso dell'interessato ai dati personali che lo riguardano, previsto da tale disposizione, implica, qualora tali dati siano stati o saranno comunicati a destinatari, l'obbligo per il titolare del trattamento di fornire a detto interessato l'identità stessa di tali destinatari, a meno che sia impossibile identificare detti destinatari o che il suddetto titolare del trattamento dimostri che le richieste di accesso dell'interessato sono manifestamente infondate o eccessive, ai sensi dell'articolo 12, paragrafo 5, del regolamento 2016/679, nel qual caso il titolare del trattamento può indicare a detto interessato unicamente le categorie di destinatari di cui trattasi». Per giungere a siffatta conclusione la prima sezione della CGUE ha proceduto ad una interpretazione sistematica della disposizione in oggetto, tenendo conto in particolare delle finalità della stessa. Accogliendo la posizione espressa dall'Avvocato Generale Pitruzzella sul punto[5], la CGUE ha statuito che la norma in discorso, la quale deve essere interpretata congiuntamente al considerando 63 del GDPR[6], obbliga il titolare del trattamento a fornire all'interessato, su sua richiesta, l'identità dei destinatari specifici. Ne consegue che il titolare ha un preciso obbligo al riguardo, nel rispetto del principio di trasparenza. La Corte ha però ricordato che il diritto alla protezione dei dati personali non ha carattere assoluto e va contemperato con altri diritti fondamentali, conformemente al principio di proporzionalità. Il suddetto obbligo del titolare del trattamento trova pertanto delle limitazioni, non soltanto allorché risulti impossibile identificare i destinatari ma anche quando il titolare dimostri che le

[5] Cfr. le Conclusioni dell'Avvocato Generale Giovanni Pitruzzella presentate il 9 giugno 2022, causa C-154/21, *RW contro Österreichische Post AG*, par. 22.

[6] «Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. […] Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento […]».

richieste dell'interessato siano manifestamente infondate o eccessive ex art. 12 par. 5 del GDPR. I giudici europei hanno poi sottolineato il ruolo cruciale svolto dal diritto di accesso, essendo lo stesso funzionale all'esercizio degli altri diritti riconosciuti dal GDPR, quali il diritto di rettifica, il diritto alla cancellazione, il diritto di limitazione di trattamento, il diritto di opposizione al trattamento o ancora il diritto di agire in giudizio nel caso in cui si subisca un danno[7].

L'interpretazione fornita dalla CGUE del diritto di accesso conferma quanto già espresso al riguardo dal Comitato europeo per la protezione dei dati (European Data Protection Board – EDPB) nelle "Guidelines 01/2022 on data subject rights - Right of access"[8]. Siffatte linee guida concepiscono il diritto di accesso in senso assai ampio, come è evidente tra l'altro dalla condotta che raccomandano al titolare del trattamento di fronte a una richiesta di accesso: il titolare, infatti, «should always be able to demonstrate, that the way to handle the request aims to give the broadest effect to the right of access and that it is in line with its obligation to facilitate the exercise of data subjects rights»[9].

D'ora innanzi, dunque, i titolari di trattamento dovranno rivedere le proprie informative, tipicamente assai generiche[10], e premurarsi che le stesse forniscano indicazioni specifiche, in primo luogo con riferimento all'identificazione dei destinatari dei dati personali oggetto del trattamento.

[7] V. in particolare il par. 38 della sentenza.

[8] Il testo delle Linee Guida, adottate dall'EDPB il 18 gennaio 2022, sono disponibili al seguente link.

[9] EDPB, *Guidelines 01/2022*, par. 35 b), p. 16.

[10] Nondimeno, indicazioni sul contenuto che dette informative dovrebbero avere sono state fornite, già da qualche anno, nelle *Guidelines on Transparency under Regulation 2016/679* del Gruppo di lavoro Articolo 29 per la protezione dei dati (adottate il 29 novembre 2017 e poi, in una versione rivista, l'11 aprile 2018).