JUS CIVILE

MARIA FRANCESCA TOMMASINI*

CYBERSICUREZZA E TUTELA DEI DATI PERSONALI: UN'ANALISI MULTILIVELLO**

CYBERSECURITY AND PERSONAL DATA PROTECTION: A MULTILEVEL ANALYSIS

ABSTRACT: La cybersicurezza rappresenta una sfida strategica nella società digitale globale, richiedendo un approccio multilivello che integri la dimensione transnazionale, il quadro normativo europeo e la sua attuazione a livello nazionale. L'Unione Europea ha adottato un corpus normativo organico — Direttive NIS/NIS2, Cybersecurity Act e Cyber Resilience Act — finalizzato alla protezione delle infrastrutture critiche, al rafforzamento della resilienza digitale e alla responsabilizzazione dei vertici aziendali. Anche l'Italia ha rafforzato la propria disciplina in materia, istituendo il Perimetro di Sicurezza Nazionale Cibernetica e l'Agenzia per la Cybersicurezza Nazionale, **assicurando la protezione delle infrastrutture digitali e dei dati personali nel rispetto dei diritti fondamentali sanciti dal GDPR**. L'assetto complessivo della cybersicurezza si configura, pertanto, quale strumento essenziale per garantire l'integrità delle infrastrutture digitali, tutelare i diritti fondamentali degli individui e promuovere uno sviluppo tecnologico sicuro, resiliente e conforme ai principi democratici.

Abstract: Cybersecurity represents a strategic challenge in the global digital society. It requires a multi-level approach that encompasses transnational, European, and domestic law. With the NIS/NIS2 Directives, the Cybersecurity Act, and the Cyber Resilience Act, the European Union has focused its efforts on protecting critical infrastructure and holding companies accountable. Italy has established the National Cybersecurity Perimeter and the National Cybersecurity Agency, thus ensuring the protection of digital infrastructure and personal data. The overall cybersecurity framework is an essential tool for ensuring the integrity of digital infrastructure and protecting the fundamental rights of individuals.

1. La cybersicurezza tra dimensione transnazionale e quadro normativo europeo

Nel contesto della società digitale contemporanea, la cibersicurezza emerge come una delle sfide giuridiche e politiche più rilevanti del XXI secolo. La diffusione delle tecnologie digitali e l'interconnessione globale delle reti informatiche hanno comportato, infatti, un aumento significativo del *cybercrime*, che

* Professoressa ordinaria di Diritto privato – Università degli Studi di Messina.

** Contributo sottoposto a revisione.

ISSN 2281-3918/2421-2563

colpisce indiscriminatamente individui, imprese e istituzioni [1]. Gli attacchi informatici non rappresentano più fenomeni occasionali o marginali, ma vere e proprie minacce sistemiche con conseguenze economiche, patrimoniali e reputazionali rilevanti [2]. Di qui la necessità di predisporre misure tecniche e organizzative costantemente aggiornate, in grado di ridurre al minimo il rischio di diffusione non autorizzata dei dati digitali prodotti [3] e di garantire una reazione rapida ed efficace in caso di violazioni della sicurezza, tutelando così la continuità operativa delle attività e la protezione dei diritti degli utenti. La complessità e la natura del fenomeno determinano l'emersione di un sistema di tutela della cibersicurezza "*multilivello*", che si sviluppa lungo una traiettoria transnazionale, si consolida attraverso interventi normativi a livello europeo e trova attuazione concreta negli ordinamenti nazionali, sino a tradursi in obblighi specifici in capo ai soggetti che, a vario titolo, trattano dati e gestiscono sistemi informativi. Se, infatti, la tutela dello spazio cibernetico è oggi dominata dai poli statunitense [4] e cinese [5], entrambi capaci di esercitare un'influenza che travalica i confini nazionali attraverso reti di cooperazione tecnologica e modelli distinti di *governance* digitale, anche l'Europa ha sviluppato negli ultimi anni un approccio innovativo e coordinato alla sicurezza digitale [6]. In particolare, l'Unione europea ha progressivamente costruito un quadro normativo organico che mira non solo a proteggere le infrastrutture critiche e i servizi essenziali, ma anche a rafforzare la resilienza complessiva del proprio ecosistema digitale [7]. Questo percorso ha trovato

---

[1] Il primo episodio significativo che ha segnato un punto di svolta nella cybersicurezza risale al 2007 quando l'Estonia per 22 giorni fu colpita da una campagna di attacchi informatici di tipo DDoS (*Distributed Denial of Service*) che presero di mira le reti informatiche del paese. La causa scatenante dell'evento fu la decisione del governo estone di spostare un monumento alle truppe dell'Armata Rossa (Il Soldato di bronzo) da un incrocio trafficato nel centro di Tallinn a un vicino cimitero militare (Boni M., *Il Soldato di Bronzo e il cyber attacco all'Estonia del 27 aprile 2007,* in *https://www.analisidifesa.it/2024/04*).

[2] Secondo il Rapporto Clusit, il primo semestre 2025 ha segnato un aumento del 36% degli attacchi *cyber* a livello globale. Sono, infatti, circa 2.775 gli incidenti registrati da Clusit –Associazione Italiana per la Sicurezza Informatica– e la maggior parte di essi sono di gravità "critica" o "elevata". In Italia la crescita degli attacchi registra un aumento del 13% (*Attacchi cyber, crescita record nel primo semestre del 2025 e Italia sempre nel mirino: i dati del rapporto Clusit*, in *https://www.innovationpost.it*).

[3] Nel 2024 circa 5,5 miliardi di persone in tutto il mondo hanno utilizzato Internet, spostando un volume di dati di circa 154 zettabyte. Si prevede che questo dato entro il 2027 salirà a ben 284,3 zettabyte (Hinz L., *...la quantità di dati digitali generati e replicati ogni anno raggiungerà i 284,3 zettabyte entro il 2027?*, in *https://bu-power.com/it).*

[4] L'amministrazione Biden nel 2020 ha messo da subito al centro del suo programma politico il tema della sicurezza informatica varando il *National Cyber Security Strategy*-NCSS (in *https://nkbpsrohini.com/wp-content)* che definisce principi e linee guida uniformi per mitigare gli attacchi cyber nel Paese. Il documento mira a coinvolgere le organizzazioni federali, i gestori di infrastrutture critiche e le grandi aziende nell'adozione di strategie di cyber security uniformate; a distribuire equamente gli investimenti per la ricerca e lo sviluppo di nuove tecnologie per la sicurezza delle infrastrutture critiche; a migliorare la collaborazione internazionale; ad aumentare gli investimenti in strategie *offensive* oltre che difensive; ad adottare un approccio *data driven* per adattare le strategie ai cambiamenti tecnologici e geopolitici. A differenza di Biden, il presidente Trump, piuttosto che continuare ad investire in questa direzione, con l'*One Big Beautiful Bill Act* 2025-2026 (in *https://www.congress.gov/bill/119th-congress/house-bill/1/text*) ha tagliato la spesa per la sicurezza informatica delle agenzie federali di oltre 1,2 miliardi di dollari.

[5] Il modello cinese si caratterizza per il fatto che la protezione del cyberspazio è considerata parte integrante della sicurezza nazionale. A partire dalla *China Cybersecurity Law* entrata in vigore il 1° giugno 2017 (Belfi M., *China Cybersecurity Law, ecco la "Grande muraglia" normativa cinese*, in *https://www.agendadigitale.eu/sicurezza/china-cybersecurity-law),* l'ordinamento ha introdotto un articolato sistema di obblighi per gli operatori di rete, imponendo misure di sicurezza, requisiti tecnici e stringenti limiti all'esportazione dei dati, in linea con la dottrina della *cyber-sovereignty*, che attribuisce allo Stato un controllo pieno sul proprio spazio digitale. Tale impianto è stato consolidato con la *Data Security Law of the People's Republic of China* (in *http://www.npc.gov.cn/englishnpc)* e con la *Personal Information Protection Law of the People's Republic of China* (PIPL) del 2021 (in *https://personalinformationprotectionlaw.com*), che disciplinano rispettivamente la gestione dei dati in base alla loro criticità e il trattamento dei dati personali.

[6] Finocchiaro G., *La proposta di Regolamento sull'Intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Diritto dell'informazione e dell'informatica* 2022, 303.

[7] Sul punto a titolo esemplificativo si vedano: Salamone L., *La disciplina del cyberspace alla luce della direttiva europea*

ISSN 2281-3918/2421-2563

espressione innanzitutto nella Direttiva UE 2016/1148 (c.d. Direttiva NIS – *Network and Information security*) che ha introdotto misure comuni al fine di conseguire un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea"[8] ed ha imposto la notifica degli incidenti "significativi" ai CSIRT (*Computer Security Incident Response Team*) nazionali[9]. Nel 2019, poi, l'Unione, con il *Cybersecurity Act*[10] ha attribuito a ENISA (Agenzia europea per la cibersicurezza) un mandato permanente per la prevenzione e gestione degli incidenti informatici, introducendo, per la prima volta, un quadro europeo di certificazione della cybersicurezza atto a garantire standard uniformi per prodotti, servizi e processi ICT (*Information and Communication Technologies*)[11]. È solo con la Direttiva UE 2555/2022 (NIS 2)[12], però, che il legislatore, non solo amplia il numero di settori e organizzazioni obbligate a rispettare i requisiti di *cybersecurity*[13], ma introduce obblighi di sicurezza più stringenti[14], l'applicazione di misure tecniche e organizzative più dettagliate e la necessità di notificare incidenti gravi in tempi più rapidi[15]. Una ulteriore novità di grande rilievo riguarda il rafforzamento della responsabilità dei vertici aziendali: il *management* è

---

delle reti e dell'informazione, in *Federalismi* 2017; e successivamente anche LAURO A., *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *Rivista del Gruppo di Pisa* 2021, 3.

[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, in *https://eur-lex.europa.eu/eli/dir/2016/1148/oj/ita/pdf*. La Direttiva NIS, e il decreto di attuazione, si rivolgono agli Operatori di servizi essenziali (OES) cioè ai soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali; e ai *Digital Service Provider* (DSP), cioè alle persone giuridiche che forniscono servizi di *e-commerce*, *cloud computing* o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale. Non sono soggetti alla normativa i DSP le piccole e medie imprese con meno di 50 dipendenti o con fatturato inferiore ai 10 milioni l'anno.

[9] SCHMITZ BERNDT S.– SCHIFFNER S., *Don't tell them now (or at all). Responsible disclosure of security incidents under NIS Directive and GDPR*, in *International Review of law. Computer & Technology* 2021, 101.

[10] Il *Cybersecurity Act*, entrato in vigore il 27 giugno 2019 con il Regolamento (UE) 2019/881(in *https://www.agendadigitale.eu/sicurezza/cybersecurity*), è stato reso esecutivo dalla Commissione europea il 18/19 dicembre 2024 con il Regolamento (UE) 2024/3143 della Commissione del 18 dicembre 2024; con il Regolamento (UE) 2024/3144 della Commissione che modifica il Regolamento di esecuzione (UE) 2024/482; e con il Regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio che modifica il Regolamento (UE) 2019/881 (in *https://www.acn.gov.it/portale/w/regolamento-ue-2019/881-cybersecurity-act-aggiornamenti normativa-europea).*

[11] In questo senso la *cibersecurity* è vista quale elemento chiave del Piano europeo per la transizione digitale (*Shaping EU's Digital Future 2020*, in *https://ec.europa.eu/info/strategy/priorities-2019-2024*) e del *Recovery Plan* (*Recovery Plan for Europe*, in *https://ec.europa.eu/info/strategy/recovery-plan-europe).*

[12] 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), in *https://eur-lex.europa.eu/eli/dir/2022/2555/oj/ita*. La NIS 2 muove, al pari della NIS 1, dall'articolo 114 del TFUE (in *https://eur-lex.europa.eu*) che permette di armonizzare le legislazioni nazionali per eliminare ostacoli alla libera circolazione di beni, servizi, persone e capitali e consente all'UE di adottare direttive e regolamenti in settori come sicurezza, salute e ambiente e per regolare settori innovativi come l'intelligenza artificiale (*AI Act*).

[13] Oltre i tradizionali operatori di servizi essenziali come energia, trasporti e sanità, l'obbligo viene esteso ai servizi postali, alla gestione dei rifiuti, a tutte le infrastrutture digitali critiche e alle grandi piattaforme *online*.

[14] L'articolo 21 del NIS 2, richiede l'adozione di misure di sicurezza basate sul rischio, comprendenti la gestione degli incidenti e della continuità operativa, la sicurezza della supply chain, la protezione dei sistemi informativi lungo il loro ciclo di vita, la valutazione dell'efficacia delle misure adottate, la formazione e l'igiene informatica, l'uso della crittografia, la gestione degli accessi e degli asset e l'impiego di autenticazione forte e comunicazioni sicure.

[15] Con riferimento agli obblighi di notifica, la NIS 2 prevede un approccio in due fasi: una prima fase di notifica, con rapporto iniziale entro 24 ore e rapporto completo entro 72 ore dalla conoscenza dell'incidente; una seconda fase di ripristino, con presentazione di un rapporto finale entro un mese dal rapporto iniziale (CASAROSA F.-COMANDÈ G., *Aspettando la NIS 2. Ovvero il diritto privato della cybersecurity*, in *Dir. dell'informazione e dell'informatica* 2024, 1, 29).

ISSN 2281-3918/2421-2563

infatti chiamato a rispondere direttamente del rispetto delle disposizioni normative, con la previsione di sanzioni personali in caso di inadempienza. La sicurezza informatica, così, cessa di essere un profilo esclusivamente tecnico o operativo e diventa a pieno titolo una responsabilità strategica e di *governance*. A completare e integrare la NIS2, nell'ultimo anno, sono intervenuti il Regolamento *Cyber Resilience Act* (CRA) del 2024 che stabilisce requisiti obbligatori di sicurezza per tutti i prodotti (*hardware* e *software*) con elementi digitali [16], e il *Cyber Solidarity Act* (CSA) del 2025 volto a predisporre un sistema europeo di capacità comuni per la rilevazione, l'analisi e la risposta agli attacchi cibernetici su larga scala [17].

2. La sicurezza nazionale e la sicurezza cibernetica nell'ordinamento giuridico italiano

In continuità con il quadro definito a livello europeo [18], l'ordinamento italiano ha progressivamente sviluppato un assetto normativo volto a presidiare la sicurezza nazionale, ampliandone progressivamente gli ambiti di riferimento sino a ricomprendervi anche la sicurezza cibernetica. Se dalla formazione del Regno d'Italia fino all'epoca fascista [19] il concetto di sicurezza nazionale era ancora poco definito [20], con l'instaurazione della Repubblica e l'entrata in vigore della Costituzione del 1948 esso è emerso in forma implicita, come risultato dell'impianto costituzionale nel suo complesso che articola un delicato bilanciamento tra la tutela dello Stato e della collettività (articoli 52, 78 e 87) e la protezione delle libertà individuali (articoli 2, 3, 13, 14 e 15) che ammettono limitazioni esclusivamente nei casi e nei modi stabiliti dalla legge e per comprovate esigenze di sicurezza [21]. Nel corso, poi, degli ultimi decenni il concetto di sicurezza nazionale si è ampliato tanto da potersi qualificare come garanzia per l'indipendenza, l'integrità e la difesa dello Stato, assumendo una dimensione "funzionale alla protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia" (articolo 6, comma 2, della L. n. 124 del 2007) [22]. Proprio al fine di predisporre procedure e misure

[16] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sui requisiti orizzontali di sicurezza informatica per i prodotti con elementi digitali e che modifica i Regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la Direttiva (UE) 2020/1828 (legge sulla resilienza informatica), in *https://eur-lex.europa.eu/eli/reg.* Il CRA impone ai produttori obblighi di sicurezza *by design* e *by default*, processi di gestione delle vulnerabilità e obblighi di notifica. In tal modo il legislatore europeo ha colmato una lacuna cruciale, creando una catena di responsabilità che parte dalla progettazione del prodotto e arriva fino all'esercizio quotidiano dei sistemi informativi (GALLOTTI C., *Cyber resilience act, la sicurezza diventa obbligatoria: cosa cambia per le aziende,* in *https://www.agendadigitale.eu/sicurezza/cyber-resilience-act).*

[17] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure volte a rafforzare la solidarietà e le capacità nell'Unione di individuare, preparare e rispondere alle minacce e agli incidenti informatici e che modifica il Regolamento (UE) 2021/694 (legge sulla solidarietà informatica), in *https://eur-lex.europa.eu/eli/reg/2025*). Il Regolamento mira a rafforzare la capacità dell'UE di rilevare e rispondere a minacce informatiche su larga scala tramite un sistema di allarme basato su SOC nazionali e transfrontalieri interconnessi, costituendo un vero e proprio "Cyberscudo europeo" (ALU' A., *Cyber Solidarity Act: lo "scudo digitale" Ue contro le minacce informatiche*, in *https://www.agendadigitale.eu/sicurezza*).

[18] CENCETTI C., *Cybersecurity: Unione Europea e Italia: Prospettive a confronto*, Roma 2014, 18.

[19] Con il passaggio dallo Stato liberale al regime fascista, i poteri di polizia e di prevenzione subirono un significativo ampliamento: le libertà e i diritti individuali furono fortemente compressi, mentre molte attività prima libere vennero assoggettate a rigidi obblighi e controlli (CORSO G., *L'ordine pubblico*, Bologna 1979; CASSESE S., *Lo Stato fascista*, Bologna 2010).

[20] Nell'ordinamento italiano, il potere di polizia, espressione della sovranità, aveva una funzione prevalentemente preventiva, volta alla tutela della collettività e del bene comune. Per un approfondimento sul tema, si veda RANELLETTI O., *La polizia di sicurezza*, in AA.VV., *Primo trattato completo di diritto amministrativo italiano* a cura di Orlando, Milano 1904, 4.

[21] URSI R., *La sicurezza pubblica,* Bologna 2022, 67 e ss.

[22] Legge n. 124 del 3 agosto 2007 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto), in *G.U.* n. 187 del 13 agosto 2007.

ISSN 2281-3918/2421-2563

tali da consentire una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti tecnologici, il legislatore è intervenuto in rapida successione prima con il D. Lgs n. 65 del 18 maggio 2018 [23], poi con il D. l. n. 105 del 21 settembre 2019 [24] e, infine, con il Decreto del Presidente del Consiglio dei ministri n. 131 del 30 luglio 2020 [25]. I provvedimenti in questione rappresentano la base normativa istitutiva del Perimetro di sicurezza nazionale cibernetica (PSNC) che "ha lo scopo di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale" (ex articolo 1 L. n. 105 del 2019). Dalla formulazione della norma emerge chiaramente la distinzione operata dal legislatore tra sicurezza nazionale e sicurezza cibernetica. La prima è tradizionalmente orientata alla tutela delle istituzioni pubbliche e viene garantita esclusivamente da autorità statali dotate di poteri di *puissance publique* [26]. La sicurezza cibernetica, invece, per la natura stessa delle infrastrutture digitali, richiede l'inclusione anche dei soggetti privati, i quali svolgono funzioni essenziali e risultano parimenti esposti ad attacchi che possono colpire reti, sistemi informativi e servizi digitali. Ne consegue che, mentre la sicurezza nazionale rimane una categoria ampia e priva di confini operativi rigidamente tracciati, la sicurezza cibernetica si caratterizza per la necessità di una tutela condivisa, fondata sulla cooperazione strutturata tra ente pubblico e soggetti privati. In quest'ottica, assume particolare rilievo il ricorso a strumenti innovativi, quali i partenariati pubblico-privati, idonei a integrare le capacità tecniche degli operatori privati con le prerogative pubbliche in materia di protezione delle infrastrutture digitali [27]. Anche i soggetti privati – così come quelli inclusi nel PSNC – sono, infatti, tenuti a predisporre misure organizzative e tecniche sottoposte ad un costante monitoraggio [28], nonché a garantire la tempestiva segnalazione e notifica di eventuali incidenti che possano incidere sugli ICT relativi alle proprie reti, servizi o sistemi informativi identificati come parte del Perimetro, contribuendo in tal modo alla sicurezza complessiva dell'infrastruttura nazionale [29].

---

[23] Decreto legislativo n. 65 del 18 maggio 2018 (Attuazione della 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), in *G.U.* n. 132 del 9 luglio 2018.

[24] D.L. n. 105 del 21 settembre 2019 (Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica) convertito con modifiche in Legge n. 133 del 18 novembre 2019 e più volte modificato anche per un coordinamento con la disciplina dei poteri speciali nei settori di rilevanza strategica (in *G.U.* n. 222 del 21 settembre 2019).

[25] Decreto del Presidente del Consiglio dei ministri n. 131 del 30 luglio 2020 (Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge n. 105 del 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge n. 133 del 18 novembre 2019), in *G.U.* n. 261 del 21 ottobre 2020.

[26] Sul punto già ROSSA S., *Cybersicurezza e pubblica amministrazione*, Napoli 2023, 13; e successivamente LONGO E., *Il diritto costituzionale e la cybersicurezza: analisi di un volto nuovo del potere*, in *Rass. parlamentare* 2024, 319.

[27] In Italia, esempi rilevanti di partenariato sono il CERTFin, promosso da Banca d'Italia e ABI per la condivisione di informazioni sulle vulnerabilità nel settore finanziario, e le collaborazioni tra imprese come Leonardo e il CIOC per lo sviluppo di capacità di difesa cibernetica. Sul punto MACCHIA M.-SFERRAZZO G., *Sicurezza e rischio tecnologico. la funzione di cybersecurity*, in *Dir. amm.* 2025, 109.

[28] Legge n. 90 del 28 giugno 2024 e successivi aggiornamenti (Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici), in *G.U.* n. 153 del 2 luglio 2024.

[29] In questo senso il Decreto del Presidente del Consiglio dei ministri n. 81 del 14 aprile 2021 (Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera

ISSN 2281-3918/2421-2563

3. *Segue*. Il ruolo e le competenze dell'Agenzia per la cybersicurezza nazionale

In tale contesto di consolidamento normativo e di crescente articolazione delle competenze in materia di protezione delle infrastrutture digitali, è emersa l'esigenza di istituire anche in Italia, al pari di quanto già accaduto in altri Stati [30], un soggetto deputato a coordinare le politiche nazionali di cybersicurezza. Per tale motivo con il D.L. n. 82 del 2021 [31] è stata istituita l'Agenzia per la cybersicurezza nazionale (ACN), una struttura avente personalità giuridica di diritto pubblico che, sotto la direzione politica del Presidente del Consiglio dei Ministri [32], si caratterizza per la sua specificità e specialità [33]. L'Agenzia, dotata "di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria" (articolo 5, comma 2) [34], in sinergia con il Consiglio Supremo di difesa [35], pone in essere le attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico (articolo 1, lettera a e b). Più nel dettaglio le corpose funzioni dell'Agenzia possono sussumersi nella predisposizione della strategia nazionale di cybersicurezza e nel coordinamento tra tutti i soggetti pubblici e privati coinvolti [36]; nello sviluppo di capacità preventive e reattive per contrastare incidenti e attacchi informatici, garantendo

---

b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza), in *G.U.* n.138 del 11 giugno 2021, ha distinto tra notifiche necessarie (articolo 3), da effettuare entro sei ore per gli incidenti di cui alla Tabella 1 e entro un'ora per quelli della Tabella 2, e notifiche volontarie (articolo 4, comma 2), ammesse solo se non comportano un onere sproporzionato o eccessivo.

[30] Così in Belgio la *Loi du 18 luglio 2019* ha attribuito i poteri in materia di cibersicurezza al *Centre pour la Cybersécurité Belgique* posto alla dipendenza del Primo ministro; in Francia il *Code de la défense dalla Loi n. 2015-917* ha istituito l'*Agence Nationale de la sécurité des systèmes d'information* che dipende dal Servizio generale della difesa e della sicurezza nazionale del Primo ministro. Infine in Portogallo, il *Centro Nacional de Cibersegurança*, ai sensi dell'articolo 7 della *Lei 46/2018*, opera nell'ambito del *Gabinete Nacional de Segurança*. Sul punto si veda LAURO A., *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *Rivista Gruppo di Pisa* 2021, 533.

[31] Decreto-Legge n. 82 del 14 giugno 2021 convertito con modificazioni dalla L. n. 109 del 4 agosto 2021 (Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale), *G.U.* n. 140 del 14 giugno 2021.

[32] Corte Costituzionale, sentenza n. 86 del 24 maggio 1977, in *https://dejure.it,* secondo cui il coinvolgimento a livello di vertice strategico del Presidente del Consiglio dei Ministri discende dal disposto di cui all'articolo 95 della Costituzione in materia di segreto di Stato e servizi segreti nel cui alveo possono farsi rientrare le questioni legate alla cibersicurezza.

[33] PARONA L., *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale dir. amm.* 2021, 712 il quale sostiene trattarsi di un modello che in parte si distacca da quello stabilito per le agenzie negli articoli 8, 9 e 10 del D. lgs. n. 300 del 30 luglio 1999 (Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge n. 59 del 15 marzo 1997), in *G.U.* n. 203 del 30 agosto 1999.

[34] RICOTTA F.N., *L'architettura di sicurezza cibernetica e l'Agenzia per la cybersicurezza nazionale*, in *Breviario giuridico della cibersicuerzza* Roma 2025, 375; MORONI L., *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi* 2024, 193; SANTANIELLO M., *Monocratic cybersecurity*, in *Rivista di Digital Politics* 2022, II, 305; LAURO A., *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *La rivista Gruppo di Pisa* 2021, 542; RENZI A., *La sicurezza cibernetica: lo stato dell'arte*, in *Giorn. dir. amm.* 2021, 547; CAROTTI B., *Sicurezza cibernetica e Stato Nazione*, in *Giorn. dir. amm.* 2020, 629.

[35] Ai sensi dell'articolo 2 del D. Lgs. n. 66 del 15 marzo 2010 (Codice dell'ordinamento militare), in *G.U.* n. 106 dell'8 maggio 2010, infatti, il Consiglio Supremo di difesa "esamina i problemi generali politici e tecnici attinenti alla difesa nazionale e determina i criteri e fissa le direttive per l'organizzazione e il coordinamento delle attività che comunque la riguardano".

[36] In questa direzione l'Agenzia ha varato un primo Piano strategico nazionale di cybersicurezza 2022-2026 adottato con DPCM del 17 maggio 2022, in *G. U.* n. 127 del 1° giugno 2022 che è in fase di attuazione (con finanziamenti specifici per il 2024-2026) e contiene 5 obiettivi strategici e 38 piani d'azione. Ad oggi sono in atto le consultazioni con gli *stakeholders* per la nuova strategia per il periodo successivo al 2026.

ISSN 2281-3918/2421-2563

la protezione delle infrastrutture digitali [37]; nello sviluppo dell'industria digitale nazionale e nell'efficientamento delle infrastrutture informatiche pubbliche, anche attraverso la certificazione di prodotti, processi e sistemi ICT [38]; nel coordinamento della cooperazione europea e internazionale in materia di cybersicurezza [39]; nel supporto alla ricerca, all'innovazione e allo sviluppo delle competenze scientifiche e professionali nel settore (articolo 7 D.L. n. 82 del 2021) [40] e, non da ultimo, nell'elaborazione della produzione normativa di settore [41]. Negli ultimi anni, poi, le attribuzioni dell'ACN sono state progressivamente estese e potenziate tramite l'istituzione del Centro nazionale di crittografia (CNC) che svolge il ruolo di centro di competenza nazionale per la crittografia in ambito non classificato, con l'obiettivo di promuovere l'adozione di tecnologie crittografiche avanzate, sviluppare algoritmi e standard, e rafforzare l'autonomia tecnologica italiana a protezione delle infrastrutture critiche, delle Pubbliche Amministrazioni e del settore produttivo. Il CNC si occupa, inoltre, della diffusione di linee guida, della certificazione dei prodotti, della ricerca con le università e della valorizzazione della crittografia anche in tecnologie emergenti, come la *blockchain*, riducendo la dipendenza da soggetti extra-europei [42]. In tal modo, il CNC si configura come un centro di eccellenza nazionale, rafforzando le competenze tecniche e organizzative dell'Agenzia e consolidando la capacità dello Stato di tutelare le infrastrutture digitali e l'interesse statale nel cyberspazio.

4. La disciplina delle misure di sicurezza nel trattamento dei dati personali tra GDPR e Codice della privacy

Sebbene la prevenzione e la gestione del rischio cibernetico rivestano un ruolo centrale sia a livello europeo che nazionale, l'aumento e la crescente diversificazione degli attacchi informatici [43] mostrano

[37] L'Agenzia svolge tale funzione tramite il CSIRT *(Computer Security Incident Response Team)* un gruppo di esperti in sicurezza IT incaricato del monitoraggio e della gestione degli incidenti informatici, dell'emissione di allerte e dell'assistenza in situazioni di crisi, le cui azioni si suddividono in *Incident Response, Proactive Activities e Reattive Activities*.

[38] L'Agenzia svolge il ruolo di Autorità nazionale di certificazione ed ha il compito di verificare la conformità dei prodotti, dei servizi e dei processi TIC (acronimo per le Tecnologie per l'informazione e la comunicazione, o "ICT" in inglese) agli standards europei di certificazione, assicurando che i fornitori di tali tecnologie stabiliti nel territorio italiano si conformino agli standards produttivi comunitari.

[39] L'Agenzia quale Centro Nazionale di Coordinamento (lett. a) si inserisce nella rete di centri nazionali di coordinamento al fine di assistere il Centro di competenza europeo nell'assolvimento della sua missione e nel conseguimento dei suoi obiettivi. L'Agenzia si connette anche ai centri transnazionali, in un sistema che fa dell'interdipendenza uno dei suoi tratti caratteristici (artt. 5-6 del Regolamento (UE) 2021/887).

[40] L'Agenzia promuove la partecipazione italiana a progetti e iniziative dell'Unione Europea e internazionali inclusi quelli in collaborazione con la NATO e con l'Agenzia europea per la difesa (lett. t). Essa, inoltre, ferme restando le competenze del Ministero degli affari esteri e della collaborazione e internazionale, stipula accordi bilaterali o multilaterali con istituzioni, enti e organismi esteri, anche mediante il coinvolgimento del settore privato e industriale (lett. s).

[41] L'articolo 1 lettera p) attribuisce all'Agenzia il potere di esprimere pareri non vincolanti su strategie normative e regolamentari in materia di cybersicurezza, al fine di garantire un quadro giuridico nazionale coerente e aggiornato. Tale funzione si estende anche alle *policy* applicabili a soggetti pubblici e privati ed è coerente con il ruolo di coordinamento dell'Agenzia a livello europeo e internazionale, valorizzando l'integrazione di orientamenti, prassi e standard internazionali (così FORGIONE I., *Il ruolo strategico dell'agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in *Dir. amm.* 2022, 4, 1113).

[42] Sul punto la Legge n. 90 del 28 giugno 2024, *cit*., definisce un rafforzamento delle misure di sicurezza dei dati tramite l'utilizzo della crittografia. In questo contesto, presso l'Agenzia per la cybersicurezza nazionale è istituito il Centro nazionale di crittografia, mentre alle strutture responsabili delle attività di cybersicurezza nelle pubbliche amministrazioni sono affidati i compiti di verifica dei programmi, delle applicazioni informatiche e delle comunicazioni elettroniche, conformemente alle linee guida sulla crittografia adottate dall'Agenzia in collaborazione con l'Autorità garante per la protezione dei dati personali.

[43] Il fenomeno del *cybercrime* si presenta oggi con forme estremamente diversificate, riflettendo la crescente complessità e

ISSN 2281-3918/2421-2563

che i sistemi di sicurezza predisposti, comprese le tecniche di filtraggio dei contenuti adottate dalle piattaforme VLOP [44], non sono sempre sufficienti a impedire condotte lesive – quali violazioni, compromissioni, furto e diffusione dei dati – che minano la sicurezza delle informazioni personali di privati, imprese e soggetti pubblici. Così, il sistema di tutela "*multilivello"* della cibersicurezza si completa, sul piano funzionale, attraverso la responsabilizzazione diretta dei soggetti che trattano dati e gestiscono sistemi informativi, tenuti ad assicurare, in via preventiva e reattiva, quell'adeguato livello di sicurezza riconosciuto come diritto fondamentale dell'individuo già dalla Convenzione di Strasburgo n. 108 del 28 gennaio 1981 [45]. In tal senso il legislatore europeo ha adottato il Regolamento (UE) 2016/679 (GDPR – *General Data Protection Regulation*) [46] che, sostituendo la Direttiva 95/46/CE [47], ha introdotto un quadro normativo uniforme e direttamente applicabile volto a rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati (articolo 1, paragrafo 2) mediante un sistema di obblighi, responsabilità e

---

pervasività delle tecnologie digitali nella vita quotidiana e nelle attività economiche. Tra le condotte più diffuse rientrano l'*hacking* cioè l'accesso non autorizzato a sistemi informatici o reti telematiche, spesso finalizzato al furto di informazioni riservate o al danneggiamento di dati, e la diffusione di *malware*, tra cui virus, *trojan* e *ransomware*, strumenti che compromettono la sicurezza dei dispositivi e possono determinare gravi perdite economiche e operative per individui, imprese e enti pubblici. Particolare attenzione meritano anche le pratiche di *phishing*, volte a ingannare gli utenti per ottenere dati sensibili, come credenziali bancarie o informazioni personali, e il furto d'identità, che consente di appropriarsi della reputazione digitale di una persona per scopi fraudolenti. Un'ulteriore dimensione del *cybercrime* riguarda le forme di molestia e persecuzione *online*, come il *cyberstalking* e il *cyberbullismo*, che determinano un impatto psicologico significativo sulle vittime. Accanto a questi fenomeni, emergono forme più sofisticate e strategiche di illeciti, come il cyberspionaggio, finalizzato all'acquisizione di informazioni riservate a scopi industriali o politici, e l'estorsione *online*, spesso veicolata attraverso *ransomware*, con richieste di pagamento per il ripristino di dati compromessi. Anche la violazione del copyright e la pirateria digitale rappresentano una dimensione significativa del cybercrime, che coinvolge la protezione della proprietà intellettuale e la responsabilità civile dei soggetti che ne traggono vantaggio indebitamente (sul punto CORASANITI G., *Strategie di contrasto al ransoware e nuove frontiere della criminalità informatica*, in *Dir. informazione e informatica* 2025, 19).

[44] Secondo quanto disposto negli articoli 34, 35 e 36 dal Regolamento UE 2022/2065 del 19 ottobre 2022 sui servizi digitali, in *https://eur-lex.europa.eu.)* "le piattaforme *online* di dimensioni molto grandi" (VLOP) devono mettere in atto sistemi algoritmici che impediscano *ab initio* "la diffusione di contenuti illeciti attraverso i loro servizi". Questa pratica di filtraggio ha spesso prodotto risultati ridicoli come la cancellazione da internet di Madonne che allattano, putti, dipinti e sculture di Venere, città e persone il cui nome rientrava nel vocabolario dei termini politicamente scorretti di Facebook (*Contenuti degli editori e standard della community di Facebook*, *in https://www.facebook.com/business*), o la sospensione della posta elettronica o di altri servizi di comunicazione personale a causa del rilevamento di messaggi e fotografie ritenuti inappropriati (ARMIJO E., *Speech regulation by algorithm*, in *30 William & Mary Bill of Rights Journal* 2021, 245).

[45] L'articolo 1 della Convenzione di Strasburgo sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (con il suo Protocollo emendativo del 10 ottobre 2018 e ratificato dall'Italia il 5 marzo 2019 in *https://rm.coe.int.*) precisa che scopo della *Convenzione "è quello di garantire ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano ("protezione dei dati")*". Essa ha, inoltre, prescritto l'adozione di misure di sicurezza adeguate per proteggere i dati registrati nei casellari automatizzati dalla distruzione o perdita accidentale, nonché dall'accesso, dalla modifica o dalla diffusione non autorizzata (articolo 7). Sul punto si vedano: MOROZZO DELLA ROCCA P., *Gestione di banche-dati e problemi della responsabilità civile*, in *Legal. giust.* 1988, 338 MIRABELLI G., *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf. inform.* 1993, 326; BUTTARELLI G., *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Milano, 1997, 18.

[46] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (Regolamento generale sulla protezione dei dati), in *https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679).*

[47] La Direttiva n. 95/46/CE del Parlamento europeo e del Consiglio dell'Unione Europea sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali (in *G.U.* n. L281 del 23 novembre 1995, 31), diversamente dalla Convenzione di Strasburgo, qualificava la sicurezza dei dati come un obbligo di condotta a carico del responsabile del trattamento, imponendo l'adozione di misure tecniche e organizzative adeguate ai rischi e alla natura dei dati (articolo 17, paragrafo 1), al fine di proteggerli da accessi non autorizzati, perdite, distruzione o trattamenti illeciti, prevedendo inoltre la designazione di incaricati che offrissero garanzie sufficienti (articolo 17, paragrafo 2).

ISSN 2281-3918/2421-2563

controlli incentrato principalmente sui soggetti titolari del trattamento. Il Regolamento, recepito in Italia con il Decreto legislativo 101/2018 che ha adeguato il Codice Privacy italiano (D. Lgs. 196/2003) alle norme europee, pur permettendo la libera circolazione delle informazioni digitali [48], stabilisce che il "trattamento dei dati personali" [49] possa avvenire solo dopo che il titolare dello stesso abbia fornito all'interessato un'adeguata informativa [50] e ne abbia ottenuto il consenso [51]. I dati personali raccolti esclusivamente per finalità determinate, esplicite e legittime, ai sensi dell'articolo 5 GDPR, devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato; ulteriormente trattati in modo non incompatibile con le finalità esplicitate (limitazione della finalità); adeguati, pertinenti e limitati a quanto necessario rispetto agli scopi perseguiti (minimizzazione dei dati); esatti e, ove necessario, aggiornati (esattezza); conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione); nonché trattati in modo da garantire un'adeguata sicurezza dei dati personali, anche mediante misure tecniche e organizzative idonee a proteggerli da trattamenti non autorizzati o illeciti e da perdita, distruzione o danno accidentali (integrità e riservatezza). Particolari cautele circondano, poi, il trattamento di quei dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici volti a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (articolo 9 GDPR; articoli 2 *sexies* e 2 *septies* Codice privacy), i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (articolo 10 GDPR; articolo 2 *octies* Codice privacy). Questi, infatti, possono essere trattati solo in presenza del consenso esplicito dell'interessato, della presenza di obblighi previsti dalla legge, della superiore tutela di interessi vitali o di finalità di rilevante interesse pubblico (articolo 9, paragrafo 2, GDPR) [52]. Il rispetto dei suddetti principi e delle previste cautele impone al titolare del trattamento (o, se nominato, al responsabile del trattamento) l'adozione di specifiche misure di responsabilizzazione e di sicurezza volte a prevenire accessi non autorizzati, alterazioni, perdite o divulgazioni illecite di dati personali (articolo 32 GDPR). Il Regolamento riconosce, infatti, in capo al titolare del trattamento la necessità di adottare un approccio proattivo nella gestione dei rischi, in conformità al principio di *accountability* sancito dagli articoli 5, paragrafo 2, e 24 del GDPR, garantendo così la tutela dei diritti e delle libertà degli interessati.

---

[48] Lionello L., *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Dir. comm. internazionale* 2021, 675.

[49] Per trattamento ai sensi dell'articolo 4, paragrafo 1 n. 2 del GDPR, si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

[50] Ai sensi dell'articolo 12 GDPR tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli 15 a 22 e all'articolo 34 relative al trattamento devono essere concise, trasparenti e chiare, soprattutto qualora destinate i minori, fornite per iscritto o con mezzi elettronici, e, su richiesta, anche oralmente previo accertamento dell'identità dell'interessato.

[51] Il consenso, ai sensi del combinato disposto degli articoli 4 (paragrafo 1 n. 11), 6 (paragrafo 1 lettera a) e 7, deve essere manifestato liberamente, inequivocabilmente e specificamente in riferimento ad un trattamento chiaramente individuato anche nelle finalità.

[52] L'articolo 9 statuisce che il divieto di trattamento non si applica quando: l'interessato ha dato consenso esplicito; il trattamento è necessario per obblighi contrattuali, diritto del lavoro, sicurezza sociale o tutela di interessi vitali; il trattamento è effettuato da organizzazioni senza scopo di lucro per fini specifici con dati dei soli membri; i dati sono resi pubblici dall'interessato; il trattamento serve a difendere diritti in sede giudiziaria; è necessario per interesse pubblico, sanità, medicina preventiva o ricerca scientifica, garantendo sempre proporzionalità e misure adeguate a tutela dei diritti fondamentali.

ISSN 2281-3918/2421-2563

5. Gli obblighi e le responsabilità del titolare e del responsabile del trattamento

Da quanto detto emerge chiaramente che la prospettiva attraverso cui esaminare i doveri di condotta del titolare del trattamento non deve essere solo quella della riparazione dell'illecito ma, *ex ante*, quella della prevenzione del danno mediante un approccio fondato sul rischio e, comunque, tale da permettere di individuare e valutare la pericolosità dei singoli trattamenti effettuati. Così, il titolare del trattamento è tenuto ad adeguare le misure tecniche e organizzative da adottare allo stato dell'arte in materia, tenendo conto dell'evoluzione tecnologica e delle conoscenze tecniche disponibili (articolo 32 del Regolamento (UE) 2016/679) [53]. Tali misure che non possono essere definite mediante il ricorso a soluzioni meramente standardizzate (quali la pseudonimizzazione [54] o la cifratura dei dati personali [55]), devono, piuttosto, essere calibrate in funzione del rischio concreto per i diritti e le libertà degli interessati, avuto riguardo alla probabilità e alla gravità dei potenziali impatti (articolo 24 GDPR). Una siffatta valutazione deve, in ogni caso, prescindere da mere considerazioni di carattere economico, poiché l'elevato onere finanziario delle misure di sicurezza non può essere invocato in senso deresponsabilizzante né assunto quale esimente rispetto agli obblighi gravanti sul titolare [56]. Il titolare del trattamento che non adempie ai propri doveri può essere ritenuto responsabile per i danni patrimoniali e non patrimoniali subiti dagli interessati a causa del trattamento non conforme (articolo 152 Codice privacy). Oltre alla responsabilità civile verso gli interessati, il titolare del trattamento è soggetto alla vigilanza e al controllo dell'Autorità Garante per la protezione dei dati personali (articolo 77 e ss. GDPR e artt. 141 e ss. Codice privacy) che può imporre provvedimenti correttivi, ammonimenti e irrogare sanzioni pecuniarie proporzionate alla gravità della violazione e alla natura dei dati trattati (articoli 83 e 84 del GDPR) [57].

Ove lo ritenga necessario, il titolare del trattamento può procedere alla designazione di un responsabile del trattamento, conferendo a quest'ultimo un ruolo strumentale e operativo nella gestione dei dati [58]. Questi, secondo le istruzioni fornitegli dal titolare del trattamento (articolo 28, paragrafo 3, lett. c), è tenuto a coadiuvarlo nella gestione dei rischi adottando misure tecniche e organizzative idonee a

---

[53] Così Tosi E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR*, Milano 2019, 37, secondo cui il regolamento comunitario "è informato da un generale principio di elasticità in base al quale gli obblighi si comprimono od espandono al massimo a seconda del rischio e gravità correlati al trattamento dei dati e della struttura organizzativa: lascia, dunque, maggiore discrezionalità al titolare del trattamento nel decidere attraverso quali modalità adeguate tutelare i dati — modello operativo flessibile — abbandonando ad esempio il concetto generale ed astratto — modello operativo rigido — di misure minime di sicurezza e di precetti vincolati con scadenze e adempimenti indifferenziati per tutti i destinatari dell'obbligo".

[54] Ai sensi dell'articolo 4, n. 5, del GDPR per pseudonimizzazione si intende "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

[55] La cifratura, ex articolo 34, comma 3, è quella misura "destinata a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi".

[56] Bravo F., *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in Aa.Vv., *I dati personali nel diritto europeo* a cura di Cuffaro-D'Orazio-Ricciuto, Torino, 2019, 782; Mollo F., *Gli obblighi previsti in funzione di protezione dei dati personali*, in Aa.Vv., *Persona e mercato dei dati. Riflessioni sul GDPR* a cura di Zorzi Galgano, Milano 2019, 25.

[57] Il rispetto delle regole relative al trattamento dei dati personali è anche presidiato da sanzioni penali ai sensi degli articoli 167 e ss. del Codice privacy.

[58] La designazione può avvenire attraverso la stipulazione di un contratto tra il titolare e in responsabile del trattamento oppure, in alternativa, attraverso un semplice atto di nomina (articolo 28, paragrafo 3, GDPR). Il contratto o l'atto possono essere stipulati in forma scritta ma anche in formato elettronico (articolo 28, paragrafo 9, GDPR).

ISSN 2281-3918/2421-2563

prevenire accessi non autorizzati, perdite, alterazioni o divulgazioni illecite (articolo 32 GDPR)[59]. Il titolare del trattamento è, quindi, tenuto a garantire la corretta applicazione del Regolamento anche quando le operazioni siano eseguite dal responsabile del trattamento. Egli può liberarsi da responsabilità solo se il responsabile del trattamento abbia occultato la propria condotta o abbia impedito al titolare o a chi operi per suo conto di vigilare sul proprio operato[60].

Sebbene il responsabile del trattamento non sia gravato da un obbligo diretto di *accountability* analogo a quello del titolare, egli può, tuttavia, rispondere direttamente dei danni patrimoniali o non patrimoniali subiti dagli interessati qualora violi le obbligazioni specificamente poste a suo carico dal Regolamento. Ciò avviene, ad esempio, quando non si conformi alle istruzioni ricevute dal titolare o adotti misure di sicurezza tecniche e organizzative inadeguate o insufficienti (articolo 28, paragrafi 3-10, GDPR)[61]. Una responsabilità diretta può, altresì, configurarsi qualora il responsabile, pur essendo tenuto a documentare le misure di sicurezza adottate per conto del titolare (articolo 30, paragrafo 2, lettera b), ometta di compilare il registro delle attività di trattamento ovvero di esibirlo all'autorità di controllo (articolo 30, paragrafo 2, lettera d, GDPR). Analogamente, tale responsabilità può sorgere nel caso in cui egli, venuto a conoscenza di una violazione dei dati personali (*data breach*), ometta di informare tempestivamente il titolare del trattamento (articolo 33, paragrafo 2, GDPR). In tali casi, alla responsabilità aquiliana del responsabile del trattamento si affianca una responsabilità contrattuale verso il titolare[62]. Infatti, se il rapporto tra titolare e responsabile del trattamento è regolato da un contratto, la violazione degli obblighi in materia di sicurezza può comportarne la risoluzione *–ope iudicis o ex lege-* e il conseguente diritto del titolare al risarcimento dei danni[63]; qualora, invece, l'incarico sia stato conferito mediante atto di designazione, la stessa violazione può determinare la revoca dell'incarico fiduciario, restando comunque ferma la facoltà del titolare di agire nei confronti del responsabile per ottenere il risarcimento dei danni subiti (art. 1723 c.c.).

Infine, quando un responsabile del trattamento ricorra ad un altro responsabile per l'esecuzione di specifiche attività di trattamento, su quest'ultimo gravano, mediante contratto o altro atto giuridico, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento. Qualora il secondo responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile principale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile (articolo 28, paragrafo 4, GDPR).

---

[59] Bocchini R.-Genovese A., *Il contratto di outsourcing*, in Aa.Vv., *I contratti di somministrazione di servizi* a cura di Bocchini-Gambino, Torino, 2011, 159.

[60] Gambini M., *Principio di responsabilità e tutela aquiliana dei dati personali*, Napoli 2018, 34.

[61] Il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 3 dell'articolo 82 del GDPR, solo se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

[62] Sbordone F.-Troise B., *Il contratto di outsourcing informatico*, in Aa.Vv., *Dei singoli contratti. Leggi collegate*, II, in *Commentario del codice civile* diretto da Gabrielli, Torino, 2016, 355; Riccio G.M., *Data protection officer e altre figure*, in Aa.Vv., *La nuova disciplina europea della privacy* a cura di Sica-D'Antonio-Riccio, Padova 2016, 47.

[63] Mantelero A., *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, in *Dir. informazione informatica* 2010, 673; Pittalis M., *Outsourcing*, in *Contratto impresa*, 2000, 1013; Musella A., *Il contratto di outsourcing del sistema informativo*, in *Dir. informazione informatica* 1998, 882.

ISSN 2281-3918/2421-2563

6. *Segue.* La figura del responsabile della protezione dei dati

L'organizzazione reticolare e multilivello nella gestione e nel trattamento dei dati personali si arricchisce ancora della figura del responsabile della protezione dei dati (*data protection officer* o DPO) che ha il compito di informare e fornire consulenza al titolare del trattamento, al responsabile del trattamento e ai dipendenti coinvolti nelle operazioni di trattamento circa gli obblighi derivanti dal GDPR e dalle altre norme dell'Unione o degli Stati membri. In particolare individua i trattamenti che richiedono un numero maggiore di risorse e tempo, rispetto a quelli concretamente messi in campo e quali i settori per i quali riservare un *audit* interno o esterno; inoltre, sorveglia l'osservanza di tali norme e delle politiche interne in materia di protezione dei dati, compresa l'attribuzione delle responsabilità e la formazione interna del personale o degli amministratori impegnati nel trattamento dei dati personali. Su richiesta, il DPO formula pareri sulla valutazione d'impatto sulla protezione dei dati e ne controlla l'attuazione, coopera con l'autorità di controllo fornendo le informazioni necessarie a ricostruire le attività connesse al trattamento, a valutare le misure di sicurezza adottate e a identificare i soggetti interessati dal trattamento (articolo 39 GDPR) [64].

L'insieme delle prestazioni del DPO –da intendersi non in senso esaustivo poiché è possibile determinare ulteriori compiti in via convenzionale o mediante l'atto di nomina– consente di rilevare che il suo ruolo non sia, dunque, per nulla marginale ma rappresenti un presidio aggiuntivo a tutela dei diritti degli interessati [65]. Questa sua posizione di *tertius inter alios* si riflette sui profili di responsabilità, tanto che l'articolo 82 del GDPR esclude il DPO dai soggetti nei confronti dei quali l'interessato può esercitare un'azione risarcitoria. L'articolo 38 paragrafo 3 del GDPR, infatti statuisce espressamente che "il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti" [66].

7. Il bilanciamento tra sicurezza cibernetica e diritti fondamentali nell'era dell'innovazione tecnologica

L'analisi svolta evidenzia come l'assetto della sicurezza cibernetica si configuri oggi come un sistema complesso, articolato su diversi piani normativi multilivello –internazionale, europeo e

---

[64] Sulla figura del DPO si vedano, solo a titolo esemplificativo: AVITABILE A., *Il data protection officer*, in AA.VV., "*Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*" a cura di Finocchiaro, Torino 2017, 381; FEROLA L, *La "nuova" figura del responsabile della protezione dei dati personali e le sue caratteristiche*, in AA.VV., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018* a cura di Panetta, Milano 2019, 350; SOLINAS C., *La nuova figura del responsabile della protezione dei dati*, in AA.VV., *I dati personali nel diritto europeo* a cura di Cuffaro-D'Orazio-Ricciuto, Torino 2019, 145; TORINO R., *Il responsabile della protezione dei dati (Data Protection Officer),* in AA.VV., *La responsabilità del professionista* a cura di Cuffaro, Bologna 2019, 658; RICCIO G., *Sub Art. 39*, in AA.VV., *GDPR e normativa privacy. Commentario*, a cura di Riccio-Scorza, Milano 2022, 352.

[65] Così BRUTTI N., *Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer*, in AA.VV., *Privacy digitale* a cura di Tosi, Milano 2019, 145, secondo cui il DPO riafferma "la centralità di un'etica societaria della protezione dei dati personali all'interno dell'organizzazione, operando, altresì, per garantire l'ottemperanza di tutti i soggetti alle prescrizioni inerenti al trattamento dei dati personali".

[66] *Contra* RENNA, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civile e previdenza* 2020, 1343, secondo cui "l'allocazione regolamentare dei rischi da illecito non esclude un riequilibrio interno delle conseguenze dannose: in tal senso possono essere configurate azioni di rivalsa, nonché di patti di manleva, sino a giungere alla risoluzione o alla revoca dell'incarico con conseguente pretesa risarcitoria".

ISSN 2281-3918/2421-2563

nazionale– e caratterizzato da una marcata eterogeneità di soggetti coinvolti. Questo assetto si fonda su presupposti comuni, tra cui assumono particolare rilievo la standardizzazione dei processi, la condivisione delle informazioni, il coinvolgimento trasversale di più settori dell'ordinamento e la cooperazione tra soggetti pubblici e privati, tutti elementi che incidono in modo significativo sull'attuazione delle politiche di *cybersecurity*. A questi elementi si aggiunge il progressivo rafforzamento degli aspetti tecnici e operativi connessi alla difesa dei dati, un ambito che, sebbene attualmente dipenda in larga misura da infrastrutture collocate oltreoceano, è oggetto di una strategia di potenziamento a livello unionale. Come si evince, infatti, dal Piano quadriennale 2021-2027, sono previsti ingenti investimenti nello sviluppo di tecnologie digitali strategiche (supercomputer, computazione quantistica, microprocessori, reti in fibra ottica e 5G) con l'obiettivo di rafforzare l'autonomia tecnologica e la resilienza cibernetica dell'Unione europea.

L'insieme degli strumenti normativi, tecnici e organizzativi che compongono l'architettura della sicurezza cibernetica non assume, però, valore in sé, ma si deve configurare come strumentale alla tutela della persona e dei valori fondamentali che ne costituiscono il nucleo essenziale. Anche la protezione delle infrastrutture digitali, dei dati e dei sistemi informativi non risponde esclusivamente a esigenze di efficienza, stabilità o continuità operativa dei sistemi, bensì persegue una finalità più ampia, consistente nel garantire che lo sviluppo tecnologico si svolga in modo coerente con la dignità dell'individuo, il pieno esercizio dei diritti fondamentali (articolo 2 della Costituzione), la libertà di autodeterminazione e di partecipazione consapevole alla vita democratica nello spazio digitale. La sicurezza digitale è, dunque, strumentale affinché diritti quali la riservatezza, la libertà di espressione (articolo 21 della Costituzione), l'autodeterminazione informativa (articoli 13 e 15 della Costituzione) e l'uguaglianza (articolo 3 della Costituzione) possano trovare effettiva tutela. In assenza di adeguate garanzie e di un comportamento digitale orientato a principi etici, le tecnologie digitali rischiano di perdere la loro funzione emancipativa, trasformandosi in strumenti di vulnerabilità per la persona ed esponendola a forme di controllo, abuso, manipolazione o discriminazione difficilmente compatibili con i principi democratici. Ne consegue che l'architettura normativa della *cybersecurity*, pur avversata da alcuni leader del settore tecnologico come Sam Altman ed Elon Musk che privilegiano l'innovazione riducendo i vincoli legislativi, deve essere letta come parte integrante di un modello di *governance* digitale orientato alla tutela della persona e dei valori democratici, volto a prevenire la concentrazione della supremazia tecnologica e strategica in capo a pochi attori privati e a favorire uno sviluppo del mondo digitale più inclusivo. In tale prospettiva, anche gli strumenti di partecipazione digitale e di *e-democracy* (quali ad esempio le piattaforme di consultazione e deliberazione *online*, i sistemi di voto elettronico, gli strumenti di *feedback* e le petizioni digitali, gli *open data* per la trasparenza, le piattaforme collaborative di *policy-making*) si inseriscono in un quadro sistemico di garanzie, nel quale la sicurezza cibernetica rappresenta una condizione necessaria per assicurare l'affidabilità dei processi, la protezione degli individui coinvolti e la legittimazione democratica delle decisioni assunte nello spazio digitale. Solo bilanciando, dunque, innovazione e sicurezza sarà possibile realizzare un sistema digitale resiliente e sostenibile, pienamente coerente con i principi democratici e orientato alla tutela effettiva dei diritti fondamentali degli individui, nel quale il ruolo degli enti preposti alla sicurezza cibernetica e alla governance digitale assume una funzione essenziale di coordinamento, garanzia e responsabilizzazione.

ISSN 2281-3918/2421-2563