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

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0160 • articolo sottoposto a peer review • pubblicato in anteprima il 3 lug. 2024

Federica Resta

Cybersicurezza e protezione dati: un rapporto ambivalente

Il saggio analizza il rapporto tra protezione dati e cybersicurezza, alla luce dell'evoluzione che lo ha caratterizzato. In particolare, la protezione dati è stata inizialmente e tradizionalmente concepita come parametro di legittimità dell'attività investigativa funzionale alla tutela della cybersecurity. Tuttavia questa declinazione del rapporto tra tali due interessi giuridici, in termini antagonisti, ha lasciato di lì a poco emergere una più interessante sinergia. Si è infatti compreso come, sul terreno del rapporto tra sicurezza (anche cibernetica) e protezione dati si giochi una sfida cruciale per la democrazia: quella di coniugare entrambe per essere più efficaci, non meno liberi.

Sicurezza nazionale – Cybersicurezza – Protezione dati – Protocollo di intesa – Violazione di dati personali

Cybersecurity and data protection: an ambivalent relationship

This paper analyzes the relationship between data protection and cybersecurity in light of its evolution. In particular, data protection was initially and traditionally conceived as a parameter of legitimacy of investigative activity functional to the protection of cybersecurity. However, this declination of the relationship between these two legal interests, in antagonistic terms, allowed a more interesting synergy to emerge shortly thereafter. Indeed, it was understood how, on the ground of the relationship between security (including cybersecurity) and data protection, a crucial challenge for democracy is played out: that of combining both in order to be more effective, not less free.

National security – Cybersecurity – Data protection – Memorandum of understanding – Data breach

L'Autrice è dottoressa di ricerca in Diritto penale. Direttrice del Servizio affari legislativi e istituzionali e del Servizio affari legali, coordinatrice della Segreteria di Presidenza del Garante per la protezione dei dati personali

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà,* a cura di Marina Pietrangelo

Sommario: 1. Il contesto. – 2. Sinergie inattese. – 3. Prospettive.

1. Il contesto

Benché non scontata, anzi spesso fraintesa o ignorata, l'interrelazione tra protezione dati e cybersecurity è tuttavia profonda e consolidata.

Questa sinergia è oggi normativamente espressa dal d.l. 14 giugno 2021, n. 82 istitutivo dell'Agenzia per la cybersicurezza nazionale. Esso sancisce, con dato significativo, le forme della specifica cooperazione dell'Agenzia con il Garante (oltre che la sua consultazione), anche mediante protocolli d'intesa, relativi tra l'altro alle notifiche dei *data breach* (protocollo siglato poi nel febbraio 2022).

Questa previsione richiama, tuttavia, uno schema che ha radici molto più profonde ed è il risultato di un percorso che ha condotto alla sinergia tra questi due interessi a partire, però, da una posizione inizialmente, essenzialmente antagonista. La collaborazione tra Garante e Autorità (prima, essenzialmente, il Dipartimento informazioni per la sicurezza - DIS) a tutela della cybersecurity risale, infatti, al 2013 quando, con la direttiva Monti, si è siglato il primo protocollo d'intesa con il DIS. Esso è stato poi, da allora, rinnovato ed esteso alla comunicazione dei *data breach* e indicato, tanto dall'allora Autorità delegata, on. Marco Minniti, quanto dalla Fundamental Rights Agency dell'Ue, esempio di migliori prassi nella declinazione del rapporto tra privacy e sicurezza nazionale. Rapporto, questo, in costante dinamismo, tanto in ragione del mutamento dei rischi da cui proteggere la «Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento» (come recita la l. 3 agosto 2007, n. 124), quanto a causa della vorticosa evoluzione della tecnica, che amplifica quei rischi e incide, profondamente, sul bilanciamento tra libertà e sicurezza.

È significativo che il primo protocollo nascesse con il fine di introdurre garanzie ulteriori rispetto all'accesso sistematico dei servizi per fini, tra l'altro, di cybersicurezza, poco prima loro attribuiti dalla "legge D'Alema" (l. 7 agosto 2012, n. 133).

La protezione dei dati rappresentava dunque, in quest'ottica, il limite esterno o, meglio, il parametro di legittimità dell'esercizio di poteri, quali quelli d'intelligence, funzionali alla tutela della cybersicurezza ma, appunto, potenzialmente lesivi della riservatezza. La cybersicurezza rappresentava, dunque, un bene giuridico, metaindividuale, la cui garanzia avrebbe potuto, potenzialmente, ledere la privacy se non correttamente orientata. Di qui il ruolo della protezione dati come condizione di legittimità di attività, pur incisive, a tutela della cybersicurezza nazionale.

Il protocollo veniva siglato in un periodo di grande enfasi, attribuita dalla CGUE, alla proporzionalità nel rapporto tra sicurezza (di cui la sicurezza cibernetica è componente importante) e protezione dati, culminata nella sentenza *Digital Rights* dell'8 aprile 2014 (Cause riunite C293/12 e C594/12) con cui, un anno dopo il protocollo tra Garante e DIS, si è annullata la direttiva 2006/24, appunto per violazione del canone di proporzionalità per quanto riguarda la *data retention*. E l'esigenza di un controllo sul trattamento di dati (anche personali) a fini di sicurezza nazionale, nella sua declinazione di sicurezza cibernetica, è stata soddisfatta perché nel nostro ordinamento, sin dal 1996, la sfera della sicurezza nazionale non è stata sottratta all'ambito applicativo della disciplina di protezione dati, con anzi una previsione innovativa che esclude l'opponibilità del segreto al Garante. Si è trattato di una previsione assai lungimirante, in quanto ha promosso soprattutto la diffusione della cultura della protezione dati in un settore, quale quello della sicurezza nazionale, dominato dalla prevalenza delle istanze pubblicistiche incontrando poi, proprio sul terreno della cybersecurity, significative affinità.

2. Sinergie inattese

Se, dunque, la protezione dati nasceva ed era concepita, nel protocollo d'intesa, come parametro di legittimità dell'attività investigativa funzionale alla tutela della cybersecurity, questa declinazione del rapporto tra tali due interessi giuridici, in termini antagonisti, ha lasciato di lì a poco emergere una più interessante sinergia. Si è infatti compreso come sul terreno del rapporto tra sicurezza (anche cibernetica) e protezione dati si giochi una sfida cruciale per la democrazia: quella di coniugare entrambe per essere più efficaci, non meno liberi.

Proprio il protocollo e l'esigenza, emersa durante la sua attuazione, di proteggere i dati e i sistemi quale presupposto indispensabile per la sicurezza dello spazio cibernetico ci hanno dimostrato, infatti, quanto il rapporto tra protezione dati e cybersecurity viva di sinergie prima – e più ancora – che di antagonismi. La formale sanzione di questa consapevolezza si è avuta nel 2019, quando con un nuovo protocollo tra Garante e DIS si sono normate specifiche procedure per l'informazione del secondo da parte del primo, in ordine a *data breach* che integrino anche violazioni di sicurezza, essendo solo l'inverso normativamente previso. Da questa previsione emerge la consapevolezza, ormai piena, della sinergia e complementarietà delle due discipline e, quindi, dei due settori di attività.

E questo essenzialmente perché la sicurezza dello spazio cibernetico implica anzitutto, inevitabilmente, la protezione dei dati, dei sistemi, delle infrastrutture di cui esso è composto; dell'ecosistema digitale, in una parola.

Pertanto una normativa, quale quella della protezione dati, che faccia della prevenzione dei dati e dei sistemi dal rischio sociale della vulnerabilità telematica il suo fulcro essenziale non può che promuovere quelle condizioni complessive di protezione indispensabili per la sicurezza cibernetica. La responsabilizzazione dei titolari, promossa dal Regolamento UE 2016/679, rispetto al rischio "sociale" derivante da sistemi informatici permeabili rappresenta, in questo senso, una risorsa preziosa (anche di tipo reputazionale) e, non a caso, valorizzata anche dalla normativa in materia di cybersecurity. Per altro verso, la garanzia, promossa dalla disciplina di cybersicurezza, di condizioni complessive di sicurezza, resilienza, affidabilità dell'ecosistema digitale anche, come recita il d.l. 82/21, in funzione della sicurezza nazionale, non può che agevolare la riservatezza dei flussi informativi cui mira la disciplina di protezione dati. E l'evoluzione delle due discipline, con lo snodo del 2016 per la direttiva NIS 1 (2016/1148), ora sostituita dalla NIS 2 (2022/2555) e il Regolamento UE 2016/679 – Regolamento generale sulla protezione dei dati, ha valorizzato ancor più questa sinergia, come sottolineato dal Presidente del Garante.

Il legislatore europeo ha anzi instaurato una significativa simmetria tra protezione dati e sicurezza cibernetica, particolarmente evidente in alcuni istituti che accomunano il Regolamento e la direttiva NIS 1, la NIS 2, fino poi al *Cybersecurity Act* (2019/881).

Così l'obbligo, per gli Stati membri, di provvedere affinché operatori di servizi essenziali e fornitori di servizi digitali adottino – pena rilevanti sanzioni – misure di sicurezza adeguate ai rischi del settore era stato mutuato dalla disciplina di protezione dati sin dalla direttiva 95/46 e ulteriormente rafforzato con il Regolamento, secondo un approccio fondato sul rischio cui corrisponde l'adozione di misure adeguate.

Quest'affinità percorre anche il *Cyber Resilience Act* (approvato definitivamente il 12 marzo 2024), rispetto al quale, ad esempio, il parere n. 23 del 2022 del Garante europeo per la protezione dei dati suggeriva di includere i criteri di sicurezza previsti in materia di protezione dati all'interno dei requisiti essenziali di sicurezza per l'immissione nel mercato dei prodotti digitali, includendovi anche le garanzie di *privacy by design*. E questo, anche considerando che il Regolamento generale sulla protezione dei dati non si rivolge ai produttori.

La stessa idea – promossa dal Regolamento generale sulla protezione dei dati – della garanzia *by design* – da realizzarsi cioè sin dalla progettazione dei dispositivi e dei sistemi – non è affatto estranea alla "filosofia" delle due direttive NIS e, poi, ancor più, al *Cyber Resilience Act*. Essa, infatti, concepisce la sicurezza informatica come un fattore che sul piano logico e cronologico non può considerarsi eventuale o successivo, ma deve "nascere" contestualmente al trattamento.

Di qui l'approccio preventivo di entrambi i plessi normativi (con obblighi di gestione del rischio estesi, con la direttiva NIS 2, a tutta la *supply chain*) e la responsabilizzazione – comune a entrambi – degli operatori, per i quali la protezione dei dati

e dei sistemi diviene un vero e proprio fattore di accountability e di competitività.

Affine è anche il ruolo svolto dalle certificazioni nel complessivo approccio preventivo, comune ad entrambi i plessi normativi.

Comune a entrambe è poi l'istituto della notificazione di eventi pregiudizievoli, volta a consentire – pena l'irrogazione di elevate sanzioni – l'intervento delle autorità rispettivamente competenti secondo tempistiche stringenti (con anche la previsione di un "preallarme" nel caso degli incidenti di sicurezza). Anche in tal caso la disciplina d cybersecurity riprendeva un istituto, quale quello della notificazione di *data breach*, consolidato nel settore della protezione dati in quanto, essendo stato introdotto settorialmente dalla direttiva 2009/136, è stato poi esteso dal Regolamento generale sulla protezione dati alla generalità dei titolari.

L'interrelazione tra cybersecurity e protezione dati è talmente forte rispetto all'istituto dei *breach* (che spesso integrano tanto violazioni di sicurezza quanto di protezione dati), come appunto detto, da aver fondato l'esigenza di specifici protocolli d'intesa tra Garante, appunto e autorità competenti in materia di cybersicurezza (dopo il d.l. 82/21, l'Autorità per la cybersicurezza nazionale).

Anche il recente disegno di legge sulla cybersicurezza, approvato definitivamente il 19 giugno 2024, prevede una significativa sinergia tra le competenze del Garante per la protezione dei dati e quelle dell'Autorità per la cybersicurezza nazionale rispetto alla crittografia, per la cui disciplina si prevede infatti una reciproca consultazione dei due organismi.

3. Prospettive

Tale complementarietà tra protezione dati e sicurezza cibernetica non è, del resto, casuale, se si pensa, come sottolineato dal Presidente del Garante, che la protezione dati è stata inizialmente concepita, sin dai tempi della direttiva 95/46, come un bene giuridico che ciascuno Stato membro avrebbe dovuto tutelare adeguatamente per poter entrare nell'area Schengen, in quanto presupposto per la sicurezza dell'area stessa.

Questa concezione in termini di sinergia, tutt'altro che di opposizione, era ovviamente quantomai lungimirante, instaurando un parallelismo significativo tra libertà di circolazione delle persone (e quindi dei dati personali) e sicurezza delle informazioni, a beneficio dei singoli e della collettività, oltre che della democrazia.

E se questa sinergia riguarda essenzialmente gli attori istituzionali, la sfida da vincere oggi è realizzare questa cooperazione anche con i vari soggetti, anche privati, coinvolti nella complessa filiera del digitale: non si può pensare di rendere sicura la supply chain in assenza di una reale responsabilizzazione di ogni suo anello, come peraltro ben dispone la direttiva NIS 2. Se per la cybersecurity si è parlato, a ragione, di bene comune (o pubblico secondo le declinazioni) perché appunto non rivale e non escludibile, ciò comporta anche il necessario coinvolgimento, nell'opera di messa in sicurezza dell'ecosistema digitale, degli operatori a vario titolo incidenti su esso; la cybersecurity esige responsabilità condivise, seppure asimmetriche.

La stessa proposta di *Cyber Resilience Act* valorizza il partenariato pubblico privato in funzione di resilienza, sovranità/indipendenza tecnologica, leadership intesa anche come contrasto della parcellizzazione dei centri di responsabilità e rafforzamento della governance in una dimensione olistica di gestione del rischio.

Inutile dire quanto ciò sia centrale in un contesto di guerra per la prima volta davvero ibrida, di traslazione delle ostilità in quello che è stato definito il sesto dominio, quando la frontiera digitale diviene bersaglio elettivo di atti ostili se e in quanto più vulnerabile di quella tradizionale. L'inclusione del 5G tra le tecnologie soggette al golden power dimostra la consapevolezza di quanto le neotecnologie siano centrali e strategiche anche in termini di difesa.

Bisogna dunque estendere la sinergia sperimentata già tra Garante e Autorità a tutela della cybersecurity a tutti gli attori, pubblici e privati, coinvolti a vario titolo dai processi d'innovazione, tanto più con l'IA, promuovendo partenariati pubblico-privati, enti di ricerca, settori diversi. La complessità del digitale esige un'adeguata articolazione nella governance, tanto più alla luce di innovazioni come il metaverso, l'*Internet of Things* e l'IA. È questa una delle più importanti sfide che si delineano nel prossimo futuro.