Relazione del Responsabile della Protezione dei Dati

Anno 2024

Roma, maggio 2025

BANCA D'ITALIA
EUROSISTEMA

INDICE

1. Quadro generale.

1.1 Scenario e sfide

L'attuale scenario esterno, già segnato da diffusi conflitti di natura geopolitica, si caratterizza per l'intensificarsi di minacce volte a compromettere la disponibilità, l'integrità e la riservatezza del patrimonio informativo, soprattutto in settori strategici per il sistema economico, nonché per la pervasività dell'evoluzione tecnologica, con particolare riferimento alla sempre maggiore diffusione di software di intelligenza artificiale integrati negli oggetti, nelle applicazioni di uso comune e nei processi decisionali.

L'effetto combinato di questi fenomeni, se non opportunamente controllato e mitigato, può costituire una seria minaccia per i diritti e le libertà dei singoli la cui tutela richiede un crescente impegno delle Istituzioni e una maggiore consapevolezza da parte degli individui, come persone e come membri di un'organizzazione, sulle tematiche di protezione dei dati personali.

Il principio di *privacy by design* deve essere affiancato da un'attenta valutazione d'impatto (*Data Protection Impact Assessment* - DPIA), obbligatoria per i trattamenti che possono comportare rischi elevati per i diritti e le libertà degli interessati, soprattutto quando le decisioni vengono prese, anche solo in parte, senza l'intervento umano. L'utilizzo di sistemi algoritmici rende quindi imprescindibile una governance dei dati che assicuri trasparenza, spiegabilità e correttezza nei trattamenti.

L'analisi delle dinamiche più recenti evidenzia come il significativo aumento delle violazioni di dati personali possa essere ricondotto, oltre che all'azione deliberata di attori malevoli che sfruttano vulnerabilità non adeguatamente presidiate insite nei sistemi, anche ai comportamenti posti in essere dagli stessi interessati che, spesso non opportunamente sensibilizzati sui rischi correlati all'uso dei dispositivi tecnologici, contribuiscono inconsapevolmente all'illecita sottrazione dei propri dati personali.

La complessità dello scenario di rischio delineato evidenzia come l'azione di sorveglianza del Responsabile della Protezione Dati (RPD) non possa risultare confinata alla sola verifica della compliance alla normativa delle attività di trattamento dei dati personali ma, in linea con l'evoluzione della frontiera dell'*Information Technology,* debba assumere carattere interdisciplinare, prestando particolare attenzione anche agli aspetti organizzativi e di sicurezza legati alla progressiva digitalizzazione dei processi operativi e alla crescente esternalizzazione dei servizi. In tale contesto, diventa centrale anche la gestione dei fornitori e degli operatori esterni che trattano dati per conto del Titolare del trattamento: è necessario assicurare che i contratti riflettano obblighi chiari in materia di sicurezza, *audit* e tracciabilità, concorrendo a rafforzare il principio di *accountability* del Titolare del trattamento.

Allo stesso tempo, un'efficace tutela della privacy richiede al Titolare del trattamento e all'RPD di "*giocare d'anticipo*" adottando un approccio olistico e proattivo teso a integrare i profili di protezione dei dati personali fin dalle fasi preliminari del ridisegno dei processi operativi da parte delle diverse Strutture di *business* e dell'individuazione delle relative misure di sicurezza, capaci di fronteggiare i nuovi e più complessi fattori di rischio introdotti dall'evoluzione tecnologica. Nell'ottica di una valutazione anticipata va condotta un'analisi approfondita delle circostanze che portano al verificarsi di un c.d. *data breach* che, anche se di scarso rilievo, possono tuttavia risultare sintomatiche di elementi di vulnerabilità nella predisposizione dei presidi di

protezione, in grado di esporre la struttura organizzativa a potenziali incidenti di sicurezza che ne possono compromettere il patrimonio informativo.

In questo quadro nel quale possono emergere minacce prima non identificate, la consapevolezza delle persone sulle tematiche di protezione dei dati personali e i loro comportamenti rappresentano un presidio insostituibile per la mitigazione dei rischi. Per questo, di pari passo con l'innalzamento della resilienza dei sistemi e dei processi, diventa determinante promuovere un'azione formativa continua e adeguata a favore del personale, con l'obiettivo di accrescerne la consapevolezza sui rischi connessi al trattamento di dati personali e di favorire comportamenti sempre attenti.

1.2 Evoluzione del quadro normativo

Gli ultimi anni sono stati caratterizzati da una copiosa emanazione di normative di derivazione europea finalizzate a regolare in modo unitario gli effetti della diffusione delle tecnologie digitali nei diversi settori dell'economia e della società nonché della vita quotidiana[1].

Tale regolamentazione, presentando diverse interazioni con la normativa in materia di protezione dei dati personali, non pregiudica l'applicazione delle disposizioni del Regolamento UE 2016/679 (General Data Protection Regulation - GDPR) e del diritto attuativo nazionale. Inoltre, le basi giuridiche che legittimano l'eventuale trattamento e la circolazione di dati personali restano esclusivamente quelle disciplinate dal GDPR.

Permane peraltro lo iato tra la delimitazione europea delle normative e delle giurisdizioni che regolano la protezione dei dati stessi rispetto alla dimensione extra-europea delle grandi piattaforme digitali di gestione delle informazioni. Inoltre, ulteriori incertezze possono derivare dal diverso rilievo attribuito alla tutela della privacy a livello extra-europeo[2].

---

[1] L'evoluzione tecnologica e la sua applicazione nei diversi settori di attività ha reso necessaria l'emanazione di discipline unitarie per regolare le condizioni di base per: a) condividere i dati nel mercato interno (Reg. UE 2022/868 - Regolamento sulla *governance* dei dati; b) assicurare equità e contendibilità nei mercati del settore digitale nei quali operano grandi imprese che offrono servizi di piattaforma di base (Reg. UE 2022/1925 - Regolamento sui mercati digitali) quali, ad esempio, intermediazione online, browser web, motori di ricerca online, social network, messaggistica e condivisione di video, cloud computing, sistemi operativi; c) promuovere la resilienza operativa digitale nel settore finanziario (Reg. UE 2022/2554 - Regolamento D.O.R.A.); d) offrire servizi digitali a pagamento, a distanza e a richiesta individuale di un utente (Reg. UE 2022/2065 - Regolamento sui servizi digitali relativo a un mercato unico dei servizi digitali); e) usare i dati personali e non personali generati da un prodotto connesso in rete o da un servizio correlato (c.d. Internet of Things o IoT - Reg. UE 2023/2854 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo); f) scambiare su piattaforme di negoziazione le cosiddette "cripto-attività (Reg. UE 2023/1114 relativo ai mercati delle cripto-attività), cioè rappresentazioni digitali di un valore o di un diritto che possono essere trasferite o memorizzate elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga.

[2] In proposito, l'accordo definito nel 2023 "EU-U.S. Data Privacy Framework" (DPF) (Decisione ex art. 45 Reg. UE 2016/679 adottata il 10 luglio 2023), vale a dire l'accordo per il trasferimento dei dati dall'UE verso gli USA che rappresenta lo strumento diretto a regolare i flussi transatlantici di dati personali tra lo Spazio Economico Europeo e gli Stati Uniti, potrebbe essere messo in discussione dai recenti orientamenti della policy statunitense propensa all'adozione di standard meno restrittivi e più favorevoli a una libera circolazione dei dati. Sul punto cfr. l'Intervento di Agostino Ghiglia, componente del Garante per la protezione dei dati personali, "*Dati Usa-Eu, terremoto Trump: ora è rischio caos su diritti e servizi*" nel quale si riporta la notizia che il presidente Trump avrebbe intenzione di chiedere la modifica o addirittura lo scioglimento del *Privacy and Civil Liberties Oversight Board* (PCLOB), organismo indipendente incaricato della sorveglianza sull'attuazione governativa delle politiche, delle procedure, dei regolamenti e delle pratiche di condivisione delle informazioni di intelligence, al fine di garantire la tutela della privacy e delle libertà civili.

1.3 La disciplina dell'intelligenza artificiale.

Il 1° agosto 2024 è entrato in vigore il Regolamento (UE) 2024/1689, *(AI Act*[3]), finalizzato a stabilire regole armonizzate e una disciplina sistematica in materia di intelligenza artificiale (AI), con l'obiettivo di garantirne lo sviluppo sicuro, etico e affidabile, contemperando la tutela dei dati personali con lo sfruttamento del patrimonio informativo per il funzionamento dei sistemi di AI.

Il Regolamento, seguendo un approccio basato sul rischio (c.d. *risk based approach*), classifica i sistemi di intelligenza artificiale sulla base dei potenziali pregiudizi che possano derivare alle libertà e ai diritti fondamentali degli utenti. Da questa classificazione discendono regimi diversi in tema di autorizzazione all'immissione e vigilanza sul mercato, doveri informativi e obblighi di trasparenza nei confronti degli utenti nonché requisiti tecnici minimi per assicurare la costante supervisione umana e la qualità dei dati di addestramento dei sistemi di intelligenza artificiale, così da prevenire risultati (c.d. *output*) affetti da discriminazioni e distorsioni cognitive (c.d. *bias*)[4].

La nuova normativa sull'AI presenta significative aree di intersezione con il GDPR, anche per l'ovvia ragione che l'addestramento e lo sviluppo dei sistemi di intelligenza artificiale, qualora sia effettuato mediante il ricorso a informazioni riferibili a persone fisiche, non fa venir meno l'obbligo che le operazioni di trattamento siano supportate da adeguata base giuridica di legittimazione. Si porrà, pertanto, nell'applicazione concreta delle due discipline, la soluzione di delicati problemi di coordinamento e di bilanciamento di interessi nei seguenti ambiti:

- revocabilità del consenso e possibilità di esercitare i vari diritti dell'interessato (es. accesso, cancellazione, opposizione, portabilità, ecc.) i cui dati siano utilizzati da sistemi di AI;
- raccordo tra la valutazione d'impatto sui diritti fondamentali (*fundamental right impact assessment* - FRIA) cui è tenuto il *deployer* di sistemi di AI "ad alto rischio", prima del loro utilizzo, e la valutazione d'impatto sulla protezione dei dati personali (DPIA), cui è tenuto il Titolare del trattamento, e predisposizione delle correlate misure di mitigazione dei rischi;
- applicazione del cd. diritto di spiegazione, attribuito a coloro i cui dati siano utilizzati da sistemi di AI ad "alto rischio" a fronte del diritto, attribuito dal GDPR a ogni interessato, di conoscere se tali dati saranno oggetto di un processo decisionale automatizzato e il

---

[3] Il Regolamento entrerà in vigore gradualmente. Il 2 febbraio 2025 sono entrate in vigore le norme relative alle pratiche di intelligenza artificiale vietate. Il 2 agosto 2025 entreranno in vigore le disposizioni relative ai modelli di intelligenza artificiale per finalità generali e quelle relative alla *governance* multi-livello tra Commissione Europea (tramite l'Ufficio per l'intelligenza artificiale), i rappresentanti degli Stati Membri e le autorità di controllo e vigilanza dei diversi settori coinvolti. La restante parte del Regolamento, incluse le norme relative ai sistemi di intelligenza artificiale a rischio limitato e alto, entreranno in vigore dal 2 agosto 2026.

[4] In caso di rischio minimo, come per i filtri *spam* della posta elettronica, non è previsto alcun obbligo ai sensi del Regolamento sebbene i fornitori di sistemi di intelligenza artificiale possano adottare volontariamente specifici codici di condotta. In caso di rischio limitato, come per i *chatbot* e i sistemi di intelligenza artificiale generativa, sono previsti circoscritti doveri di trasparenza al fine di informare gli utenti che stanno interagendo con un sistema di intelligenza artificiale. In caso di rischio alto, come per i *software* utilizzati nella diagnosi delle malattie, nella guida autonoma e nell'identificazione biometrica delle persone coinvolte in attività criminali, si applica l'intero complesso di obblighi informativi e requisiti tecnici previsti dalla disciplina in esame. In ultimo, in caso di rischio inaccettabile, come per i *software* utilizzati nella manipolazione cognitivo-comportamentale, nella polizia predittiva, nel *credit scoring* sociale e nell'identificazione biometrica remota in tempo reale, il Regolamento impone un divieto di implementazione, seppur mitigato da talune eccezioni associate alla sicurezza nazionale.

diritto di ottenere l'intervento umano da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Nei primi mesi del 2025, la Banca d'Italia, nella duplice veste di soggetto interessato allo sfruttamento responsabile, corretto ed efficiente di tecnologie e sistemi di IA nonché in relazione alla prospettata attribuzione del ruolo di *Market Surveillance Authority* (MSA) per l'IA, ha creato al proprio interno il Sottocomitato per l'intelligenza artificiale che rappresenta una sede organizzativa trasversale per assicurare una governance unitaria delle iniziative di sviluppo delle diverse funzioni dell'Istituto.

Infine, si segnala che l'Agenzia per l'Italia Digitale ha posto in pubblica consultazione le *Linee Guida per l'adozione, l'acquisto, lo sviluppo di sistemi di intelligenza artificiale nella Pubblica Amministrazione* al fine di dettare principi comuni per la compliance e l'utilizzo pertinente dell'AI.

1.4 L'azione dell'RPD.

Nel 2024 il mandato del Responsabile della Protezione dei Dati[5], diretto alla sorveglianza sull'osservanza della normativa privacy e alla consulenza nei confronti delle strutture e dell'utenza, è stato esercitato per la difesa della riservatezza, dell'integrità e della disponibilità delle informazioni personali.

L'azione dell'RPD si è svolta nel quadro degli orientamenti espressi dal Garante della Protezione dei Dati Personali a livello nazionale e dall'European Data Protection Board (EDPB) a livello europeo, nonché tenendo conto dei risultati degli approfondimenti svolti all'interno del Network Data Protection Officers (DPO) del Sistema Europeo Banche Centrali (SEBC) e del Single Supervisory Mechanism (SSM) nonché della Rete nazionale degli RPD delle Authority[6].

Le priorità di tale azione sono individuate in base al criterio del rischio, mediante la costante ponderazione dei pericoli inerenti al trattamento dei dati personali, considerandone la natura, le finalità, il contesto e l'ambito di utilizzo. In tale ambito è stata riservata una particolare attenzione nei confronti dei pericoli derivanti da condotte esterne malevole e da comportamenti inconsapevoli nella circolazione dei dati personali. A tal fine, d'intesa con il Dipartimento Informatica e con il Servizio Sviluppo delle professionalità, è stata progettata una campagna di sensibilizzazione sugli aspetti di Privacy e Cybersicurezza che coinvolgerà nel corso del 2025 i Capi delle strutture e delle unità di base, i loro sostituti, nonché il restante personale.

---

[5] I suoi compiti sono individuati nell'art. 39 del Regolamento UE 2016/679 (GDPR) e si distinguono in compiti di consulenza, di sorveglianza in materia di protezione dei dati e di collegamento con il Garante per la protezione dei dati personali (Garante *privacy*), autorità di controllo nazionale in materia *ex* art. 51 GDPR.

[6] Il network rappresenta la sede di confronto inter-istituzionale sui temi di protezione dei dati personali ad esso partecipano, oltre all'RPD (coadiuvato dal Nucleo di Supporto), gli RPD dell' Autorità di Regolazione per Energia Reti e Ambiente (ARERA), dell'Autorità di Regolazione dei Trasporti (ART), dell'Autorità Garante della Concorrenza e del Mercato (AGCM), della Commissione Nazionale per le Società e la Borsa (CONSOB), dell'Autorità Nazionale anticorruzione, (ANAC), dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM), della Commissione di Vigilanza sui fondi Pensione (COVIP), della Commissione di Garanzia nei servizi pubblici essenziali (CGSSE), del Garante privacy (GPDP), dell'Istituto di Vigilanza sulle Assicurazioni (IVASS), dell'Agenzia per la Cybersicurezza Nazionale (ACN), della Cassa per i Servizi Energetici e Ambientali (CSEA), dell'Acquirente Unico S.p.a. (AU) e del Garante per l'Infanzia e l'adolescenza; vi prendono parte, in qualità di osservatori, anche gli RPD dell'Istituto Nazionale di Statistica (ISTAT), dell'Agenzia per l'Italia Digitale (AgID) e della Centrale di acquisto nazionale (Consip spa).

2. Le attività svolte nel 2024.

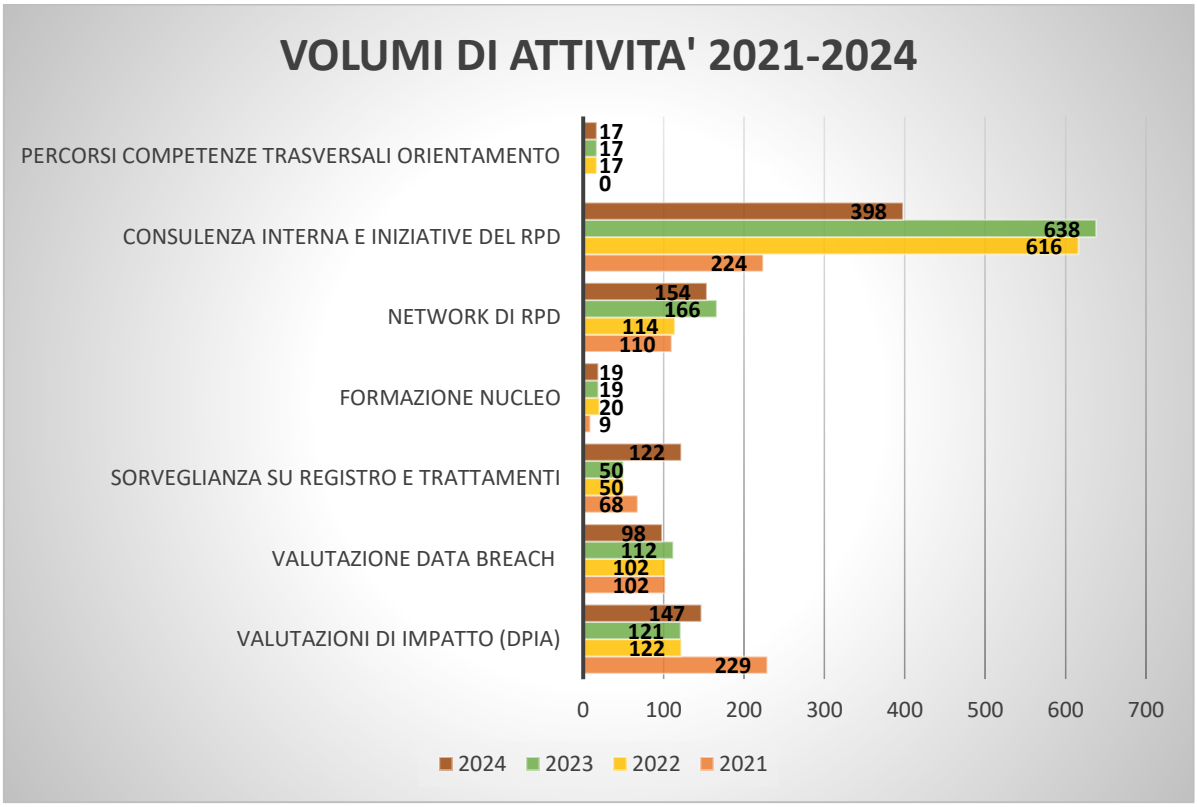
Nell'anno in esame è stata realizzata una modifica organizzativa che, ferma restando la posizione di terzietà e indipendenza, ha collocato l'RPD e la relativa Unità di supporto, all'interno del Dipartimento Pianificazione, Organizzazione e Bilancio.

Tale modifica è finalizzata a rendere più stretta ed efficiente l'interazione con il Servizio Organizzazione che, oltre a svolgere i compiti del Titolare del trattamento dei dati personali, ha la responsabilità di promuovere le linee di sviluppo organizzativo della Banca favorendo l'innovazione e la semplificazione dei processi e delle relative normative. La nuova collocazione dell'RPD, pertanto, rende ancora più effettivo il principio di *privacy by design* in quanto consente di tener conto, sin dalla fase progettuale, delle implicazioni per la protezione dei dati personali derivanti da interventi su assetti, normative e processi di lavoro determinati da cambiamenti organizzativi. Nella stessa ottica si inquadra la partecipazione dell'RPD alle riunioni del Comitato per le Tecnologie dell'informazione.

Nel complesso si è registrato un accresciuto impegno per la sorveglianza sul Registro dei trattamenti, frutto dell'intensificarsi dell'interazione con il Servizio Organizzazione, a fronte di una complessiva riduzione dell'attività di consulenza che, pur evidenziando un'espansione delle attività legate ai lavori di preparazione dell'euro digitale, ha risentito del minore impegno richiesto, rispetto ai due anni precedenti, per la partecipazione ai team di supporto ai progetti vincitori della *Call for proposal* di MI-Hub. Peraltro, nei primi mesi del 2025, con l'avvio della terza *Call,* tale impegno si sta confermando sui livelli degli anni precedenti. Nelle restanti aree di lavoro i volumi di attività sono rimasti sostanzialmente stabili.

Nei grafici seguenti si fornisce la distribuzione delle attività svolte nel 2024 nonché il raffronto tra i volumi di attività registrati nel periodo 2021-2024.

[§] La rappresentazione grafica si riferisce agli "affari trattati" o ai "processi lavorativi svolti" o alle "iniziative completate" o agli "incontri/meeting esterni" effettuati dalla struttura nell'ambito di ciascuno dei compiti affidati alla funzione dell'RPD. La quantificazione di alcune categorie di "attività" è stata effettuata mediante l'elaborazione su dati segnalati in procedura ASTRA.



Il lavoro svolto dall'RPD nei diversi ambiti di competenza è descritto in maniera analitica nei paragrafi che seguono.

2.1 La partecipazione al Network dei DPO del SEBC/SSM.

Nel corso del 2024 negli incontri, in streaming e in presenza presso la Banca di Spagna, del Network dei DPO delle Banche Centrali del SEBC e delle Autorità Nazionali Competenti (NCA) per la supervisione bancaria del SSM sono stati analizzati, con il coordinamento della BCE, principalmente i seguenti temi comuni per le istituzioni interessate:

- le problematiche sorte nell'ambito dei lavori preparatori dell'euro digitale relative alla tutela della *privacy* che, come emerso dalla Consultazione della BCE indetta nel 2020, rappresenta per i cittadini europei il secondo fattore in ordine di importanza dopo la sicurezza;
- le decisioni assunte dall'EDPS sulla base delle analisi condotte sul software di lavoro Microsoft Dynamics 365 adottato dalla Commissione europea e dalla BCE con particolare riferimento alle misure di salvaguardia per assicurare ai dati che transitano al di fuori dell'UE/ European Economic Area (EEA) lo stesso grado di protezione previsto dal GDPR;
- gli accordi per la *Joint Controllership* tra le Banche centrali nazionali e la BCE nella gestione dei dati personali nel contesto della vigilanza prudenziale delle istituzioni creditizie;
- lo scambio di dati personali tra autorità pubbliche nella lotta a corruzione, frodi, antiriciclaggio e contrasto del finanziamento del terrorismo;

- il grado di *compliance* alla protezione dei dati prevista nel GDPR/EUDPR nel Rapporto settembre 2023-marzo 2024 sui Servizi Target, con particolare riferimento agli accordi per la *Joint Controllership* per T2, T2S e TIPS;
- le riflessioni sull'utilizzo dell'AI nelle Istituzioni con riguardo alla regolamentazione europea introdotta con l'*AI Act* (cfr. *supra*) e la prospettiva di conformità al GDPR;
- l'analisi sulle lezioni apprese e gli sviluppi futuri dopo i primi cinque anni di applicazione del GDPR/EUDPR.

2.2 La partecipazione alla rete nazionale degli RPD delle *Authority*.

L'RPD della Banca partecipa alle riunioni del Network degli RPD delle Autorità indipendenti nazionali che rappresenta la sede di confronto inter-istituzionale sui temi di protezione dei dati personali[7].

I principali argomenti trattati, spesso approfonditi con l'ausilio di docenti universitari e funzionari del Garante e di altre Autorità, hanno riguardato molteplici aspetti che coinvolgono in modo costante lo svolgimento dell'attività di sorveglianza e consulenza dell'RPD. In particolare, nel corso delle riunioni tenute con cadenza mensile:

- sono state analizzate le modalità di presidio del rischio *cyber,* con il contributo di riconosciuti esperti della materia in ambito nazionale;
- è stata discussa una pronuncia della Corte di Giustizia Europea[8] relativa a casi di processi decisionali automatizzati, coinvolgenti dati di persone fisiche, finalizzati al *credit scoring*;
- sono stati approfondite con esponenti del Garante privacy alcune problematiche applicative della disciplina sul trattamento dei dati del rapporto di lavoro con il personale dipendente;
- è stata predisposta una rassegna sul ruolo e sulla collocazione organizzativa dell'RPD a oltre 5 anni dal GDPR;
- è stato effettuato un monitoraggio delle criticità nell'applicazione della disciplina sul *whistleblowing* emanata dall'ANAC (in attuazione del d.lgs. n. 24/2023);
- è stata approfondita con l'ausilio di esponenti dell'Agenzia per la Cybersicurezza nazionale la normativa di recepimento della Direttiva Network and Information Systems (NIS2).

Infine, il Network degli RPD ha partecipato alla pubblica consultazione avviata dal Garante privacy sul Documento "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" volto a migliorare la consapevolezza sulle scelte tecniche e organizzative effettuate dai datori di lavoro, con l'obiettivo di assicurare che i metadati raccolti attraverso l'utilizzo della posta elettronica dei dipendenti siano effettuati nel rispetto della normativa sulla protezione dei dati personali.

---

[7] La rete, costituita conformemente alle linee di indirizzo del Garante sull'RPD in ambito pubblico (Provvedimento 29 aprile 2021 n. 186, par. 8) è disciplinata da *Regole di organizzazione e funzionamento del Network degli RPD delle Autorità Amministrative indipendenti* deliberate il 24 settembre 2021.

[8] Sentenza del 7 dicembre 2023 C-634/21.

2.3 Cooperazione e interlocuzione con l'Autorità Garante della privacy.

Nel corso del 2024 è proseguita la cooperazione con l'Autorità Garante della privacy su tematiche di comune interesse grazie alla partecipazione dell'RPD della Banca al Network, coordinato dal Garante, costituito dagli RPD del settore bancario e da quelli di ABI e Federcasse.

Tale Network costituisce una importante sede di confronto per approfondire la conoscenza dei fenomeni di effettiva rilevanza privacy nel comparto bancario e coordinare eventuali iniziative per armonizzare la regolazione delle attività che coinvolgono la protezione dei dati relativi alle persone fisiche.

In tale ambito è in corso un'iniziativa di razionalizzazione dell'informativa privacy destinata alla clientela bancaria, i cui lavori si protrarranno nel 2025. Inoltre, al fine di acquisire informazioni in vista dell'elaborazione di indirizzi in materia di prevenzione del riciclaggio, l'RPD della Banca ha collaborato con il Garante nell'avvio di un'iniziativa che coinvolge l'ABI e gli intermediari bancari con riferimento all'elaborazione di linee di indirizzo privacy nelle attività di contrasto al riciclaggio, nell'ambito dell'utilizzo delle *watchlists* da parte dei "soggetti obbligati".

2.4 Le consultazioni dell'RPD.

L'attività di consulenza è condotta dall'RPD principalmente mediante pareri formali (cfr. par. 2.6 e 2.7) resi obbligatoriamente, ai sensi degli artt. 33 e 35 del GDPR, prima dell'avvio o della modifica di processi strutturati che comportano trattamenti di dati personali (DPIA) nonché a seguito di segnalazioni di incidenti che possono comportare violazioni dei dati personali (c.d. *data breach*).

A questa consultazione formalizzata si affianca, in misura rilevante, l'attività di consulenza sull'applicazione uniforme della normativa privacy che si estrinseca mediante suggerimenti e raccomandazioni, resi in modo informale, in risposta a quesiti o problemi posti dalle Strutture.

Rientra in tale attività di consulenza, l'esame delle clausole *privacy* di accordi o protocolli da perfezionare con istituzioni pubbliche per lo svolgimento di compiti istituzionali e, in particolare:

- una convenzione per la fornitura a una Filiale regionale del servizio di medicina del lavoro da parte della locale Azienda sanitaria, con particolare riguardo alla designazione dell'ASL come Titolare del trattamento dei dati personali archiviati nella procedura SICURWEB, a disposizione del medico competente, incaricato per lo svolgimento delle attività connesse con la sorveglianza sanitaria obbligatoria;
- il rinnovo dell'accordo di collaborazione con l'Istituto per la vigilanza sulle assicurazioni (IVASS), già sottoscritto nell'agosto del 2019, per l'utilizzo da parte di quest'ultima Autorità dei servizi informatici messi a disposizione dall'Istituto;
- le convenzioni in materia di iniziative di formazione del personale con la Consob e l'AGCM.

Inoltre, sono stati forniti raccomandazioni e suggerimenti per la verifica della compliance alla *privacy*:

- per la conservazione dei fascicoli delle procedure di concorso;

- per l'uso delle immagini e per l'acquisizione del relativo consenso, anche alla luce della normativa sul diritto all'immagine;
- nell'ambito della disciplina in tema di obbligo di comunicazione degli investimenti finanziari privati dei supplenti dei membri partecipanti alle riunioni degli organi direttivi della BCE[9];
- delle modalità e della durata della pubblicazione dei provvedimenti sanzionatori irrogati nei confronti di persone fisiche.

Inoltre, l'RPD ha fornito, in via anticipata, contributi alla redazione del testo del "Regolamento recante disposizioni sul trattamento dei dati personali effettuato dalla Banca d'Italia nell'ambito delle attività di supporto all'Arbitro Bancario Finanziario (ABF)", attualmente oggetto di interlocuzione con il Garante, con particolare riguardo all'osservanza della normativa *privacy* con riferimento all'uso dell'AI per il trattamento dei dati personali delle parti coinvolte.

Nel quadro del progetto dell'euro digitale, è proseguito l'impegno dell'RPD e del Nucleo di supporto nell'analisi fornita sugli aspetti connessi alle problematiche *privacy* sia all'High Level Task Force sia ai rappresentanti che seguono il negoziato presso la Commissione europea volto a definire l'impianto normativo della *Proposal for a Regulation on the establishment of the digital euro*.

Infine, l'RPD ha collaborato con il Servizio Organizzazione nell'aggiornamento della clausola di designazione del Responsabile del trattamento ai sensi dell'art. 28 GDPR da inserire nei contratti nei quali il fornitore è incaricato di trattare dati personali di titolarità dell'Istituto.

2.5 La sorveglianza sul Registro delle attività di trattamento

L'attività di sorveglianza sul Registro delle attività di trattamento si estrinseca, principalmente, attraverso il monitoraggio periodico delle informazioni iscritte nel Registro[10] che ha l'obiettivo di verificare la pertinenza, la coerenza, la completezza e l'efficacia della rappresentazione della generalità o di gruppi di trattamenti inseriti dalle Strutture competenti e promuoverne le eventuali rettifiche e integrazioni.

Nel corso del 2024, la nuova collocazione organizzativa dell'RPD e del Nucleo di supporto ha consentito di accrescere l'efficacia e la tempestività dell'attività di sorveglianza per effetto del costante confronto con il Servizio Organizzazione, responsabile della tenuta del Registro. In questo quadro è stata avviata una riflessione congiunta per aumentare la qualità e l'efficienza delle valutazioni effettuate durante l'intero ciclo di vita del dato personale (raccolta, conservazione, utilizzo, condivisione, cancellazione).

Raffrontando la situazione del Registro al 31 dicembre 2024 con quella risultante dalla precedente Relazione, si è rilevato il complessivo aumento dei trattamenti di dati personali (223 a fronte di 209 dell'anno precedente), in prevalenza ascrivibile all'ampliamento delle attività o alla

9 Tale obbligo informativo è previsto dalle disposizioni del "Codice di condotta per le alte cariche delle BCE".

10 La tenuta del Registro è prevista dall'art. 30 del GDPR tra gli adempimenti principali del Titolare (e del Responsabile) del trattamento. Il Registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. Secondo quanto previsto dalle Linee Guida europee (WP Art. 29, *Guidelines* 5 aprile 2017, par. 4.1 e 4.5) per sorvegliare l'osservanza del GDPR, l'RPD conduce con regolarità il monitoraggio del Registro con l'obiettivo di valutare complessivamente l'efficacia informativa dei trattamenti censiti.

crescente articolazione dei processi di lavoro di competenza delle diverse Strutture e delle nuove iniziative di informatizzazione.

Nel complesso si è registrato un miglioramento della qualità informativa del Registro per effetto dell'aggiunta di ulteriori elementi descrittivi del trattamento (informative *privacy*, valutazioni preliminari condotte, indicazione dei responsabili del trattamento, tempi di conservazione).

2.6 Le valutazioni di impatto sulla protezione dei dati (DPIA)

Nel corso del 2024 l'RPD ha fornito il suo parere per 12 *Data Protection Impact Assessment* (DPIA) legati alla realizzazione di progetti informatici o procedure di lavoro oggetto di studio o revisione[11] che, comportando una potenziale esposizione a rischio per i dati personali delle persone fisiche interessate, hanno richiesto di implementare presidi di protezione adeguati. Tra le valutazioni di maggior rilievo si segnalano:

- il progetto per la realizzazione di un sistema unico integrato dei dati aziendali (denominato "Pratico"), volto a integrare gli archivi informativi Astra (rilevazione degli output delle attività svolte dalle Strutture), Siria (informazioni sulla ripartizione delle prestazioni del personale tra le attività svolte dalle Strutture) e ORM (processi di lavoro valutati per la gestione del rischio operativo), al fine di agevolare la descrizione e la misurazione dei fenomeni aziendali nonché l'analisi complessiva sulle *performance* dei processi produttivi;
- la manutenzione evolutiva del prototipo "*knowledge graph* delle imprese italiane", finalizzato a elaborare, attraverso tecniche di analisi del grafo, il flusso informativo estratto dalla base dati di Infocamere fornendo una vista completa dei dati relativi alle imprese italiane e riproducendone gli assetti proprietari e gli eventuali rapporti di tipo familiare tra i soci;
- la revisione della configurazione del sistema di videosorveglianza (TVCC) dell'Istituto, progettato con caratteristiche tecniche e presidi di sicurezza diversi a seconda che la finalità perseguita per il trattamento dei dati personali sia la sicurezza anticrimine (c.d. *security*) ovvero la supervisione di particolari processi operativi;
- la maggiore automazione nella gestione dell'archivio della Centrale di Allarme Interbancaria (CAI), affidata a un *service provider* di elevata affidabilità come responsabile del trattamento dei dati personali di titolarità dell'Istituto, prevedendo la possibilità per le Filiali di interrogare direttamente l'archivio centrale nell'evasione delle istanze di accesso dell'utenza nonché la possibilità, per l'utenza identificata tramite SPID, di effettuare le visure attraverso portale web;
- il rinnovamento, a seguito del mutato contesto delle minacce *cyber* e della progressiva adozione di tecnologie *open source*, dell'infrastruttura a chiave pubblica per rilasciare i

11 L'art. 35 del GDPR prevede che: «*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. ..... Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati* ...». Le valutazioni di impatto si rendono necessarie quando l'acquisizione e la gestione delle informazioni implicano un trattamento di dati personali di rilevanza particolare o su larga scala o con l'utilizzo di tecnologie innovative e in tutte le fattispecie individuate dal Garante *ex* art. 35.4 GDPR (cfr. Provv. n. 467 dell'11 ottobre 2018).

certificati digitali ai dipendenti del SEBC nonché i certificati applicativi utilizzati dai servizi informatici erogati dall'Istituto (*Public Key Infrastructure* -PKI);
- il completamento del progetto "Sistema informativo SNA" attraverso l'implementazione di un nuovo servizio ICT finalizzato a garantire una maggiore automazione e integrazione con gli altri sistemi informativi aziendali per un'efficace gestione dei processi di supervisione antiriciclaggio e di contrasto al finanziamento del terrorismo;
- l'introduzione di un cruscotto informativo per la gestione del personale ("*HR dashboard*"), finalizzato a migliorare l'accessibilità e la fruibilità dei dati personali archiviati e il loro collegamento con il *data warehouse* aziendale, "Sibaris", oggetto di una coerente manutenzione evolutiva.

Inoltre, l'RPD ha fornito un parere sulla modifica del progetto "Portale dei servizi per il personale in servizio e in quiescenza" (PEGASO), finalizzato a realizzare un unico *entry-point* per l'erogazione dei predetti servizi. In tale circostanza è stata validata una semplificazione dell'architettura progettuale prevedendo la possibilità, in alcuni casi e con determinati presidi di sicurezza, di memorizzare temporaneamente sul *cloud* pubblico i dati personali di titolarità dell'Istituto, secondo quanto previsto dalle nuove *policy* aziendali in tema di *cloud* pubblico.

2.7 Le segnalazioni dei *data breach*.

Nel 2024, le potenziali violazioni dei dati personali rilevate e sottoposte alla valutazione dell'RPD (c.d. *data breach*) sono state 48 (a fronte delle 56 registrate nel 2023): su ciascun evento l'RPD ha fornito al Titolare del trattamento il proprio parere sulla qualificazione del fatto segnalato come violazione dei dati personali e sulla ponderazione del conseguente rischio per i diritti e le libertà delle persone fisiche, ai fini delle eventuali determinazioni previste dal GDPR[12].

La valutazione dei rischi derivanti da tali violazioni ha comportato in un caso[13], caratterizzato da una azione dolosa e malevola esterna, la segnalazione all'Autorità Garante prevista dall'art. 33 del GDPR. Per gli altri casi di *data breach* non è stato necessario effettuare la predetta segnalazione, in quanto è stato ritenuto trascurabile il livello di rischio per i soggetti interessati nelle varie fattispecie alla luce delle circostanze fattuali e delle cautele adottate.

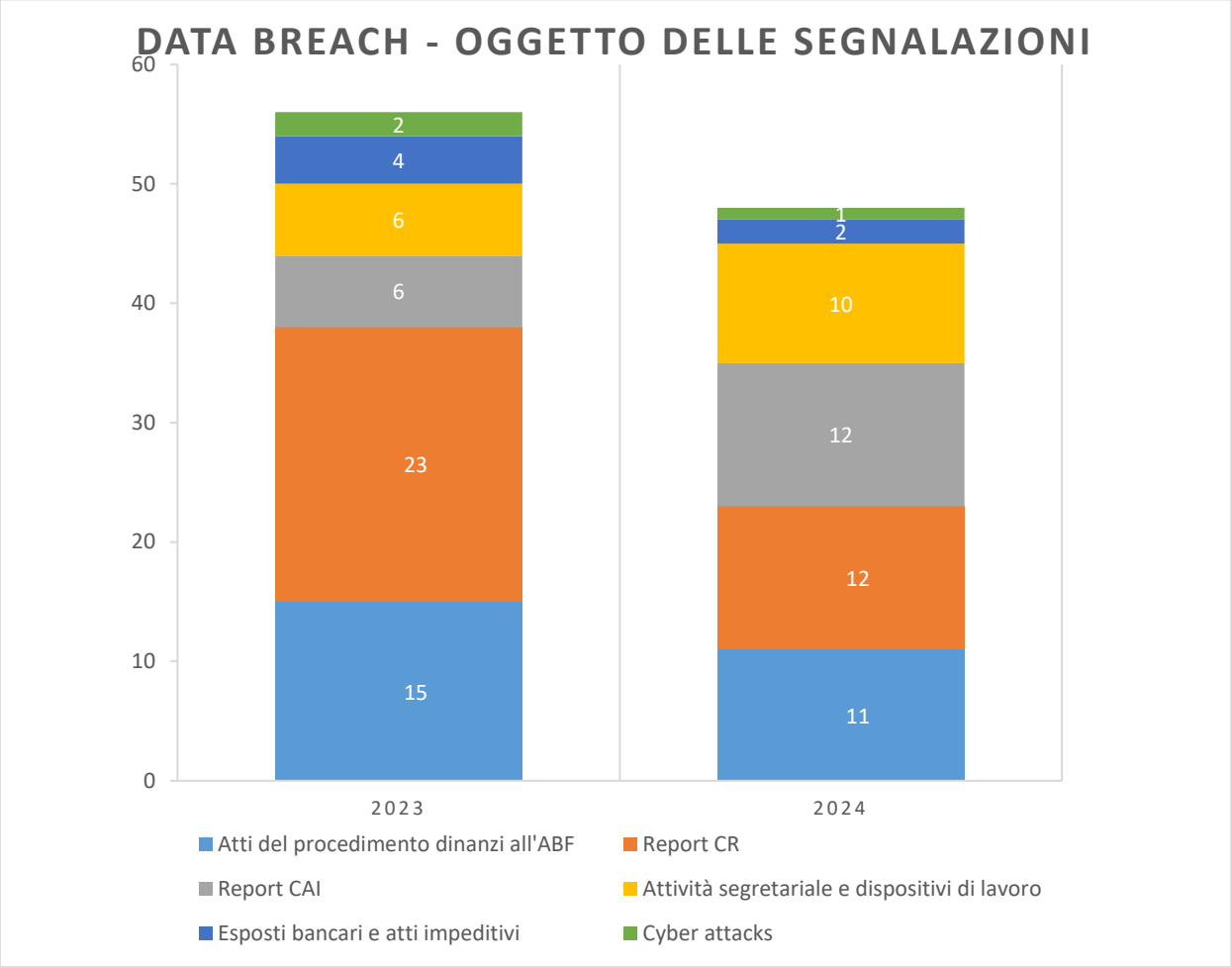
Gli ambiti nei quali si sono concentrate maggiormente le segnalazioni di violazione dei dati personali sono quelli inerenti agli accessi alla Centrale dei Rischi (C.R.) e alla Centrale di Allarme Interbancaria (C.A.I.), nonché quello relativo alla gestione dei procedimenti dinanzi all'Arbitro Bancario e Finanziario (A.B.F.).

Nel grafico seguente vengono posti a raffronto il numero di *data breach* registrato nel 2023 e nel 2024 per ciascun ambito di attività.

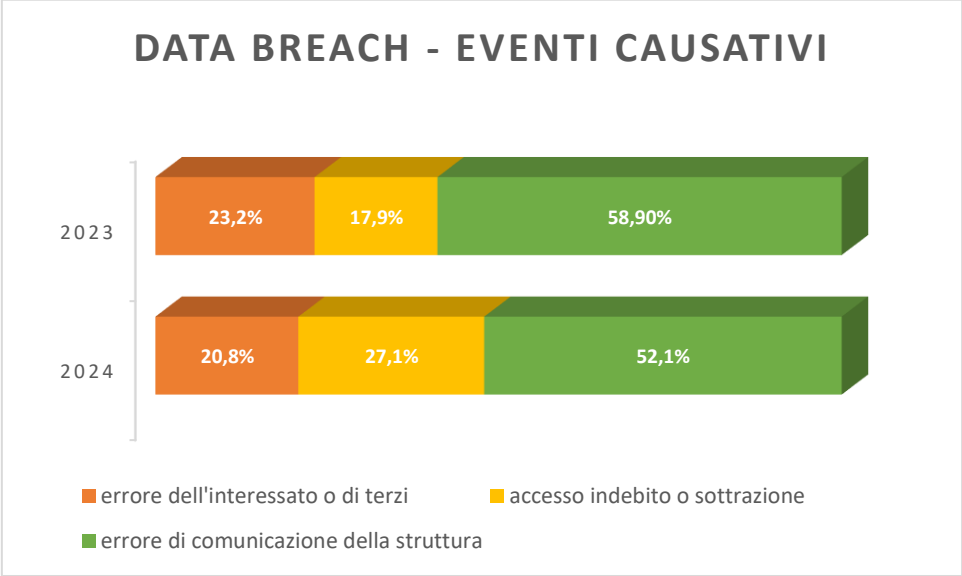
---

[12] L'RPD fornisce al Titolare del trattamento un parere nei casi di perdita, alterazione o sviamento (accidentali o illeciti) di dati personali configurabili come *data breach*. Il GDPR (art. 33), qualora si verifichino i presupposti di un *data breach*, impone al Titolare del trattamento dei dati di darne notifica all'Autorità Garante, entro 72 ore dal momento in cui ne ha avuto conoscenza (salvo giustificazione dei motivi del ritardo, ove la notifica non possa essere effettuata entro tale stringente termine), a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche; qualora, poi, la violazione presenti un rischio elevato per i diritti e le libertà degli interessati, il Titolare del trattamento deve darne comunicazione, senza ingiustificato ritardo, anche agli interessati (art. 34).

[13] Si è trattato di un caso di *cyber attack* a un fornitore di servizi, attraverso lo sfruttamento di una vulnerabilità *zero-day*.



La maggioranza delle violazioni è stata determinata dall'errore operativo nelle comunicazioni da parte delle strutture ovvero a condotte negligenti da parte degli stessi interessati o di terzi. In casi limitati i *data breach* sono imputabili ad atti dolosi commessi da attori malevoli.



2.8 Le altre iniziative dell'RPD.

Nell'esercizio dei propri compiti di sorveglianza sull'applicazione della normativa *privacy*, l'RPD promuove, anche di propria iniziativa, attività dirette a verificare e, ove del caso, adeguare la *compliance* complessiva delle strutture.

A seguito dell'emanazione da parte del Garante privacy di linee di indirizzo per difendere i dati personali pubblicati online da soggetti pubblici e privati dal *web scraping*, e specialmente la raccolta indiscriminata di dati personali effettuata da terzi per addestrare i modelli di AI, sono state riesaminate con l'ausilio della funzione informatica l'adeguatezza delle misure concrete messe in atto, ancorché non obbligatorie, per impedire o, almeno, ostacolare tale raccolta.

Nel quadro delle iniziative di sensibilizzazione sulla privacy, nel mese di dicembre, il Nucleo di Supporto all'RPD ha concorso all'organizzazione di un incontro, in modalità ibrida, presso la Filiale di Catania su "Sicurezza informatica, Trattamento dei dati e riservatezza", durante il quale sono stati esposti i principi della normativa sulla *privacy* e l'importanza di mettere in atto tutte le procedure in grado di limitare i possibili rischi di perdita di integrità, riservatezza e disponibilità dei dati personali nell'ambito delle attività di lavoro.