BANCA D'ITALIA
EUROSISTEMA

Relazione del Responsabile della Protezione dei Dati

Anno 2023

Roma, maggio 2024

INDICE

Introduzione.

Nel 2023 l'azione di consulenza e di sorveglianza del Responsabile della Protezione dei Dati (RPD)[1] ha accompagnato la progressiva transizione digitale dei processi e prodotti dell'Istituto.

La digitalizzazione nel settore pubblico e nel contatto con l'utenza implica la trasposizione di attività e relazioni in un ambiente immateriale nel quale l'evoluzione tecnologica tende a costituire la variabile preponderante da valutare nell'azione di adeguamento alle norme sulla tutela dei dati personali e sulla sicura e legittima circolazione degli stessi.

Diversi sono gli aspetti rilevanti per la protezione dei dati personali:

i) il mondo digitale ha causato un'enorme espansione nella quantità di dati raccolti sia per la connettività dei dispositivi, che ha aumentato il potenziale informativo, sia per la diffusione delle tecnologie relazionali (ad es. mediante il controllo continuo delle attività *online* degli utenti in caso di uso dei *social media* e delle piattaforme di *e-commerce,* che grazie a una copiosa e duratura raccolta di dati ottengono una raffinata profilazione dei comportamenti degli utenti e delle loro preferenze); questo ha reso più difficile, per le persone, comprendere per quale motivo i propri dati vengono utilizzati e soprattutto con quali modalità sono impiegati, trovandosi spesso a doverli conferire senza capire le reali intenzioni di chi li raccoglie;

ii) la complessità della tecnologia digitale ha reso sempre più difficile proteggere adeguatamente i dati personali: con l'intensificarsi del ricorso all'intelligenza artificiale, alle tecnologie a registro distribuito *(distributed ledger technologies)* e alla gestione delle informazioni mediante *cloud* o mediante articolati passaggi di valore (*supply chain*), innumerevoli si rivelano le modalità attraverso cui i dati possono essere compromessi o violati, a partire dalle vulnerabilità del *software* fino alla perdita fisica del dispositivo di archiviazione; come pure la rapidità di evoluzione delle tecniche rende complicato per le aziende e per la Pubblica Amministrazione mantenere il passo con le minacce alla sicurezza dei dati;

iii) la delocalizzazione delle forme moderne di trattamento del dato personale favorisce l'inefficacia delle regole nazionali e sovranazionali e un conseguente indebolimento delle normative di tutela, legate a una dimensione territoriale di applicabilità.

L'attenzione del RPD si concentra sui rischi collegati all'avvento delle nuove tecnologie, alla delocalizzazione e all'internazionalizzazione delle attività, indirizzando la sua azione verso una più articolata conoscenza tecnologica per la valutazione dei rischi *privacy* e per lo sviluppo di sistemi e di applicazioni che assicurino una protezione adeguata fin dalla progettazione.

Nell'anno in rassegna, l'azione del RPD è stata esercitata valorizzando la natura di diritto fondamentale della riservatezza e, in tale contesto, osservando il bilanciamento con la fisiologica necessità di circolazione delle informazioni, che è condizione di trasparenza e di legalità.

[1] I suoi compiti sono individuati dall'art. 39 del Regolamento UE 2016/679 (GDPR) e si articolano in consulenza, sorveglianza in materia di protezione dei dati e collegamento con il Garante per la protezione dei dati personali (Garante *privacy*).

Nella Banca d'Italia questa azione si attua nella convinzione che l'attenzione per il rispetto della *privacy* nella raccolta, nella custodia e nella gestione trasparente e sicura dei dati personali contribuisce a consolidare reputazione e affidabilità.

* * *

1. Il quadro normativo.

L'anno trascorso ha confermato la crescente connotazione sovranazionale del quadro normativo in materia di protezione dei dati personali.

Con l'adozione del Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario[2] sono state poste le basi normative per una valutazione integrata del sistema ICT e dell'assetto *privacy*, sul presupposto della conoscenza degli scenari aziendali effettivi, dove il rischio di incidente informatico coesiste nella maggior parte dei casi con quello di violazione dei dati personali.

La diffusione degli archivi di informazioni decentralizzati basati su *distributed ledger technologies* ha indotto il legislatore europeo a definire un quadro regolamentare degli asset digitali e delle criptovalute, nel quale troveranno coordinamento i principi fondamentali di tutela dei dati personali[3].

Nel quadro del progetto dell'euro digitale nel giugno 2023 è stata pubblicata la *Proposal for a Regulation on the establishment of the digital euro*, che per quanto concerne la *privacy compliance* persegue l'obiettivo dichiarato di garantire un elevato livello di tutela della vita privata nei pagamenti in linea con la normativa dell'Unione in materia di protezione dei dati (Regolamento UE 2016/679 e Regolamento UE 2018/1715).

Di grande rilevanza è stata l'adozione (10 luglio 2023) da parte della Commissione europea della Decisione di adeguatezza sul c.d. "*EU-U.S. Data Privacy Framework*" (DPF)[4] diretta a regolare i flussi transatlantici di dati personali e a superare le obiezioni sollevate dalla Corte di giustizia dell'Unione europea nella sentenza denominata *Schrems II* del luglio 2020, che aveva annullato una precedente Decisione in materia adottata nel 2016[5].

---

[2] *Digital Operational Resilience Act* ("DORA"), formalmente adottato il 16 gennaio 2023 e applicabile a decorrere dal 17 gennaio 2025.

[3] Cfr. Regolamento UE 2023/1114 relativo ai mercati delle cripto-attività; Regolamento UE 2022/858 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito.

[4] Il DPF UE-USA si fonda su un sistema di certificazione in base al quale le organizzazioni statunitensi si impegnano a rispettare una serie di principi sulla *privacy* individuati nella Decisione; tali certificazioni, da rinnovare annualmente, presuppongono l'assoggettamento ai poteri di indagine e di controllo della *Federal Trade Commission* (FTC) o del *Department of Transportation* (DoT) degli Stati Uniti nonché a una serie di obblighi tra cui la cancellazione dei dati personali quando non sono più necessari per lo scopo per cui sono stati raccolti, la garanzia di continuità della protezione quando i dati personali sono condivisi con terzi, l'equivalenza di protezione delle categorie particolari di dati, particolari restrizioni per i cosiddetti "trasferimenti successivi", ossia i trasferimenti di dati personali da un'organizzazione certificata DPF UE-USA a un terzo responsabile del trattamento o incaricato del trattamento, indipendentemente dal fatto che quest'ultimo si trovi negli Stati Uniti o in un paese terzo al di fuori degli Stati Uniti (*accountability for onward transfers*).

[5] Con sentenza del 16 luglio 2020 (caso C-311/18) la Corte di giustizia dell'Unione europea ha annullato la precedente Decisione di adeguatezza del c.d. *Privacy Shield* UE-US, in quanto non idonea a garantire un livello di protezione sostanzialmente equivalente a quello richiesto dal GDPR, in particolare per l'insufficienza dei diritti effettivi e azionabili

Il 3 aprile 2023 la Commissione europea ha inoltre pubblicato la relazione sul primo riesame del funzionamento della Decisione di adeguatezza per il trasferimento dei dati personali verso il Giappone, adottata il 23 gennaio 2019, alla luce di alcune revisioni introdotte dopo il primo biennio di applicazione che hanno accresciuto la convergenza tra i sistemi di protezione dei dati europeo e giapponese[6].

Il Comitato europeo per la protezione dati (EDPB) ha adottato un Report a conclusione della prima *Coordinated enforcement action* che nel 2023 ha avuto a oggetto l'uso di servizi *cloud* da parte del settore pubblico[7]. L'EDPB ha sottolineato la necessità per gli enti pubblici di agire nel pieno rispetto del GDPR, fornendo alle Pubbliche Amministrazioni una serie di raccomandazioni per la corretta formulazione dei contratti di affidamento in *cloud*, prevedendo il coinvolgimento del RPD di ciascuna istituzione interessata e invitando le Autorità di protezione dei dati a promuovere la conformità delle soluzioni *cloud* e l'importanza di condurre una valutazione d'impatto.

Inoltre vanno citate:

- in sede europea, l'approvazione da parte del Parlamento europeo e del Consiglio del Regolamento recante il quadro giuridico in materia di intelligenza artificiale (esplicitamente denominato "*Artificial Intelligence Act*[8]");
- in sede nazionale, l'approvazione della legge 7 dicembre 2023 n. 193 in materia di diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa patologia (cosiddetto "oblio oncologico")[9].

attribuiti alle persone i cui dati sono stati trasferiti verso il Paese Terzo e per la persistenza di prerogative di accesso non regolato ai dati da parte delle autorità statunitensi per ragioni di sicurezza nazionale. In tema di trasferimento *extra* SEE (Spazio Economico Europeo) dei dati personali, il GDPR disciplina una serie di strumenti che possono legittimare tale operazione: oltre alla Decisione di adeguatezza della Commissione il trasferimento è consentito in presenza di: uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; specifiche *Standard Contractual Clauses* adottate o approvate dalla Commissione; adozione di *Binding corporate rules* all'interno di un gruppo imprenditoriale transfrontaliero; assoggettamento dei titolari di trattamento a un codice di condotta ex art. 40 GDPR o a un meccanismo di certificazione ex art. 42 GDPR vincolanti per l'importatore del Paese Terzo; autorizzazione dell'Autorità di controllo su clausole contrattuali di trasferimento o su disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che contemplano diritti effettivi e azionabili per gli interessati.

6 Cfr. EDPB, *Statement* 1/2023 *on the first review of the functioning of the adequacy decision for Japan*, del 18 luglio 2023, che ha posto l'accento sulla permanenza di disallineamenti nella protezione dei cosiddetti *onward transfers* di dati personali verso Paesi terzi.

7 Il Report è frutto dell'attività di 22 Autorità garanti della *privacy* dello Spazio Economico Europeo che, nell'ambito del Quadro di attuazione coordinata (CEF - *Coordinated Enforcement Framework*), hanno avviato indagini contestuali sull'utilizzo del *cloud* nelle amministrazioni pubbliche, interpellando un centinaio di enti, attivi in settori cruciali come sanità, fisco e istruzione, ma anche centrali di acquisto e fornitori ICT.

8 Il 13 marzo 2024 il Parlamento europeo in plenaria ha approvato il testo; l'obiettivo dell'*AI Act*, in sintesi, è assicurare che i sistemi AI utilizzati all'interno dell'Unione europea siano completamente in linea con i diritti e i valori unionali, garandendo il controllo umano, la sicurezza, la *privacy*, la trasparenza, la non discriminazione e il benessere sociale e ambientale.

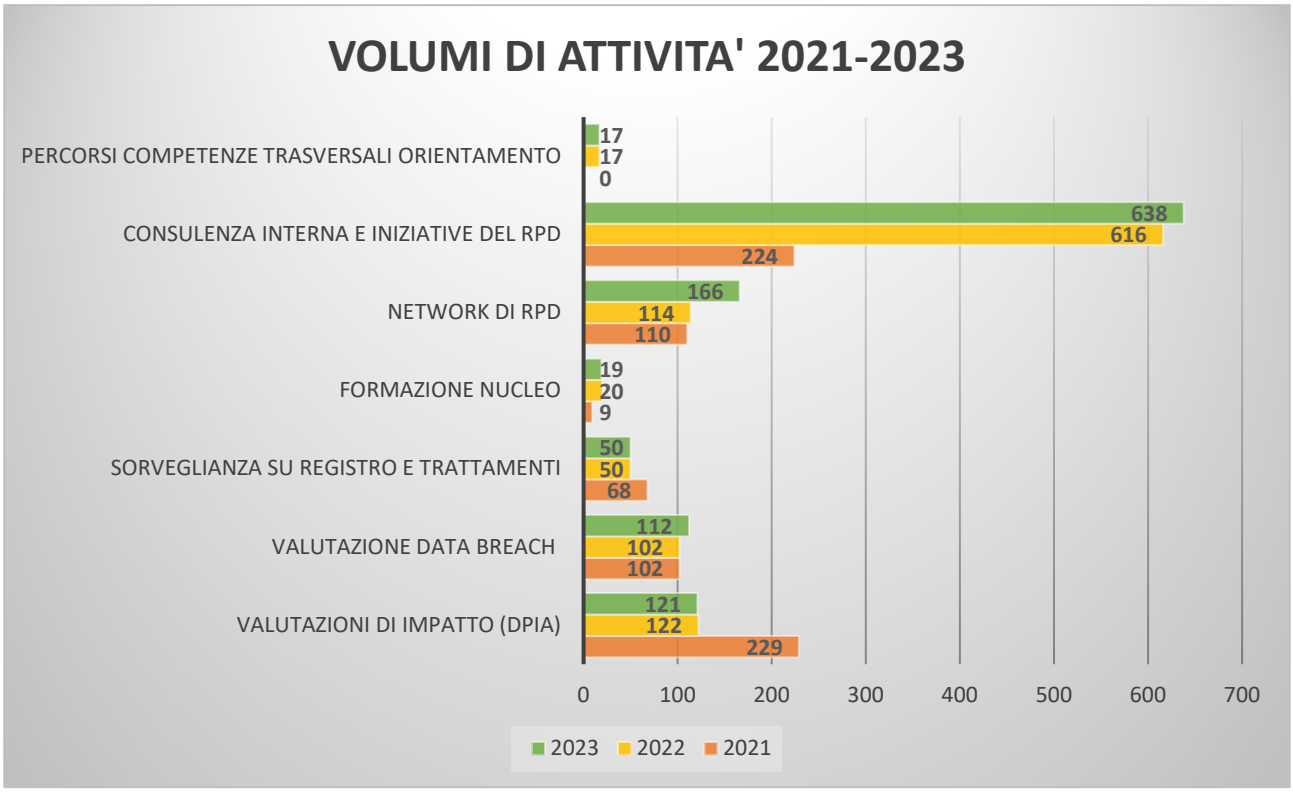
9 In linea con i diritti costituzionali e internazionalmente riconosciuti, la legge ha lo scopo di garantire la parità di trattamento, la non discriminazione e il diritto all'oblio delle persone guarite da malattie oncologiche (art. 1 co. 1). Il diritto all'oblio oncologico viene definito dall'art. 1 co. 2 come "*il diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica*".

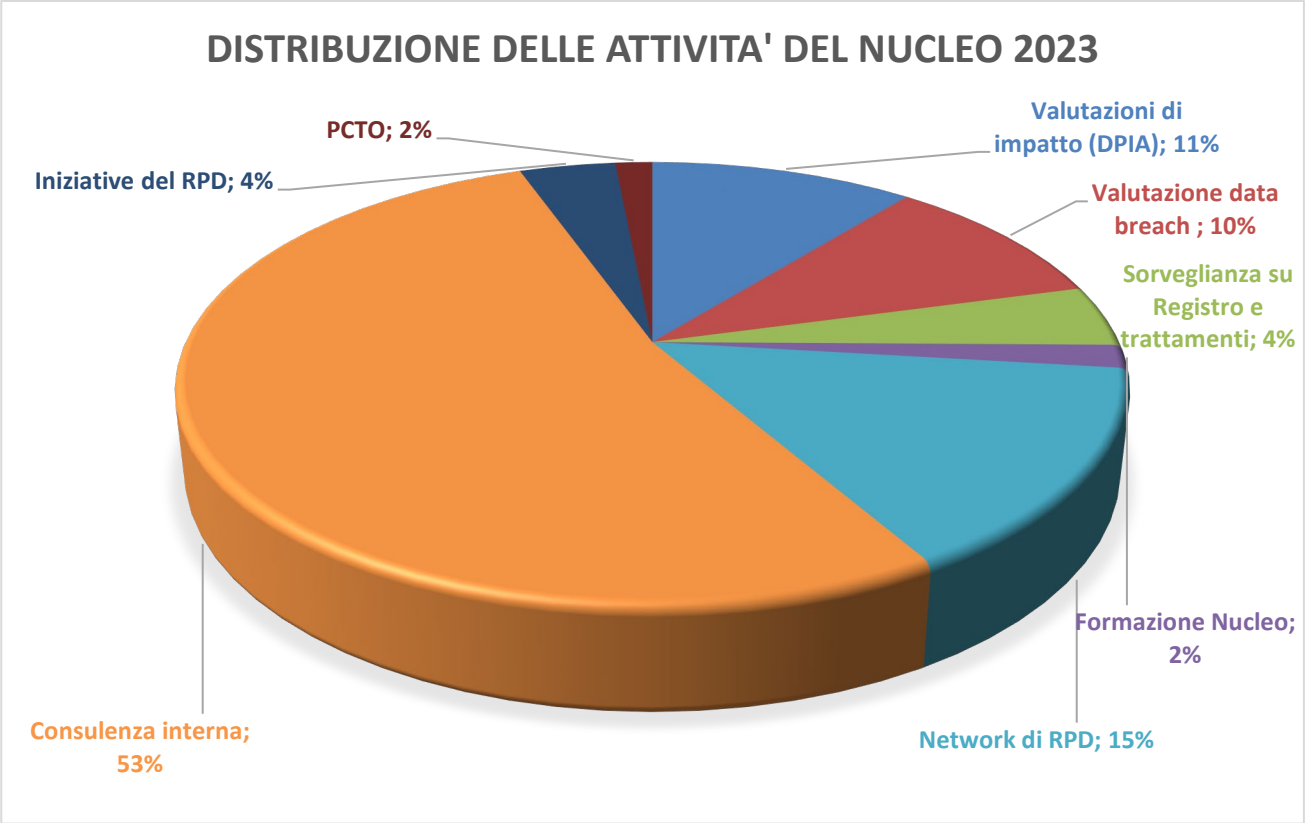
2. L'attività svolta nel 2023.

L'attività svolta dal RPD ha confermato nel 2023 la progressiva espansione della funzione di consulenza alle strutture e di interlocuzione anche esterna in specifici network nazionali ed europei, per i profili di applicazione della normativa sulla protezione dei dati personali.

Specifica attenzione è stata destinata alla formazione specialistica del personale addetto alla struttura di supporto del RPD, anche in relazione ai costanti sviluppi sul piano normativo e su quello tecnologico del contesto in cui sono svolte le funzioni di sorveglianza e di consulenza.

Nei grafici seguenti si fornisce una rappresentazione quantitativa dei volumi dell'attività svolta in raffronto con gli anni precedenti e per composizione interna dell'assorbimento delle risorse dedicate.





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

2.1 Cooperazione e interlocuzione con il Garante della Protezione dei Dati Personali (Garante *privacy*).

L'anno è stato caratterizzato da una costante attenzione del Garante *privacy* alla figura del RPD, al presidio dei suoi compiti di sorveglianza in materia di protezione dei dati personali e al suo costante coinvolgimento nell'attività dei titolari dei trattamenti di dati. A cinque anni dall'applicazione del GDPR il Garante ha inteso rinnovare il dialogo con i Responsabili della protezione dei dati del settore pubblico e privato per fare un bilancio dell'esperienza maturata e per individuare le aree di intervento volte a rafforzare il ruolo del RPD[10]. Nell'incontro plenario tenutosi a Bologna il 23 giugno, diverse sono state le tematiche al centro del confronto tra Garante e RPD: in particolare, si è discusso sulle modalità di designazione, sul profilo di competenze e conoscenze del RPD ma anche sui rischi connessi alla posizione organizzativa del RPD e sui profili di autonomia e conflitto di interessi; infine, oggetto del dibattito è stato il ruolo del RPD nell'attività di consulenza al Titolare del trattamento e di tutela dell'interessato nonché il contributo del RPD nelle situazioni complesse anche nel delicato rapporto con l'Autorità Garante.

[10] Il Garante ha sempre posto particolare attenzione alla funzione strategica del RPD, nel favorire l'osservanza della disciplina *privacy* all'interno delle organizzazioni, e sulla capacità di essere un valore aggiunto all'interno dell'organizzazione aziendale. L'Autorità ha dedicato agli RPD numerose iniziative informative, a partire dal Progetto T4Data ("*Training For Data*"), promuovendo anche la creazione di "reti di RPD" per settori omogenei, di cui l'iniziativa in ambito bancario rappresenta un significativo esempio.

È proseguita nell'anno in esame, con il coordinamento del Garante, l'attività della rete dei RPD del settore bancario, cui ha partecipato anche una rappresentanza dell'Istituto, che ha costituito un gruppo di lavoro permanente finalizzato a conoscere i fenomeni aziendali e coordinare eventuali iniziative allo scopo di armonizzare la regolazione delle attività che coinvolgono la protezione dei dati relativi alle persone fisiche.

Il Garante ha suggerito al gruppo di lavoro come prime attività nel corso del 2023 l'elaborazione e la somministrazione presso le banche di un questionario per verificare lo stato di radicamento della funzione di RPD a distanza di cinque anni dall'applicazione del GDPR. Nel questionario, al quale hanno risposto 87 soggetti tra banche individuali e capogruppo di gruppi bancari, sono state proposte domande sulle modalità di designazione, sui requisiti necessari per svolgere i compiti previsti, sulle risorse assegnate, sul ruolo e sulla posizione nell'ambito dell'organizzazione societaria. I risultati dell'indagine sono stati presentati e commentati nel corso di un incontro tenutosi presso l'ABI all'inizio del 2024 alla presenza del Presidente del Collegio del Garante e del Presidente dell'ABI[11].

Come membro di tale *network* il RPD ha preso parte al Tavolo tecnico organizzato dal Garante il 18 settembre a Roma nell'ambito del Convegno "*State of privacy* 2023", dove sono stati approfonditi i temi dell'utilizzo dei dati della clientela bancaria per l'applicazione dell'intelligenza artificiale nei servizi finanziari e la condivisione delle informazioni tra destinatari e autorità pubbliche ai fini dei processi e della normativa in materia di antiriciclaggio e di cybersicurezza. Tra gli argomenti più interessanti nel Convegno figurano anche l'etica dei dati e della *privacy* e l'importanza del rapporto tra emozioni e algoritmi. Inoltre, si è sottolineata la natura multidimensionale della protezione dei dati e la necessità di difendere i diritti alla *privacy* di fronte all'avanzare della tecnologia e della sorveglianza.

Nell'ambito della cooperazione con il Garante, il RPD ha collaborato al riscontro di una richiesta di informazioni rivolta alla Banca ai sensi dell'art. 157 del d.lgs. 30 giugno 2003, n. 196 (Codice *privacy*), in ausilio all'istruttoria di un reclamo presentato al Garante da un cittadino nei confronti di terzi per furto di identità digitale attraverso SPID, in occasione di accesso ai servizi offerti all'utenza.

2.2 Le consultazioni del RPD.

L'attività di consulenza sull'applicazione della normativa *privacy* è condotta dal RPD in maniera strutturata nei pareri resi sui casi di *data breach* e sulle valutazioni di impatto sulla protezione dei dati ai sensi degli artt. 33 e 35 GDPR (cfr. *infra*) mediante suggerimenti e raccomandazioni sulle questioni sollecitate dalle Strutture, in costante confronto con il Servizio Organizzazione.

[11] Dall'indagine è emerso che i RPD: i) sono nominati con un apposito atto di designazione; ii) hanno una provenienza professionale principalmente di area giuridica ed economica; iii) hanno un'esperienza media tra i 3 e gli 8 anni; iv) dispongono in prevalenza di uno staff di supporto; v) prestano sempre maggiore attenzione ai rischi collegati all'intelligenza artificiale e all'applicazione delle nuove tecnologie; vi) ritengono essenziale il costante coordinamento tra le Autorità alla luce delle normative nazionali ed europee del settore finanziario.

L'attività consultiva in numerosi casi ha riguardato l'esame delle clausole *privacy* di accordi o protocolli da perfezionare con soggetti pubblici per lo svolgimento di compiti istituzionali. In particolare:

- una convenzione di collaborazione con l'Agenzia delle Entrate in applicazione dell'art. 120-*sexiesdecies* del Testo Unico Bancario per consentire lo svolgimento dei controlli nell'ambito dell'attività di vigilanza macroprudenziale, assicurare il flusso informativo necessario alla Banca per calcolare alcuni indicatori richiesti dalla raccomandazione ESRB/2016/14, nonché per svolgere attività di ricerca sul tema dei rischi per la stabilità finanziaria derivanti dal mercato residenziale e sul tema della distribuzione della ricchezza immobiliare e del debito delle famiglie italiane;
- un accordo di collaborazione con il Ministero delle Imprese e del *Made in Italy*, con la finalità di realizzare attività di ricerca e analisi in campo statistico ed economico su temi di reciproco interesse[12];
- una convenzione con il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), per la condivisione e l'analisi delle informazioni idonee a prevenire e contrastare attacchi o danneggiamenti in pregiudizio delle infrastrutture critiche informatiche della Banca, nonché per la segnalazione tempestiva di emergenze relative a vulnerabilità, minacce e incidenti in danno della regolarità dei servizi di telecomunicazione o contro infrastrutture critiche che abbiano come destinazione le infrastrutture tecnologiche utilizzate o gestite dalla Banca;
- una convenzione con l'Agenzia per l'Italia Digitale (AGID) per l'accreditamento della Banca come soggetto aggregatore per la fornitura del servizio di autenticazione informatica degli utenti attraverso lo SPID ai fini dell'accesso ai servizi in rete che la Banca eroga per conto dell'IVASS dai propri sistemi;
- un accordo con il Politecnico di Milano finalizzato a stabilire un rapporto di collaborazione, nel rispetto delle rispettive competenze istituzionali, riguardo alle tematiche della digitalizzazione e dell'innovazione nel settore bancario, finanziario, assicurativo e dei pagamenti;
- altri protocolli di collaborazione inter-istituzionale, per i quali si è reso necessario valutare la conformità rispetto ai ruoli *privacy* rivestiti dai contraenti e alla cornice di regolazione del trattamento di dati personali[13].

L'attività di consulenza del RPD è stata richiesta altresì per la definizione della clausola "*Data protection*" nell'accordo di collaborazione con la BCE relativo al funzionamento dell'*Eurosystem Quality Control Tool Test Centre* (QCTTC) nell'ambito del processo di produzione delle banconote; sugli aspetti relativi alla conformità dell'informativa da rilasciare agli interessati a corredo del questionario per l'Indagine sulla digitalizzazione delle Amministrazioni Locali 2023; per l'analisi della conformità ai principi della disciplina sulla *privacy* dell'articolazione dei canali di acquisizione del *whisteblowing* alla luce delle modifiche introdotte nella specifica normativa dal

[12] Le tematiche individuate nell'accordo concernono l'analisi (a) dei fabbisogni di *input* produttivi, materie prime e risorse umane, necessari per accrescere la produttività e competitività del sistema manifatturiero italiano; (b) dell'impatto delle restrizioni economiche (sanzioni, *export control*) e rischi sulle filiere produttive, sulla competitività delle imprese e sul sistema industriale italiano; (c) delle misure di incentivi alle imprese e degli strumenti di politica industriale nazionale.

[13] Convenzione tra Banca d'Italia e l'Associazione Nazionale Costruttori Edili (ANCE) per la realizzazione di progetti di ricerca di interesse comune; accordo tra il CERT della Banca e l'Arma dei Carabinieri per lo scambio informativo e la cooperazione per la protezione dalle minacce *cyber*.

d.lgs. 10 marzo 2023 n. 24 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e delle disposizioni normative nazionali. Inoltre, il RPD ha preso parte per i profili di propria competenza alle attività di studio di possibili forme di collaborazione tra la Banca e l'IVASS ai fini dello svolgimento dei compiti di sorveglianza sanitaria assegnati dalla legge nei confronti dei propri dipendenti e ha cooperato negli approfondimenti dei profili di protezione dei dati personali da trattare nell'ambito di attività e iniziative formative condivise con altre Autorità amministrative indipendenti[14].

La funzione consulenziale nell'anno ha avuto per oggetto anche numerose altre questioni particolari per le quali dalle diverse strutture sono state sollecitate al RPD opinioni o indicazioni in collaborazione con il Servizio Organizzazione (per es. informative *privacy* connesse ad attività presso la rete periferica; atti di designazione dei medici competenti; quesiti su basi giuridiche e tempi di conservazione dei dati riferiti a specifici trattamenti; questioni *privacy* con fornitori esterni designati responsabili del trattamento dei dati; ricorrenza dei presupposti di obbligatorietà delle valutazioni di impatto; quesiti sullo scarto di documentazione digitale; metodi di valutazione del rischio *privacy* aziendale).

2.3 La sorveglianza sul Registro delle attività di trattamento

Nel corso del 2023, nell'ambito dell'attività di sorveglianza sul Registro delle attività di trattamento, si è proceduto al monitoraggio periodico delle informazioni iscritte nel Registro[15] che ha l'obiettivo di verificare la completezza e la coerenza della descrizione dei trattamenti inseriti dalle Strutture competenti (209 al 31 dicembre) e promuoverne eventuali rettifiche e integrazioni.

L'attività ha messo in evidenza che:

- il numero dei trattamenti è leggermente diminuito (da 215 a 209) per effetto della ridefinizione del perimetro dei trattamenti di competenza delle diverse Strutture;
- la distribuzione interna dei trattamenti mantiene significative diversificazioni, evidenziando una particolare concentrazione nella Funzione Risorse Umane e Informazione e nei Dipartimenti Mercati e sistemi di pagamento e Vigilanza bancaria e finanziaria (complessivamente 104 trattamenti);
- la qualità informativa delle iscrizioni continua a migliorare per effetto della progressiva precisazione degli elementi obbligatori nella descrizione del trattamento, tra i quali le modalità di rilascio dell'informativa *privacy* e l'indicazione dei tempi di conservazione dei dati personali.

Nel complesso, le dinamiche rilevate testimoniano una maggiore sensibilizzazione delle Strutture nel censimento delle annotazioni di competenza, con conseguente incremento della qualità del patrimonio informativo del Registro.

Da ultimo, è stato curato col Servizio Organizzazione un riesame del Registro del Responsabile del trattamento, procedendo all'aggiornamento delle fattispecie in cui la Banca

---

14 Nella circostanza l'analisi è stata a supporto di iniziative condivise con l'Autorità Garante per la Concorrenza e il Mercato, con la Commissione Nazionale per le Società e la Borsa e con l'Autorità per la Cybersicurezza Nazionale.

15 La tenuta del Registro è prevista dall'art. 30 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 per sorvegliare l'osservanza del GDPR il RPD conduce con regolarità il monitoraggio del Registro con l'obiettivo di valutare complessivamente l'efficacia informativa dei trattamenti censiti.

d'Italia tratta dati personali di titolarità di altre Amministrazioni con le quali ha sottoscritto accordi di collaborazione inter-istituzionale.

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

Nel corso del 2023 il RPD ha fornito il suo parere su otto *Data Protection Impact Assessment* (DPIA) in relazione a trattamenti di dati personali la cui esposizione a rischi per le persone fisiche interessate è stata valutata in dipendenza di progetti informatici o procedure di lavoro oggetto di studio o revisione[16].

Nell'ambito delle funzioni istituzionali e aziendali sono state valutate le implicazioni sui trattamenti di dati personali delle seguenti iniziative:

- "Ethos (*ETHical Operative System*)", finalizzato a introdurre un applicativo informatico per la gestione e il controllo dei dati finanziari dei dipendenti comunicati in base a quanto disposto, in tema di investimenti finanziari privati dei dipendenti delle banche centrali, dalle Linee Guida BCE e dalla normativa attuativa emanata dall'Istituto;
- manutenzione evolutiva della procedura di acquisizione dei dati finanziari sugli investimenti esteri comunicati dai contribuenti in sede dichiarativa e trattati dall'Istituto per la compilazione della bilancia dei pagamenti dell'Italia nonché, in forma aggregata con le statistiche degli altri Paesi membri, della bilancia dei pagamenti dell'area euro e dell'Unione europea;
- "RepTech", progetto volto a sviluppare indicatori reputazionali degli intermediari vigilati ricorrendo a fonti pubbliche di informazioni (a es. Twitter e Factiva) successivamente elaborate tramite l'utilizzo di tecniche di intelligenza artificiale e messe a disposizione degli analisti della vigilanza di tutela;
- "*E-learning*", finalizzato alla gestione strutturata delle iniziative di educazione finanziaria predisposte dall'Istituto e svolte tramite formazione a distanza a beneficio della cittadinanza e degli stessi formatori (a es. insegnanti, esponenti di associazioni di categoria, ecc.);
- "Nuova piattaforma *back office* per ABF", volta ad assicuare una maggiore integrazione degli applicativi informatici in uso alle Segreterie Tecniche per il trattamento dei dati personali nell'istruzione dei ricorsi presentati all'Arbitro Bancario e Finanziario (ABF) e nelle comunicazioni da inoltrare alle parti del procedimento;
- introduzione, tramite la piattaforma *BlackBerry AtHoc*, di un sistema di comunicazione massiva e multicanale destinata a tutto il personale da attivare in situazioni di emergenza (relative alla tutela della salute e sicurezza sui luoghi di lavoro o al regolare svolgimento dei processi operativi dell'Istituto), a fronte della totale o parziale impossibilità di utilizzo dei dispositivi informatici aziendali;
- "PI.CO (*PIattaforma COncorsi*)", finalizzato alla gestione delle procedure di selezione esterna e interna del personale dell'Istituto in un'ottica di semplificazione degli oneri amministrativi,

[16] L'art. 35 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 par. 4 GDPR (cfr. Provvedimento n. 467 dell'11 ottobre 2018).

crescente automazione dei processi operativi e maggiore integrazione tra tale piattaforma e le altre basi di dati aziendali a disposizione della Funzione del personale;

- "ABACO-PA (*Attivi Bancari COllateralizzati-Procedura Ancillare*)", volto a introdurre un applicativo informatico per la gestione dei portafogli di prestiti bancari che la Banca d'Italia, nell'ambito del *framework* temporaneo "*additional credit claims*" predisposto dalla BCE, può accettare come garanzia per le operazioni di credito dell'Eurosistema.

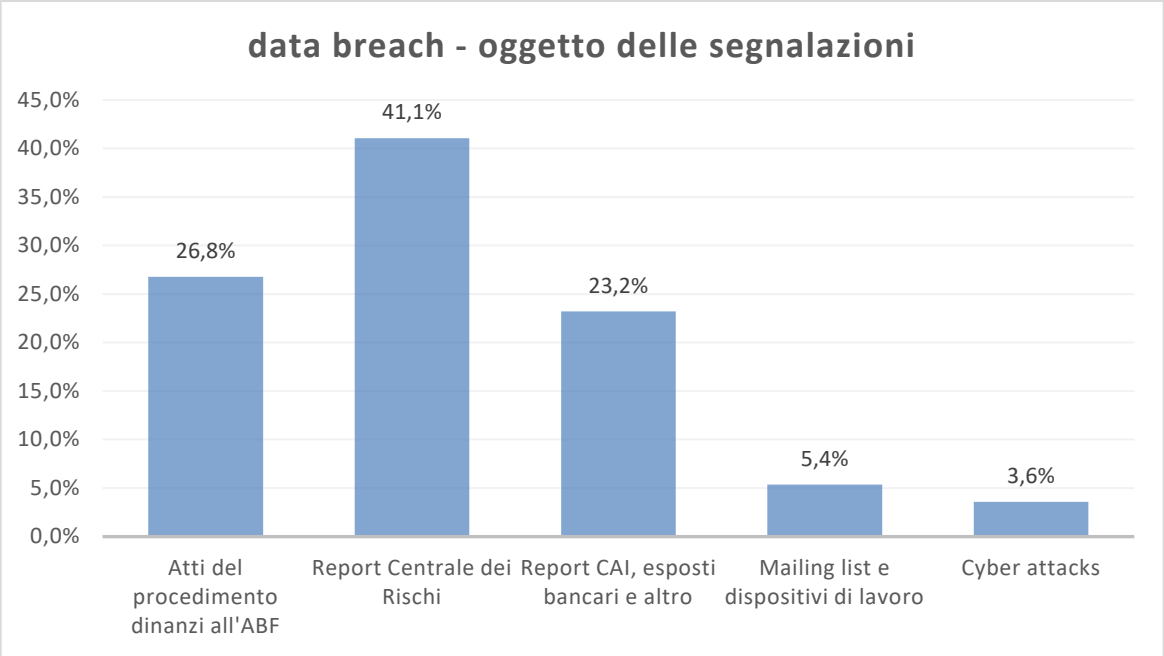
In ambito istituzionale il RPD ha inoltre fornito un parere sull'iniziativa di manutenzione evolutiva della procedura POLIS, finalizzata alla gestione delle informazioni del comparto operativo contabile delle Filiali, rispetto alla quale si era proceduto nel corso del 2020-2021 alla valutazione di impatto sulla protezione dei dati personali. Il RPD ha condiviso le valutazioni della Struttura competente di non eseguire una nuova valutazione di impatto in quanto, alla luce dei presidi di sicurezza predisposti e tenuto conto dell'ambito di applicazione e delle finalità del trattamento dei dati, non è emerso un rischio residuo complessivo di livello significativo per i diritti e le libertà delle persone fisiche interessate.

2.5 Le segnalazioni dei data breach.

Nel 2023 sono state rilevate e segnalate 56 violazioni dei dati personali (c.d. *data breach*): su ciascun evento il RPD ha fornito il suo parere relativo alla sussistenza di una 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[17].

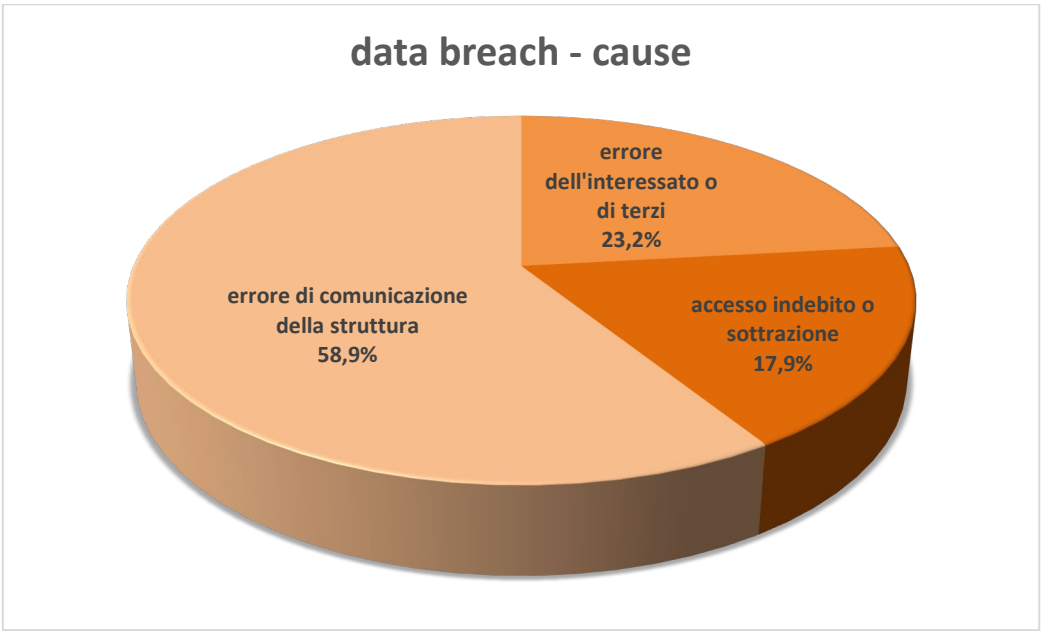
L'ambito nel quale si sono concentrate maggiormente le segnalazioni di violazione dei dati personali, come per l'anno precedente, è quello inerente agli accessi alla Centrale dei Rischi, seguito da quello relativo alla gestione dei procedimenti dinanzi all'ABF. In misura meno frequente si rilevano incidenti nella comunicazione dei report CAI, nella gestione degli esposti bancari e nell'utilizzo delle *mailing list*. Un rischio meritevole di separata e particolare menzione per via del suo potenziale effetto lesivo è quello dei tentativi di *cyber attacks*, che si affacciano per la prima volta tra i potenziali *data breach* (cfr. grafico seguente).

[17] Il RPD fornisce al Titolare del trattamento un parere che rafforza gli elementi di valutazione nei casi di perdita, alterazione o sviamento (accidentali o illeciti) di dati personali configurabili come *data breach*. Il GDPR (art. 33), quando si verificano i presupposti di un effettivo *data breach*, impone al Titolare del trattamento dei dati di darne notifica alla competente 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). A questi ultimi deve essere data comunicazione con un un linguaggio semplice e chiaro, contenente un'accurata descrizione della natura della violazione dei dati personali, nonché suggerimenti e raccomandazioni su come poter attenuare i potenziali effetti negativi derivanti dalla violazione dei suoi dati personali.



In 'altro' vengono ricomprese fattispecie di *data breach* occorsi nelle diverse attività dell'Istituto, tra le quali a titolo esemplificativo si ricordano attività amministrative relative a compiti segretariali ed atti impeditivi.

Tra le cause degli eventi di violazione risulta predominante l'errore operativo nella comunicazione da parte delle strutture, seguito da quello da parte degli stessi interessati o di terzi e dalle condotte dolose poste in essere da attori malevoli (cfr. grafico seguente).



La valutazione dei rischi derivanti da tali violazioni ha indotto in due casi[18] a effettuare al Garante *Privacy* la segnalazione prevista dall'art. 33 GDPR, per una rilevata azione malevola

[18] Si è trattato di un caso di *cyber attack* a un fornitore di servizi di un Resposabile del trattamento e di un accesso tramite

esterna. Negli altri casi (96,43%) non è stato necessario effettuare la segnalazione, dato che si è ritenuto trascurabile il livello di rischio per i soggetti interessati nelle varie fattispecie alla luce delle circostanze fattuali e delle cautele adottate.

2.6 Le iniziative del RPD.

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

I 14 progetti ammessi a Milano Hub all'esito della *Call for proposals 2022* che ha avuto come tema l'applicazione della tecnologia basata su registri distribuiti (*Distributed Ledger Technology* – DLT) ai servizi bancari, finanziari, assicurativi e di pagamento, si sono anche avvalsi di un team trasversale per gli aspetti di tutela della *privacy* composto dai Servizi Organizzazione, Consulenza legale e dal Nucleo di Supporto al RPD.

Nel mese di marzo 2023 il RPD ha organizzato un incontro presso la Sede di Bologna della Banca con il tema "La sicurezza dei dati personali nel GDPR: prevenire il *data breach*" 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 normali attività di lavoro.

In generale, sulle diverse questioni applicative della disciplina sulla *privacy* all'interno della Banca e nelle interlocuzioni con le strutture il RPD ha continuato a mantenere il confronto con il Servizio Organizzazione nelle funzioni di Titolare del trattamento conformemente alle linee di indirizzo sul DPO in ambito pubblico emanate dal Garante[19].

3. La partecipazione ai network di RPD.

3.1 L'attività internazionale.

Nei meeting del Network dei RPD (*Data Protection Officers*, DPOs) delle Banche Centrali Nazionali e delle Autorità Nazionali Competenti per la supervisione bancaria con il coordinamento della BCEsi è avviato il confronto principalmente su quattro temi comuni alle istituzioni interessate:

- le problematiche sorte nell'ambito della fase di indagine relativa al progetto di emissione dell'euro digitale per i riflessi *privacy* e per l'interesse manifestato dai cittadini a preservare la possibilità di effettuare transazioni nel rispetto della riservatezza individuale, che si è attestato come secondo fattore di importanza, dopo il fattore sicurezza; dal confronto è emersa l'esigenza di un coinvolgimento dei DPOs delle istituzioni nazionali sui profili di protezione dati del progetto;

sportello *online* alla situazione in Centrale dei Rischi di una persona giuridica, sulla base di autocertificazione rivelatasi non rispondente al vero, per i quali è stata altresì effettuata segnalazione all'Autorità giudiziaria.

[19] Provvedimento 29 aprile 2021, n. 186, *Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico.*

- le problematiche sorte dall'utilizzo del sistema di comunicazione e di condivisione di documenti basato sul *software* di lavoro *Microsoft Dynamics* 365, che non consentirebbe di poter avere le tutele previste all'interno della disciplina europea regolamentata dal GDPR[20];

- gli aspetti attinenti alle problematiche connesse alla condivisione dei dati all'interno dell'Eurosistema negli accordi di *Joint Controllership* nella gestione dei dati personali nel contesto della vigilanza prudenziale delle istituzioni creditizie svolta in ambito SSM e la BCE; su tale tema è stato fornito alla BCE un articolato contributo nel procedimento di definizione del progetto di Decisione destinato a recepire gli accordi.

- le problematiche comuni allo scambio di dati personali tra autorità pubbliche nella lotta a corruzione, frodi, antiriclaggio e contrasto del finanziamento del terrorismo (AML/CFT) che ha contribuito a formare posizioni condivise in merito alle iniziative in corso per il coordinamento delle informazioni antiriciclaggio.

3.2 L'attività nazionale.

L'attività del Network dei DPOs delle Autorità indipendenti nazionali[21], sede di confronto inter-istituzionale di cui fa parte il RPD della Banca per lo scambio informativo sui temi di protezione dei dati personali[22], si è aperta nel gennaio 2023 con la riunione tenutasi presso il Centro Congressi della Banca.

Il RPD dell'Istituto ha introdotto alcuni temi di evidente interesse per il network nel nuovo anno:

- l'aumento della sensibilità al tema della *cyber* sicurezza, alimentata dalle continue minacce alla riservatezza di persone e istituzioni, con le conseguenti implicazioni riguardo alla mitigazione dei rischi di violazione dei dati personali;

- l'applicazione dell'intelligenza artificiale, in particolare nel mondo della finanza, dove i dati costituiscono una risorsa determinante da cui dipendono le possibilità di funzionamento del sistema, rappresentando gli *input* da cui gli algoritmi riescono a trarre risultati.

---

[20] Il 12 marzo scorso il Garante europeo ha emanato un provvedimento nei confronti della Commisisone europea con la quale rende noto che il prodotto (in uso anche alla BCE), non essendo conforme alla normativa sulla protezione dei dati personali su vari aspetti, deve essere dismesso ento il 9 dicembre 2024 se non dovessero essere recepite le modifiche richieste.

[21] Oltre il RPD della Banca d'Italia, compongono attualmente il Network i 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) e dell'Acquirente Unico S.p.a. (AU), del Garante per l'Infanzia e l'adolescenza nonché dell'Istituto Nazionale di Statistica (ISTAT) in qualità di osservatore.

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

Negli incontri periodici sono stati approfonditi i temi di interesse per le Autorità partecipanti, quali:

- l'uso degli strumenti di tracciamento/monitoraggio offerti da terzi fornitori nella configurazione dei siti *web* e dei servizi digitali della PA, per il connesso rischio di trasferimento di informazioni al di fuori dello Spazio Economico Europeo (ad esempio per l'utilizzo di *web analytics* e di componenti di terze parti incorporati sui propri siti *web*, come *font* tipografici, *video player*, *social plug-in*, ecc.);

- i risultati dell'indagine avviata dall'EDPB nell'ambito del CEF - *Coordinated Enforcement Framework* sull'uso di servizi basati su *cloud* da parte del settore pubblico, da cui è emersa l'esigenza di equilibrare i rapporti tra Titolare del trattamento e fornitore esterno per consentire all'ente pubblico di negoziare adeguate condizioni contrattuali per la protezione dei dati personali;

- i possibili sviluppi dell'attività consultiva dei RPD nelle valutazioni di impatto sulla protezione dei dati;

- la ricognizione delle norme in vigore in materia di trasferimento dei dati personali fuori dello Spazio Economico Europeo, anche a seguito delle decisioni di adeguatezza della Commissione europea nonché delle pronunce della Corte di giustizia dell'Unione europea;

- l'approfondimento del quadro delle norme che regolano il trattamento dei dati personali nell'ambito del rapporto di lavoro, con *focus* sui provvedimenti del Garante che ne hanno chiarito l'applicazione pratica.

Il 24 novembre 2023 la Rete dei RPD ha organizzato un Seminario, ospitato dall'Autorità Garante della Concorrenza e del Mercato, sul tema "Il principio della *privacy by design* e *by default* nella Pubblica Amministrazione", durante il quale gli interventi del Garante *privacy*, del Presidente ANAC e di esponenti dell'ACN e dell'ISTAT, hanno approfondito argomenti quali la progettazione dei trattamenti di dati secondo i principi del GDPR, la digitalizzazione nel nuovo codice dei contratti pubblici, il *Cyber Resilience Act* e il trattamento dei dati personali mediante l'intelligenza artificiale nella Pubblica Amministrazione e nella statistica ufficiale. È altresì emersa la consapevolezza che obiettivi complessi, ambiziosi e sfidanti possono essere raggiunti solo collaborando tra RPD e facendo rete.

Dagli interventi si è tratta la generale considerazione che per la PA del futuro la *privacy by design* e *by default* deve sempre più essere considerata una modalità di lavoro che rafforza la trasparenza e la legittimazione dell'azione amministrativa. Ne discende che essa:

- deve porsi in *frontline*, come esempio virtuoso, modello e stimolo per vincere la sfida e generare fiducia nel suo corretto operare nell'interesse comune;
- deve compiere il delicato bilanciamento tra i diritti fondamentali, tra i quali rientra il diritto alla protezione dei dati personali;
- può ricorrere a strumenti evoluti, quali l'intelligenza artificiale, sottomettendone le potenzialità alla trasparenza degli algoritmi, alla qualità del dato, al coinvolgimento dei soggetti che intervengono a vario titolo nel trattamento e in tutto il ciclo di gestione dell'informazione, alla sicurezza consapevole degli interessati.