BANCA D'ITALIA
EUROSISTEMA

Relazione del Responsabile della Protezione dei Dati

Anno 2022

Roma, marzo 2023

INDICE

Introduzione.

Nel 2022 è cresciuta la complessità dello scenario nel quale si attua la protezione dei dati delle persone fisiche e si svolge l'azione di sorveglianza della funzione di Responsabile della Protezione dei Dati (RPD)[1].

Soprattutto nel settore pubblico progredisce a ritmo crescente la generale informatizzazione dei processi, delle attività e delle relazioni con i cittadini, in relazione alla quale si registrano un incremento del volume dei dati scambiati e la conseguente necessità di adeguamento alle norme sul rispetto dei trattamenti di dati personali.

L'attività del RPD deve tener conto della progressiva digitalizzazione e delocalizzazione delle informazioni che determinano rischi nuovi ed esigenza di presidi di sicurezza più raffinati nell'azione di protezione degli interessati. La tutela dei dati delle persone fisiche, come delineata dal GDPR, costituisce per le organizzazioni pubbliche e private un obbligo giuridico, del cui adempimento sono tenute a rendere conto; ma nello stesso tempo essa rappresenta nel settore pubblico anche un impegno etico, dal cui assolvimento dipendono i beni immateriali della reputazione della PA e della fiducia del cittadino.

Il disegno del legislatore comunitario, che postula l'*accountability* di ogni titolare di trattamento di dati personali, impone per diffuso convincimento uno stile di conduzione delle attività che presuppone una costante attenzione alla tutela dei dati personali, espressa da una coerente ideazione e impostazione dei processi di lavoro, dalla valutazione del rischio di violazione nei confronti delle persone e dalla scelta delle misure di sicurezza tecniche e organizzative ritenute adatte a contenere il rischio.

Lo scenario si arricchisce della persistenza di sfide sempre aperte per le amministrazioni pubbliche, nei diversi ambiti di supervisione o di regolazione, quali il bilanciamento della sicurezza dei dati e del presidio sull'accesso agli stessi con gli obblighi di semplificazione e trasparenza o la promozione della fiducia degli utenti attraverso l'educazione al controllo sulle informazioni che riguardano la propria persona e la propria identità.

* * *

1. Il quadro normativo.

L'anno trascorso ha segnato l'apertura di una impegnativa stagione di regolamentazione comunitaria del mondo digitale e dell'utilizzo dei dati (personali e non) applicabile dal 2023[2] che prelude a una necessaria attività di coordinamento applicativo delle nuove norme con il GDPR[3]. In particolare:

---

[1] Le funzioni del RPD in Banca sono svolte dal Revisore Generale che per la natura della funzione a cui è preposto mantiene un rapporto di terzietà con tutte le attività e le strutture aziendali. 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.

[2] La normativa regolamentare dell'UE di norma ha una decorrenza applicativa differita rispetto alla formale entrata in vigore per consentirne l'adeguamento nei diversi Paesi Membri.

[3] Ciò soprattutto nei rapporti di prevalenza tra norme regolamentari, nell'armonizzazione delle forme di tutela dei diritti e delle libertà fondamentali degli individui e nel coordinamento delle diverse attività di supervisione da parte delle autorità di controllo coinvolte.

- il Regolamento UE 2022/868 relativo alla *governance* europea dei dati ha definito la cornice normativa per consentire il riutilizzo sicuro da parte delle imprese di determinate categorie di dati detenuti da enti pubblici ove giustificato e necessario per la fornitura di un servizio di interesse generale;
- il Regolamento UE 2022/1925 relativo ai mercati digitali disciplina l'attività dei cosiddetti *gatekeeper,* ossia le imprese che forniscono servizi *online* di intermediazione a titolo vario (es. motore di ricerca, social network, condivisione di video, browser web, *cloud computing* o pubblicità in rete) e che per dimensione e operatività assumono di fatto il ruolo di struttura connettiva delle relazioni digitali e possono esercitare una funzione di controllo dell'accesso al mercato digitale[4];
- in stretta connessione con il predetto atto normativo è stato emanato il Regolamento UE 2022/2065 relativo agli altri servizi di intermediazione digitale (a esempio, mercati online, piattaforme per la condivisione di contenuti, per l'offerta di viaggi e alloggi online, app store e social network) che tra l'altro regola le responsabilità di utilizzo dei dati intermediati e impone altresì l'istituzione di autorità nazionali di controllo in materia.

La copiosa produzione normativa della UE non pregiudica le norme stabilite da altri atti giuridici dell'Unione sul trattamento dei dati personali e, senza introdurre nuove fonti di legittimazione del trattamento dei dati, impone un'estensione delle conoscenze e dell'azione di controllo sia alle Autorità nazionali sia alle funzioni investite dei compiti di sorveglianza in materia di *privacy*.

Nei contatti con la funzione del RPD si è registrata l'attenzione accademica al tema dell'applicazione della normativa sul diritto alla riservatezza dei dati personali nell'ambiente di lavoro, dove le relazioni giuridiche e quelle sociali sono in misura crescente influenzate dall'uso della tecnologia (principio di responsabilizzazione del datore di lavoro titolare del trattamento dei dati e introduzione di nuove tecnologie di tracciamento nello svolgimento dell'attività lavorativa)[5].

2. L'attività svolta nel 2022.

L'attività svolta dal RPD ha registrato un marcato incremento del contributo consulenziale alle diverse Strutture della Banca, per iniziative e interventi che hanno richiesto l'analisi di problematiche connesse con il trattamento dei dati personali, anche nell'ambito di relazioni con altre Amministrazioni pubbliche, per la partecipazione a due dei Gruppi di supporto costituiti per accompagnare il perfezionamento di progetti ammessi a Milano Hub all'esito della *Call for*

[4] La normativa comunitaria in particolare vieta ai *gatekeeper* di combinare dati personali ricavati da servizi di piattaforma di base con dati personali provenienti da altro servizio offerto dal *gatekeeper* stesso o da terzi a meno che l'utente finale non abbia prestato il proprio consenso. Una speciale regolamentazione è posta altresì per favorire la modifica o la revoca del consenso degli interessati.

[5] Il tema, affrontato nel corso di un Convegno organizzato dalla Facoltà di Giurisprudenza dell'Università di Roma Tre nel mese di ottobre, trova fondamento nel collegamento normativo tra lo Statuto dei lavoratori e il Codice privacy, sia per quanto concerne la raccolta e l'elaborazione delle informazioni sul dipendente (art. 113 Codice e art. 8 St. Lav.), sia nell'utilizzo degli strumenti tecnologici per lo svolgimento e il controllo dell'attività lavorativa (art. 114 Codice e art. 4 St. Lav.), secondo quanto consentito dall'art. 88 del Regolamento UE 2016/679. Tale collegamento è anche consacrato nella previsione di carattere sanzionatorio della violazione di tali norme.

proposals 2021 e per l'intensificazione delle interlocuzioni con il Garante della Protezione dei Dati Personali (Garante privacy).

Sono proseguiti l'attività di esame e valutazione delle segnalazioni di potenziali violazioni di dati personali per la ricostruzione degli eventi che possono rappresentare *data breach*[6] e l'impegno relativo alla partecipazione alle reti (*network*) costituite tra RPD delle Autorità amministrative indipendenti nazionali e tra *Data Protection Officer* delle Banche centrali nazionali e delle Autorità nazionali competenti in seno al SEBC.

Sono stati inoltre rilasciati i pareri a corredo delle valutazioni di impatto sulla protezione dei dati sui nuovi trattamenti (c.d. DPIA[7]), derivanti in prevalenza in area istituzionale dalla concentrazione e dallo sviluppo delle iniziative informatiche che implicano la gestione di dati personali promosse dalle Strutture interessate ed è stata esercitata la sorveglianza specifica sui trattamenti di dati effettuati dalla Banca, essenzialmente sull'articolazione e sulla coerenza del censimento operato dalle Strutture attraverso il Registro obbligatorio previsto dall'art. 30 del GDPR.

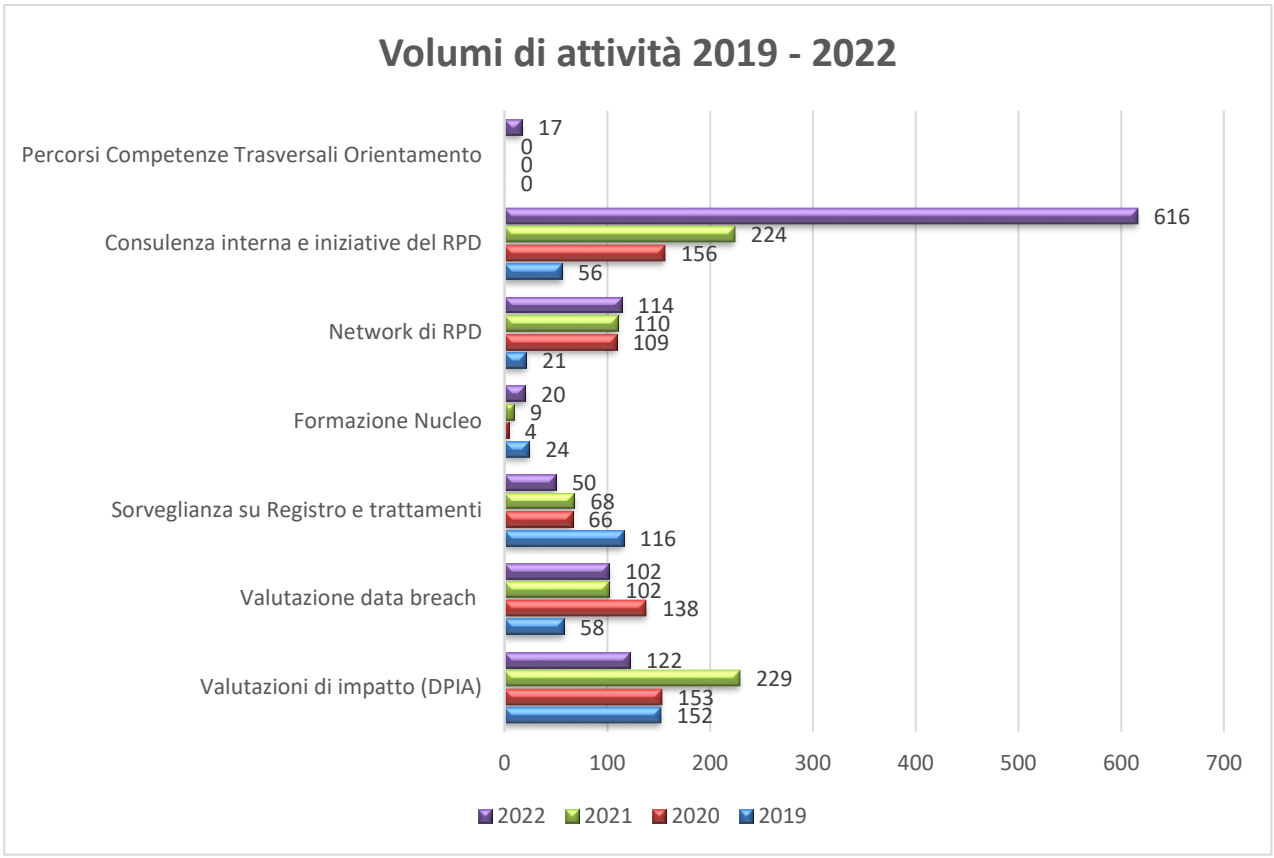
In relazione all'evoluzione del contesto in cui devono essere esercitati i compiti di consulenza e sorveglianza della funzione di RPD, nel 2022 è stata inoltre incrementata l'attività di formazione specialistica degli addetti. Va infine rilevato che la funzione di RPD ha preso parte per la prima volta all'offerta formativa dei "Percorsi per le competenze trasversali e per l'orientamento" (PCTO) per l'anno scolastico 2021-2022, rivolto a un gruppo di studenti di un liceo classico romano (13-17 giugno 2022).

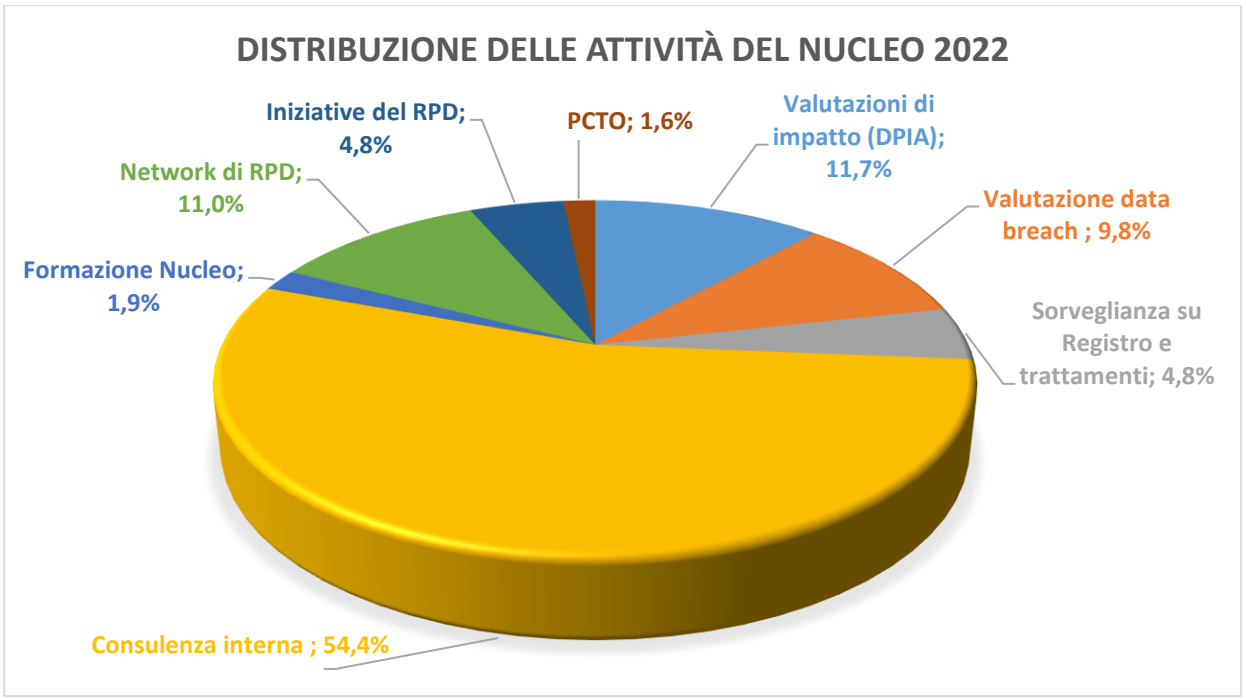
Nei grafici seguenti si fornisce una rappresentazione quantitativa dei volumi dell'attività svolta in raffronto con gli anni precedenti e per composizione interna dell'assorbimento delle risorse dedicate.

Nei paragrafi successivi si dà conto in maggior dettaglio del lavoro svolto nei diversi ambiti di competenza.

[6] Art. 33 GDPR.

[7] La valutazione di impatto sulla protezione dei dati (DPIA) è un processo finalizzato – di norma a seguito di modifiche tecnologiche od organizzative - a riesaminare il trattamento dei dati, valutarne la necessità e la proporzionalità in termini di minimizzazione dei dati utilizzati e dei tempi di conservazione, esaminarne i rischi per i diritti e le libertà delle persone fisiche destinatarie del trattamento e determinare le misure di sicurezza adeguate per mitigarli.





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

Lo svolgimento di compiti di sorveglianza in materia di protezione dei dati personali nell'attività dell'Istituto implica il coinvolgimento del RPD nelle forme di collaborazione con il Garante privacy e nelle richieste da questo rivolte alla Banca.

Al quadro delle relazioni in argomento va in particolare ascritta l'iniziativa, promossa dal Garante privacy, volta a costituire una rete dei RPD del settore bancario, per acquisire conoscenza dei fenomeni di effettiva rilevanza nel comparto e individuare possibili profili di coordinamento con l'Autorità in materia di protezione dei dati personali: a tale network è stato invitato a partecipare anche il RPD della Banca[8].

Nell'anno la funzione del RPD ha anche collaborato a un'analisi approfondita della *compliance* con la normativa sulla protezione dei dati personali sollecitata dal Garante privacy sull'Anagrafe dei Soggetti gestita dalla Banca: sono state fornite articolate informazioni su ampiezza del trattamento effettuato, specifiche finalità perseguite, natura dei dati personali oggetto di trattamento, modalità di raccolta, base giuridica nel quadro delle fonti che disciplinano i poteri della Banca alla luce dell'art. 6, par. 3, lett. b), del GDPR e dell'art. 2-ter del Codice privacy, nonché sul rispetto degli altri principi posti dal GDPR e dell'esercizio dei diritti da parte degli interessati.

Va segnalata infine la cooperazione prestata dal RPD nell'ottemperanza a due richieste di informazioni rivolte alla Banca dal Garante privacy ai sensi dell'art. 157 Codice privacy.

2.2 Le consultazioni del RPD.

L'attività di consulenza sull'applicazione della normativa sulla privacy che il RPD svolge in modo stabile nel confronto dialettico con le Strutture e il Servizio Organizzazione è stata recepita in modo organico nel 6 ° aggiornamento della circolare 257/2004, emanato nel mese di ottobre del 2022. Tale attività si è accresciuta in maniera sensibile nel corso dell'anno in relazione alle numerose e varie esigenze di applicazione e osservanza della normativa sulla privacy.

I compiti consultivi, che si affiancano ai pareri espressi sui casi di *data breach* e sulle valutazioni di impatto sulla protezione dei dati ai sensi degli artt. 33 e 35 del GDPR, hanno riguardato un'ampia casistica. Essi hanno avuto ad oggetto:

- l'accordo quadro tra Dipartimento Economia e Statistica e l'Agenzia Nazionale Politiche Attive del Lavoro (ANPAL), per consentire alla Banca di accedere ai dati elementari di cui l'ANPAL è titolare allo scopo di migliorare il funzionamento del sistema delle politiche attive e proseguire nella pubblicazione di analisi sulla congiuntura del mercato del lavoro con standard di sicurezza idonei a tutelare la riservatezza dei dati personali ai sensi dell'art. 5-ter , c. 2 del d. lgs. 33/2013;
- la revisione della normativa sulla gestione documentale e archivistica, in modo da individuare la coerenza nei tempi di conservazione e/o nei criteri di cancellazione dei dati riportati nel Registro dei trattamenti dalle Strutture (c.d. *data retention period*) con il Piano di conservazione (Massimario di selezione e scarto)[9];

[8] I lavori della "rete" hanno preso avvio il 12 dicembre 2022. Considerato il numero elevato di istituti bancari e di RPD coinvolti per ragioni di pratica funzionalità dell'organismo il Garante privacy ha proceduto, con la collaborazione di ABI e Federcasse, a costituire un gruppo di RPD rappresentativi delle aree di riferimento del settore.

[9] Nella disciplina della materia le nuove Linee guida AGID (giugno 2021) prevedono espressamente che sia sentito il RPD in merito al Manuale della gestione documentale e al Manuale/Piano della conservazione.

- i rapporti di contitolarità tra Banca d'Italia in qualità di gestore della Tesoreria della Stato e INPS in base alla Convenzione per l'esecuzione dei servizi di pagamento delle prestazioni non pensionistiche, nel trattamento dei dati personali connessi alle attività di pagamento in funzione dell'interesse pubblico perseguito da ciascuna delle Istituzioni nell'erogazione delle prestazioni. La Banca in quanto Titolare del trattamento utilizza tali dati in forma aggregata anche per il monitoraggio del fabbisogno statale di liquidità, che concorre alle decisioni di politica monetaria nell'ambito del Sistema europeo delle Banche centrali (SEBC);
- la nomina della Banca d'Italia in qualità di responsabile del trattamento dei dati, ai sensi dell'art. 28 del GDPR, nella gestione per conto dei medici competenti dell'Istituto delle informazioni per lo svolgimento delle attività connesse con la sorveglianza sanitaria obbligatoria tramite supporto cartaceo o elettronico attraverso la procedura SICURWEB;
- la definizione di due accordi di collaborazione tra la Banca e l'Agenzia per la Cybersicurezza Nazionale (ACN), ai sensi dell'art. 15 della legge n. 241/1990, per lo scambio informativo e la cooperazione per la protezione dalle minacce *cyber* e la conduzione delle procedure informatiche di concorso pubblico per il reclutamento del personale;
- il Regolamento concernente il trattamento dei dati personali effettuato dalla Banca d'Italia nell'ambito della gestione degli esposti riguardanti la trasparenza delle condizioni contrattuali, la correttezza dei rapporti tra intermediari e clienti e i diritti e gli obblighi delle parti nella prestazione dei servizi di pagamento, materie sulle quali la Banca d'Italia svolge una funzione da considerarsi di rilevante interesse pubblico[10];
- la revisione del Codice deontologico per i trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, su iniziativa dell'Istat, con il duplice obiettivo di aggiornare la regolamentazione, a seguito del provvedimento del Garante della protezione dei dati personali n. 133 del 15 aprile 2021, e semplificare gli adempimenti necessari al fine del trattamento dei dati personali a fini statistici;
- la designazione quali responsabili del trattamento dei dati delle banche commerciali aderenti allo schema nazionale di cambio istituito dal D.l. 17 maggio 2022, n. 50 per la conversione nella valuta degli Stati membri ospitanti delle banconote in hryvnia a beneficio degli sfollati provenienti dall'Ucraina, sulla base di una convenzione tra ciascuna Banca Centrale Nazionale e la Banca Nazionale di Ucraina[11];
- un approfondimento sul trattamento dei dati personali raccolti dalla Banca al centro e presso la rete territoriale nell'ambito delle attività di educazione finanziaria;
- la definizione di un accordo di accreditamento per la gestione di un Laboratorio di analisi con accesso da remoto, predisposto tra l'ISTAT e la Banca secondo quanto consentito

[10] La fonte normativa di legittimazione del relativo trattamento dati è stata emanata ai sensi degli articoli 6 par. 3 lettera b), 9 par. 2 lettera g), e 10 del GDPR, nonché degli articoli 2-ter, 2-sexies, comma 1 e 2-octies, comma 3, del Decreto legislativo 196/2003 (Codice privacy). L'atto ha ottenuto il favorevole parere preventivo del Garante privacy (provv. n. 78 del 24 febbraio 2022) ai sensi degli artt. 36, par. 4, e 58, par. 3, lett. b), del GDPR (cfr. anche *infra* paragrafo 2.4).

[11] L'operazione è stata sollecitata dalla Raccomandazione del Consiglio dell'Unione Europea del 19 aprile 2022 (2022/C 166/01): i dati personali dei profughi sono stati raccolti nella piattaforma EDAHEX messa a disposizione dalla BCE, che si è occupata del relativo trattamento anch'essa quale responsabile del trattamento dei dati per conto delle BCN di riferimento.

dall'art. 5-ter del D.lgs. 14 marzo 2013, n. 33, che disciplina l'accesso per fini scientifici ai dati elementari raccolti per finalità statistiche dagli enti e dagli uffici del Sistema statistico nazionale (SISTAN): per gli aspetti privacy dell'accordo l'Istat riveste il ruolo di titolare del trattamento dei dati elaborati e la Banca quello di responsabile ai sensi dell'art. 28 del GDPR per il funzionamento del Laboratorio;

- lo svolgimento di attività di formazione congiunta tra la Banca e l'IVASS, mediante la stipula di una Convenzione per la realizzazione di un'offerta unificata, comprendente l'intero spettro delle iniziative di formazione tecnico-specialistica e trasversale, che prevede la designazione della Banca come responsabile del trattamento, ai sensi dell'art. 28 del GDPR, in relazione alle operazioni di trattamento dei dati personali dei dipendenti dell'IVASS.

2.3 La sorveglianza sul Registro delle attività di trattamento

L'attività di sorveglianza del RPD sul Registro delle attività di trattamento tenuto dalla Banca si è concentrata nel 2022 sul monitoraggio periodico del complesso delle informazioni iscritte nel Registro[12], con la finalità di verificare la completezza e la coerenza delle descrizioni dei trattamenti censiti dalle Strutture competenti (214 al 31 dicembre).

L' attività come di consueto è stata svolta con cadenza semestrale e ha messo in evidenza che:

- la crescita del numero dei trattamenti censiti è stata determinata dalla differenziazione operata in relazione alla specificità delle attività o dei processi di lavoro di riferimento, in particolare nell'ambito dei compiti di supervisione, in linea con la prassi sviluppata a livello comunitario;
- la distribuzione interna dei trattamenti mantiene significative diversificazioni tra Dipartimenti o altre strutture non dipartimentali e mostra una concentrazione particolare nei Dipartimenti Risorse umane Comunicazione e Informazione, Mercati e sistemi di pagamento e, più recentemente, anche Vigilanza bancaria e finanziaria (complessivamente 110 trattamenti);
- la qualità informativa è significativamente migliorata per effetto della progressiva precisazione degli elementi obbligatori e integrativi di decrizione del trattamento;
- un numero elevato di trattamenti riporta i tempi di conservazione dei dati.

Su tale ultimo punto, a fronte della perdurante difficoltà di realizzare una compiuta valutazione dei tempi di conservazione dei dati personali in rapporto alle finalità dei trattamenti eseguiti, nella recente modifica della normativa interna sulla protezione dei dati (circ. 257), in attuazione del principio di accountability e sulla base dei risultati del lavoro di una specifica Task-force sugli indirizzi per la conservazione dei dati personali, è stata promossa un'analisi delle finalità dei trattamenti volta a supportare la determinazione dei termini di cancellazione dei dati, che si dovrà concludere nella prima parte dell'anno 2023.

12 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 Regolamento UE 2016/679 il Responsabile della Protezione dei Dati conduce con regolarità il monitoraggio del Registro con l'obiettivo di verificare la completezza e la coerenza dei trattamenti censiti, nonché di osservare complessivamente l'efficacia informativa dei contenuti.

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

Nel corso dell'anno il RPD ha fornito il suo parere per dieci *Data Protection Impact Assessment* - DPIA riguardanti trattamenti di dati la cui esposizione a rischi per gli interessati, unitamente allo specifico fabbisogno di misure protettive adeguate, è stata rivalutata in dipendenza di progetti informatici o procedure di lavoro oggetto di studio o di revisione[13].

Nell'ambito delle funzioni istituzionali sono state valutate le implicazioni sui trattamenti di dati personali dello sviluppo dei seguenti progetti:

- nuova "Piattaforma candidature ABF", disegnata per realizzare un archivio informatizzato della documentazione inerente alla selezione dei candidati a componenti dei Collegi dell'Arbitro Bancario Finanziario (ABF), semplificare la raccolta e l'analisi delle manifestazioni d'interesse creando un fascicolo elettronico per ciascuna candidatura presentata, corredato delle informazioni legalmente desumibili da banche dati pubbliche;
- realizzazione di una applicazione informatica basata sulla metodologia di Knowledge Graph (ragionamento automatico)[14] volta a ricostruire un quadro completo degli assetti partecipativi al capitale degli intermediari vigilati mediante l'integrazione e l'organizzazione delle informazioni ottenibili da una molteplicità di fonti o comunicazioni esterne (es. Infocamere, Consob, Orbis, verbali assembleari di approvazione del bilancio, bilanci, variazioni di assetti proprietari, patti di sindacato), per supportare la gestione di diversi procedimenti amministrativi di vigilanza e anche attività di vigilanza extra-procedimentali[15];
- creazione di un nuovo servizio ICT, destinato agli analisti di vigilanza per l'attività off-site e on-site a supporto dell'analisi della *Corporate Governance*, per organizzare le informazioni in una base dati omogenea e rafforzare l'analisi delle prassi degli organi collegiali e dell'attività dell'intermediario vigilato[16];
- *Gestione delle informazioni relative alle operazioni segnalate come sospette dalle strutture della Banca d'Italia*, finalizzata ad affinare gli archivi e le funzionalità disponibili per la produzione dei flussi

---

[13] 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 privacy ex art. 35.4 GDPR (cfr. Provvedimento n. 467 dell'11 ottobre 2018). La funzione del RPD ha anche concorso in qualche caso alla preliminare valutazione della ricorrenza di tale obbligo (es. acquisizione di nuove infrastrutture antimalware della Banca per i sistemi domestici e per i sistemi a sostegno dei servizi TARGET).

[14] Tale tecnologia, inquadrabile nell'intelligenza artificiale di tipo deduttivo (*automated reasoning*), si avvale di un motore di ragionamento rappresentativo delle informazioni come una topologia di dati strutturati a grafo. Un "grafo di conoscenza", noto anche come rete semantica, rappresenta una rete di entità del mondo reale - cioè oggetti, eventi, situazioni o concetti contestualizzati mediante un processo di *semantic enrichment* - e illustra la relazione tra loro. Queste informazioni sono di solito reperite con motore di ricerca da molteplici ambienti informativi di fonte e struttura eterogenea, memorizzate in un database a grafo e visualizzate come una struttura a grafo.

[15] A esempio, acquisto di partecipazioni qualificate nel capitale delle banche e degli intermediari non bancari, procedure di licensing e di autorizzazione degli intermediari bancari e non bancari, modifiche dello statuto sociale, verifiche del possesso dei requisiti degli esponenti aziendali (Fit and Proper assessment).

[16] Per l'osservanza dei vincoli normativi posti al trattamento parzialmente automatizzato di dati anche personali, alla soluzione informatica sono stati espressamente imposti limiti agli atti contenenti dati personali di carattere particolare o giudiziario.

informativi verso la UIF e delle segnalazioni delle operazioni sospette, agevolando le Unità della Banca nell'osservanza della normativa antiriciclaggio[17];

- realizzazione del sottosistema di "Rendicontazione" della Tesoreria dello Stato nell'ambito del programma di "*Reingegnerizzazione delle procedure di tesoreria*" (ReTes), diretto ad adeguare gli strumenti di informazione al Ministero dell'Economia e delle Finanze e alle altre controparti istituzionali interessate e migliorare la capacità di analisi e di previsione delle determinanti del fabbisogno del settore statale (e del settore pubblico) nonché il monitoraggio dei conti delle Amministrazioni Locali.

Sempre in ambito istituzionale la funzione ha fornito consulenza nella definizione della nuova piattaforma "SupTech – Analisi Esposti", progetto per la realizzazione di una piattaforma di elaborazione informatica per la semplificazione della gestione degli esposti bancari con l'ausilio di meccanismi di intelligenza artificiale (tecniche di *text mining* e *machine learning*), che ha posto l'esigenza di effettuare una complessa valutazione di impatto sulla protezione dei dati, non soltanto perché riguardante un trattamento su larga scala di dati personali di varie tipologie con il ricorso a soluzioni tecnologiche innovative, ma anche perché:

- ha preventivamente richiesto l'adozione di una specifica base giuridica regolamentare per la disciplina del trattamento dei dati, in quanto la tipologia di informazioni personali contenute negli esposti è molto ampia e non definibile *a priori*, non potendosi escludere che i soggetti segnalanti vi riversino anche dati soggetti a tutela rafforzata, come quelli c.d. particolari o giudiziari, il cui trattamento postula la determinazione delle modalità e delle tipologie ammissibili ad opera di specifiche fonti normative primarie o regolamentari[18];
- è stata sottoposta alla consultazione preventiva del Garante (art. 36, par. 1 GDPR), a causa del potenziale rischio elevato del trattamento per i soggetti interessati, per le modalità e le cautele da adottare nel trattamento dei dati personali contenuti nei documenti (esposti) oggetto dell'elaborazione automatizzata[19].

Sul versante aziendale, non minore è stata l'attenzione alla prevenzione della rischiosità dei trattamenti di dati personali. Sono state infatti valutate le implicazioni sul trattamento dei dati di alcuni importanti progetti informatici, quali:

---

[17] La Banca d'Italia, pur non rientrando tra i destinatari diretti degli obblighi previsti dal decreto antiriciclaggio (D.lgs. n. 231/2007), a presidio del rischio di riciclaggio e di finanziamento del terrorismo collabora alla identificazione, alla raccolta e alla conservazione dei dati relativi alle operazioni effettuate con l'utenza, comunicando alla UIF le operazioni ritenute "sospette" e le Segnalazioni Antiriciclaggio Aggregate S.AR.A.. Il D.lgs. n. 90/2017, nel dare attuazione alla Direttiva UE 849/2015 (c.d. "IV Direttiva antiriciclaggio"), ha innovato il D.lgs. 231/2007, introducendo, tra l'altro: i) modifiche in tema di obblighi di registrazione e conservazione delle informazioni; ii) nuove previsioni circa la trasmissione di informazioni alla UIF individuate sulla base di criteri oggettivi (art. 47).

[18] Le fonti di legittimazione del trattamento dei dati della specie sono disciplinate dagli artt. 9 e 10 GDPR, nonché dagli artt. da 2-*sexies* a 2-*octies* del D.lgs. 196/2003 Codice privacy. Atteso che il Regolamento a suo tempo emanato dalla Banca per la legittimazione del trattamento di dati cosiddetti "sensibili" e "giudiziari" (Regolamento 6 novembre 2015) autorizza la raccolta ed elaborazione di dati giudiziari per finalità di vigilanza prudenziale, si è resa necessaria la previa adozione di un nuovo strumento normativo, di rango regolamentare, per il trattamento dei dati in questione per finalità di vigilanza di tutela.

[19] Lo schema di regolamento, in applicazione dell'art. 36, par. 4 del GDPR, è stato sottoposto al parere preventivo del Garante della Protezione dei Dati Personali, il quale il 24 febbraio 2022 ha pronunciato il proprio avviso favorevole ai sensi dell'art. 154, comma 5 del Codice privacy (e lo ha pubblicato sul proprio sito web). Contestualmente anche le misure di protezione individuate nella valutazione di impatto sono state ritenute adeguate.

- il consolidamento su un'unica piattaforma di *Application Delivery Controller* (*ADC*) delle funzionalità attualmente erogate dalla *webfarm* aziendale[20] per presidiare efficacemente il traffico dati in ingresso e in uscita da applicazioni o servizi web;
- la reingegnerizzazione del sistema di gestione e di controllo degli eventi di sicurezza (*SIEM-Security Information and Event Management*) nonché della connessa rilevazione delle vulnerabilità presenti nei sistemi informatici dell'Istituto;
- la gestione integrata del sistema informativo della Consulenza Legale, allo scopo di snellire il reperimento e la condivisione delle informazioni necessarie per gli avvocati della Banca e per il personale amministrativo addetto, mediante l'integrazione di tutte le fonti informative e l'interazione con gli strumenti e le piattaforme del sistema giudiziario e con le procedure e le altre applicazioni della Banca;
- la realizzazione di un nuovo Portale con la funzione di *entry-point* unico per l'interlocuzione diretta delle strutture della Banca che forniscono i servizi interni con il personale in servizio e in quiescenza, integrando le procedure, le diverse fonti informative esistenti e i canali utilizzati per la trasmissione delle informazioni.

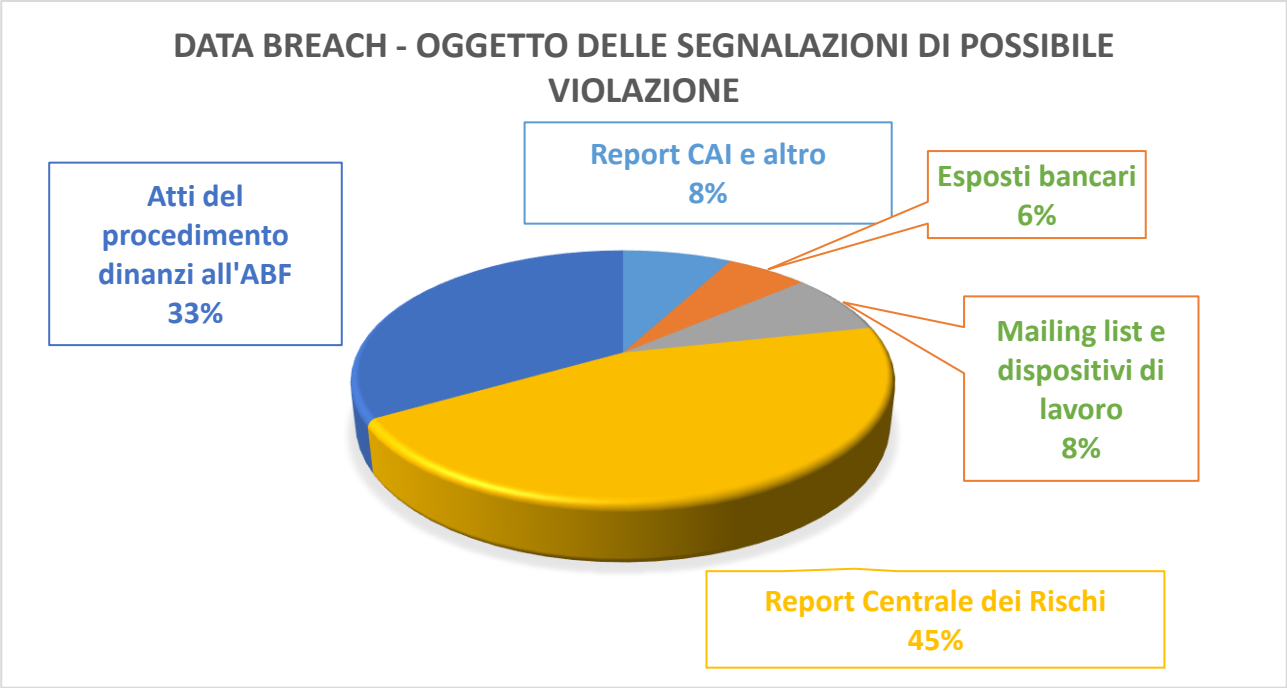
2.5 Le segnalazioni dei data breach.

Nel 2022 sono state sottoposte alla valutazione del RPD 51 potenziali violazioni dei dati personali (c.d. *data breach*) nella stessa misura di quelle segnalate l'anno precedente: su di esse il RPD ha fornito al Servizio Organizzazione il suo parere sul rischio per i diritti e le libertà degli interessati, ai fini delle conseguenti determinazioni previste dal GDPR[21].

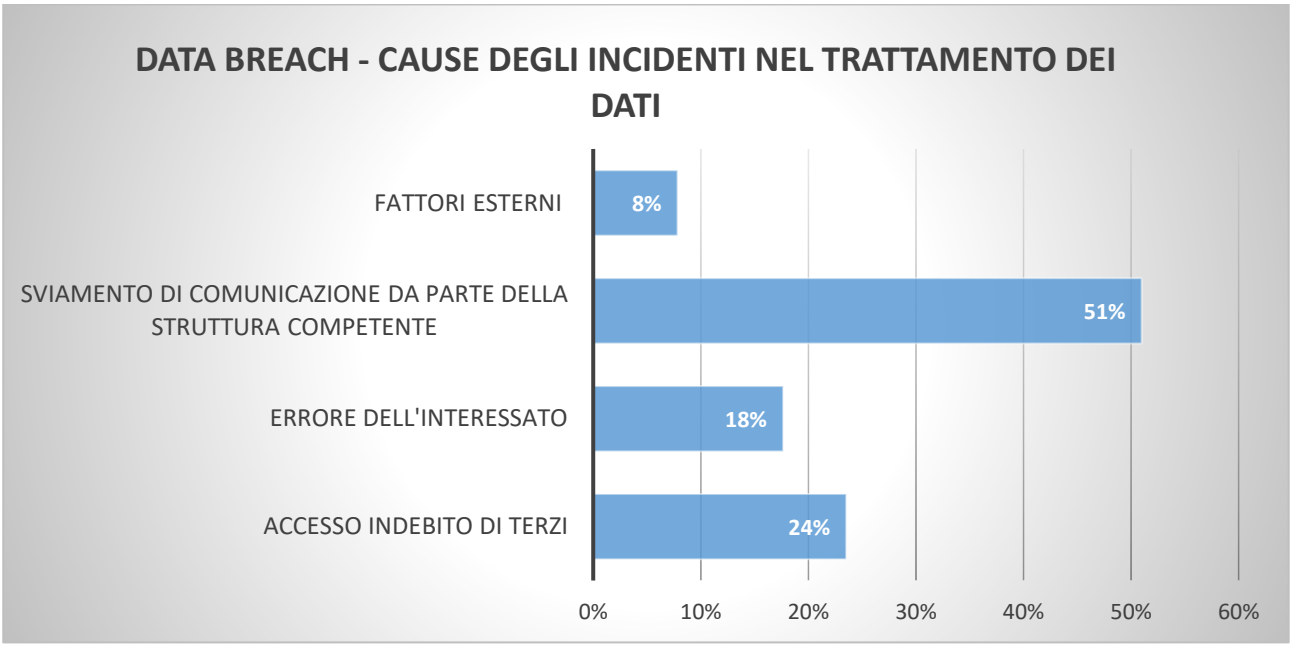
L'ambito nel quale maggiormente si concentrano i rischi di violazione dei dati resta quello delle comunicazioni con l'utenza negli accessi alla Centrale dei Rischi e nella gestione dei procedimenti dinanzi all'ABF (cfr. grafico seguente), sebbene non vadano trascurati la potenziale lesività dei meno frequenti incidenti riguardanti la gestione degli esposti bancari e l'utilizzo delle *mailing list* nelle diverse attività di ufficio.

[20] Infrastruttura a supporto di numerose applicazioni per l'erogazione su internet di servizi *web* verso l'esterno in favore di cittadini e per lo scambio di dati informativo/statistici con enti pubblici.

[21] Il RPD fornisce al Titolare del trattamento un parere che rafforza gli elementi di valutazione in caso di perdita, alterazione o sviamento accidentali 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) e qualora, poi, la violazione presenti un rischio elevato per le libertà e i diritti individuali, di darne comunicazione, senza ingiustificato ritardo, anche agli interessati.



Analizzando le cause di tali eventi si rileva che l'azione di prevenzione del rischio di violazione deve orientarsi prevalentemente sul raffozamento delle misure dirette a presidiare la comunicazione dei dati nei casi richiesti dalle diverse attività svolte (cfr. grafico seguente).



Per la quasi totalità degli eventi di presunto *data breach* non è stato necessario effettuare la segnalazione al Garante Privacy prevista dall'art. 33 del GDPR, visto il livello trascurabile di rischio per i soggetti interessati nelle varie fattispecie alla luce delle cautele adottate. La valutazione dei rischi derivanti da dette violazioni ha indotto solo in un caso a effettuare la predetta segnalazione[22], mentre un altro caso è stato oggetto di una richiesta di informazioni da parte del Garante privacy, in relazione a un accertamento da parte dell'Autorità.

[22] Si è trattato di un accesso tramite sportello *online* alla situazione in Centrale dei Rischi di una persona giuridica, sulla base

Tra i fattori che hanno concorso successivamente a contenere il rischio di effetti lesivi dei potenziali *data breach* è risultato prevalente quello delle misure adottate dalla Banca unitamente alla cooperazione di eventuali terzi coinvolti.

Al fine di consentire alla funzione che svolge i compiti di titolare del trattamento, e al RPD che deve rendere un parere in merito, di valutare il livello di rischio della violazione e di mettere in atto con tempestività adeguati rimedi, il RPD ha cooperato alla definizione di Linee guida per la gestione delle segnalazioni e per lo svolgimento omogeneo e strutturato dell'istruttoria dei data breach, correlate di un template per la segnalazione, che sono state diffuse alla rete territoriale nell'aprile dell'anno in esame.

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.

Nell'approssimarsi del termine di adeguamento fissato dalla Linee guida del Garante *privacy* per la gestione dei cookies e degli altri strumenti informatici di tracciamento (gennaio 2022), il RPD ha interessato la funzione competente per avviare una verifica della conformità delle impostazioni dei siti web di pertinenza della Banca, anche in relazione ai collegamenti con eventuali siti terzi, a quanto indicato dal Garante.

Sono stati altresì condotti approfondimenti tematici riguardo alle linee guida sulla metodologia di calcolo delle sanzioni amministrative connesse alle violazioni del GDPR, poste in pubblica consultazione dal Comitato europeo per la protezione dei dati (EDPB), all'assetto privacy della UIF alla luce delle connotazioni di autonomia dell'Unità, e ad altri argomenti oggetto di pareri e provvedimenti del Garante privacy.

In sede di costituzione dei *team* di supporto incaricati di seguire lo sviluppo dei 10 progetti ammessi a Milano Hub all'esito della *Call for proposals 2021*[23], per l'apporto di un contributo delle diverse competenze in relazione alle caratteristiche di ciascun progetto e alle esigenze di supporto segnalate dai proponenti selezionati, la funzione del Responsabile della Protezione dei Dati (RPD) è stata chiamata a partecipare a due dei predetti *team* di supporto: i componenti del Nucleo di supporto del RPD hanno preso parte ai lavori con riferimento ai progetti "*Alternative Scoring by Digital Data Insights*"(settore *Deposit and lending*) e "*WoX Edge: uno smart speaker customer-centric e inclusivo per la filiale del futuro*" (settore *Payments*).

Nel quadro dei compiti di sensibilizzazione e di formazione sulla privacy che il RPD deve curare nei confronti delle strutture[24], è stato avviato un programma di iniziative diretto a promuovere la prevenzione delle potenziali violazioni della sicurezza dei dati personali.

---

di autocertificazione rivelatasi non rispondente al vero, per la quale è stata altresì effettuata segnalazione all'Autorità giudiziaria.

[23] Il concorso di idee ha avuto come tema "*Il contributo dell'intelligenza artificiale nel migliorare l'offerta dei servizi bancari, finanziari e di pagamento alle imprese, alle famiglie e alla pubblica amministrazione, con particolare riguardo ai profili di inclusione finanziaria, efficace tutela del consumatore e sicurezza dei dati*".

[24] Cfr. art. 39, par. 1, lett. b) del GDPR: « *Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: (...) b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché (...) la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo».*

In particolare, nei confronti delle strutture dell'Amministrazione centrale il RPD, coadiuvato dal Nucleo di supporto, ha organizzato il 17 novembre 2022 un seminario interno sulla protezione dati e sulle questioni di *cybersecurity* ad essa connesse (seguito anche in streaming dalle Filiali), con l'intervento del Responsabile Protezione Dati dell'Istituto Superiore di Sanità, esperto in protezione dati e sistemi di sicurezza per la gestione delle informazioni.

Le principali tematiche affrontate hanno riguardato la tutela dei dati personali di fronte alle moderne minacce di violazione con particolare riferimento agli aspetti caratterizzanti introdotti dal Regolamento UE 2016/687 (GDPR): tutela dei diritti e delle libertà, *accountability*, sicurezza dei dati personali dal punto di vista tecnico e organizzativo.

Ci si è inoltre soffermati sull'analisi e sulla gestione nell'eventuale perdita accidentale o dolosa, modifica o divulgazione non autorizzata del dato personale (c.d. data breach): sono state esaminate le misure da intraprendere, che comportano la valutazione del rischio anche da parte del RPD, espressa in un apposito parere, e la valutazione dell'eventuale notifica al Garante e agli interessati.

Conformemente alle linee di indirizzo del Garante privacy sul DPO in ambito pubblico, il RPD ha continuato a mantenere il confronto con il Servizio Organizzazione nelle funzioni di Titolare del trattamento su questioni applicative della disciplina sulla *privacy* all'interno della Banca.

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 BCE, tenutisi nel corso dell'anno, sono stati trattati argomenti di interesse comune per l'osservanza della regolamentazione europea sulla privacy. Gli aspetti di *compliance* sono stati esaminati con riferimento a: il ricorso a servizi in *cloud* [25] da parte della BCE concernente un progetto di *Customer Relationship Management tool*, la cui valutazione di impatto è stata sottoposta a consultazione preventiva dell'*European Data Protection Supervisor* (EDPS); il progetto *ESCB Collaboration Prototype on Microsoft Teams* per un nuovo sistema di comunicazione e di condivisione di documenti basato su *MS Teams* cui partecipano 14 Banche Centrali Nazionali, inclusa la Banca d'Italia; il manuale *Artificial Intelligence Playbook* redatto dalla BCE per l'adozione dell'Intelligenza Artificiale secondo soluzioni conformi alla normativa dell'EUDPR (Reg. UE 1725/2018) che dovrà essere rivisto una volta approvata la regolamentazione europea sull'intelligenza artificiale; la definizione di un nuovo accordo per la gestione di una piattaforma centralizzata gestita da EBA con le istituzioni interessate (denominato EuReCa) per il coordinamento delle informazioni antiriciclaggio[26].

[25] A seguito della sentenza della Corte di Giustizia dell'Unione Europea del luglio 2020 che ha annullato la Decisione di adeguatezza della Commissione che legittimava il trasferimento di dati personali dall'Unione europea verso gli Stati Uniti, nell'assunto che il livello di protezione fosse sostanzialmente equivalente a quello richiesto dal GDPR (art. 45, paragrafo 2, lettera a).

[26] L'istituzione dell'archivio centralizzato è prevista dalla *EBA Regulation* (art. 9a Regolamento UE 1093/2010).

Il *network* sarà chiamato a contribuire alla definizione di un nuovo *Joint controllership agreement* tra la BCE-SSM e le NCAs per il riparto delle responsabilità nei trattamenti di dati relativi alle procedure autorizzative di supervisione bancaria, che sarà definito nel corso del 2023.

3.2 L'attività nazionale.

Il RPD partecipa stabilmente al *Network* dei DPO delle Autorità indipendenti nazionali[27], costituitosi successivamente all'entrata in applicazione del GDPR allo scopo di avere uno scambio istituzionale sui temi di protezione dei dati personali nell'ambito delle rispettive amministrazioni[28].

Gli incontri a cadenza mensile hanno riguardato in particolare: gli approfondimenti sulla figura del responsabile del trattamento dei dati; alcune prime riflessioni sui rapporti tra intelligenza artificiale e tutela dei dati; l'organizzazione di un seminario aperto a tutti i soggetti interessati appartenenti alle istituzioni partecipanti, tenutosi presso l'ANAC il 25 novembre 2022, nel quale è stato affrontato il rapporto tra Pubblica Amministrazione italiana e tutela dei dati personali nell'attività svolta, a quattro anni dall'entrata in vigore del Regolamento europeo, da un punto di vista amministrativo, normativo, informatico e ispettivo.

E' stato inoltre pubblicato sulla rivista elettronica Forum PA un documento a cura del *Network* concernente la figura del Responsabile del trattamento dei dati nella normativa comunitaria e nelle applicazioni nazionali (Documento n. 2 del 4 luglio 2022).

Alla fine del 2022, dopo tre anni di riunioni "a distanza", la Banca ha proposto al *Network* di avviare una nuova stagione di incontri periodici in presenza, ospitandone il primo del nuovo anno. La riunione del 23 gennaio 2023 è stata aperta dal RPD della Banca, che ha sottolineato la rilevanza del lavoro svolto dal *Network* a partire dall'applicazione del GDPR e ha evidenziato la sensibilità da sempre prestata dalla Banca d'Italia al tema della tutela dei dati personali, attestata anche dall'assetto organizzativo apprestato.

Nell'apertura dell'incontro, il RPD ha evidenziato alcuni aspetti che rivestono particolare importanza per la Banca:

- la sensibilità al tema della *cybersicurezza*, alimentata dalle continue minacce alla riservatezza che subiscono le persone e le istituzioni, e l'applicazione dell'intelligenza artificiale nel mondo della finanza nel quale i dati personali rappresentano la risorsa determinante per il funzionamento degli algoritmi, ma anche postulano il continuo rispetto dei limiti normativi ad automatismi decisori e profilazioni;
- il progetto relativo alla creazione dell'euro digitale, che sta progressivamente prendendo forma sotto la guida del membro italiano del Comitato esecutivo della Banca Centrale Europea, nella

---

[27] 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 (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), dell'Istituto Nazionale di Statistica (ISTAT) in qualità di osservatore.

[28] La rete è disciplinata da *Regole di organizzazione e funzionamento del Network di RPD delle Autorità Amministrative indipendenti* deliberate a maggioranza assoluta il 24 settembre 2021.

cui realizzazione la tutela della *privacy* è stata indicata come uno degli aspetti di maggiore sensibilità per il pubblico (43% delle risposte nella consultazione pubblica effettuata dalla BCE nel 2020).

La riunione ha portato alla definizione metodologica delle attività di studio del *Network*, organizzata in seminari interni diretti all'aggiornamento su profili di interesse concreto per le istituzioni partecipanti, in gruppi di studio volti alla produzione di documenti di approfondimento e in seminari esterni aperti alla partecipazione di altre amministrazioni destinati al confronto con esperti e all'incontro con il Garante *privacy*.