BANCA D'ITALIA
EUROSISTEMA

Relazione del Responsabile della Protezione dei Dati

Anno 2021

Roma, marzo 2022

INDICE

Introduzione.

L'anno 2021, ancora condizionato da contesti emergenziali sanitari, ha visto una crescente domanda di condivisione delle informazioni per finalità di pubblico interesse, unita alla manifestazione del valore sociale ed economico legato alla disponibilità di dati personali e alla loro circolazione in ambito privato; ciò ha rinnovato l'attenzione sulla tutela dei dati personali, sollecitata dall'opinione pubblica sempre più sensibile alle istanze di protezione della *privacy*.

In un'ottica di impegno civile, l'Istituto ha messo a disposizione delle autorità sanitarie il proprio *know how* statistico per condividere informazioni e basi dati, utili a comprendere le modalità di diffusione della pandemia e mettere a punto le misure più appropriate di risposta.

Sono state avviate le iniziative dirette a favorire l'integrazione e l'interoperabilità tra i diversi sistemi informativi per l'accesso telematico in sicurezza dei privati ai servizi della Pubblica Amministrazione, proteggendo la riservatezza dei dati dei cittadini; l'informatica nel settore pubblico appare progressivamente indirizzata verso lo sviluppo delle infrastrutture digitali e l'adozione di un modello *cloud* per la Pubblica Amministrazione, che richiede particolari cautele per la protezione dei dati nell'affidamento del servizio a providers esterni, sovente anche extraeuropei.

Nel contesto comunitario si registra la spinta dell'Unione Europea verso un'articolata regolamentazione della circolazione delle informazioni e, in particolare, dei dati personali, caratterizzata dal "pacchetto digitale" predisposto dalla Commissione europea finalizzato a facilitare l'ulteriore uso e la condivisione dei dati (personali) tra più parti pubbliche e con i privati all'interno della cosiddetta *data economy*.

Anche il progetto di emissione dell'euro digitale, che consentirebbe di disporre di una moneta digitale emessa dalla banca centrale, fin dalle prime indagini della BCE ha riscontrato l'interesse della collettività purché l'aspettativa di sicurezza dello strumento di pagamento sia corrisposta da un'adeguata tutela della *privacy* del cittadino[1].

La protezione dei dati personali è cruciale nel quadro della tecnologia digitale che, attraverso l'espansione della connettività (es. 5G, *Internet of Things*) e l'ampliamento dei metodi di cattura e sfruttamento delle informazioni, tende a sfuggire alla regolamentazione europea e pone un problema di "sovranità tecnologica"nella circolazione dei dati.

Il tema è evidentemente connesso con quello dell'emersione del *cyber risk*, le cui implicazioni si estendono ben oltre l'ambito dei dati personali e richiedono presidi e strumenti di mitigazione innovativi e ad ampio raggio d'azione[2].

---

[1] L'integrazione dell'euro digitale con le infrastrutture di pagamento e il supporto di adeguata tecnologia sono considerati cruciali per contemperare l'esigenza di un soddisfacente livello di protezione dei dati personali degli utenti con il necessario potere di controllo della banca centrale a salvaguardia degli interessi pubblici legati alla circolazione monetaria (non ultimo anche il contrasto delle attività illecite). Su tale argomento si registra la richiesta indirizzata alla BCE e alle Istituzioni comunitarie dall'European Data Protection Board di promuovere fin dalla fase di progettazione un livello elevato di protezione della *privacy* e dei dati personali per rafforzare la fiducia degli utenti finali nell'offerta di un euro digitale, fattore chiave ai fini del suo successo (EDPB; sessione plenaria del 21 giugno 2021).

[2] L'impellenza del presidio di tale rischio ha indotto il Governo a promuovere l'istituzione di un'Agenzia per la cybersicurezza nazionale (d.l. 14 giugno 2021, n. 82, convertito con modificazioni in legge 4 agosto 2021 n. 109).

All'interno dell'organizzazione dell'Istituto, il Responsabile della Protezione dei Dati (RPD), rappresentato 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, ha esercitato le proprie funzioni mantenendo costante il confronto dialettico con le strutture e, in particolare, con il Servizio Organizzazione, a cui sono attribuiti i compiti di Titolare del trattamento dei dati attribuiti alla Banca.

Il RPD nell'autonomo esercizio del proprio ruolo riferisce direttamente al Vertice aziendale, predisponendo una relazione annuale per il Direttorio, che viene pubblicata sul sito web dell'Istituto. In relazione al considerevole volume di attività svolta, è stata costituita nell'anno un'apposita unità organizzativa (Nucleo) a supporto del RPD, divenuta operante nel mese di ottobre.

1. Il quadro normativo.

L'anno trascorso è stato principalmente caratterizzato dall'intervento del legislatore che, con l'art. 9 del decreto legge 8 ottobre 2021 n. 139, convertito con modifiche dalla legge 3 dicembre 2021, n. 205, ha innovato alcune significative disposizioni del Codice della protezione dei dati personali (Codice *privacy*; d.lgs. 30 giugno 2003 n. 196). In particolare:

- accanto alle preesistenti fonti di legittimazione al trattamento dei dati da parte della P.A. per "*esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*" (artt. 6.1 e 6.3 GDPR [3]), costituite solo da legge o regolamento, sono stati previsti anche l'"atto amministrativo generale" e la "necessità" di adempiere un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri attribuiti all'Amministrazione procedente, sempre nel rispetto dei principi e della tutela dei diritti e delle libertà degli interessati stabiliti dal GDPR;
- la condivisione tra pubbliche amministrazioni e la divulgazione a terzi dei dati che la P.A. può trattare sono state rese possibili, nei casi non contemplati da norma di legge o di regolamento, ove consentite dalle predette nuove forme di legittimazione al trattamento, senza la previa autorizzazione del Garante della Protezione dei Dati Personali (Garante) espressa o tacita (mediante silenzio-assenso);
- è stato consentito alla P.A. il trattamento di categorie "particolari" di dati per motivi di interesse pubblico rilevante[4] purché i limiti e le condizioni del trattamento di cui all'art. 2-*sexies* del Codice *privacy* (motivi di pubblico interesse, tipi di dati trattati, operazioni eseguibili e misure appropriate e specifiche a tutela degli interessati) siano esplicitati almeno in un atto amministrativo generale.

[3] Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, Regolamento generale sulla protezione dei dati.

[4] Si tratta del caso previsto dall'art. 9.2 lett. g) GDPR; le "categorie particolari" di dati sono quelle che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica e i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Sul versante sovranazionale, la Commissione Europea ha adottato decisioni rilevanti in materia di regolazione dei rapporti che implicano trattamenti di dati personali; in particolare, sono state approvate:

- le clausole contrattuali standard volte a disciplinare il trasferimento di dati personali verso Paesi terzi od organizzazioni extraeuropee per colmare una lacuna creatasi con la pronuncia della Corte di Giustizia dell'Unione Europea 16 luglio 2020 che aveva annullato la Decisione di adeguatezza del c.d. *Privacy Shield* tra UE e USA[5];
- le clausole contrattuali standard dirette a disciplinare i rapporti tra titolari di trattamento dei dati e responsabili del trattamento nel contesto dell'Unione[6].

In tema di regolamentazione occorre segnalare altresì che nel dicembre 2021 si è anche definito il quadro delle proposte legislative racchiuse nel pacchetto digitale predisposto dalla Commissione europea per regolare in maniera uniforme a livello comunitario lo sfruttamento dei dati (personali) nell'ambito del sistema economico generale[7].

Il Comitato europeo per la protezione dei dati personali (EDPB)[8] ha di recente suggerito alla Commissione UE che nelle iniziative da avviare sulla normativa digitale e sulla gestione delle informazioni sia posta l'attenzione sui rischi per i diritti fondamentali alla riservatezza e alla protezione dei dati e sulla necessità dell'effettiva cooperazione e dello scambio di informazioni tra le autorità di controllo per evitare il rischio di incongruenze.

Va infine registrata l'adozione il 28 giugno 2021 di una decisione di adeguatezza ai sensi dell'art. 45 del GDPR da parte della Commissione europea, con la quale si è riconosciuto che il livello di protezione dei dati apprestato nel Regno Unito è essenzialmente equivalente a quello assicurato all'interno dell'Unione dal GDPR: tale provvedimento ha pertanto definito la questione della legittimità dei trasferimenti di dati personali verso l'ex Stato Membro, ponendo termine alle incertezze in materia determinatesi in esito alla "Brexit"[9].

---

5 Commissione UE, Decision 2021-914 del 4 giugno 2021, in attuazione della previsione dell'art. 46.2, lett. c) del GDPR.

6 Commissione UE, Decision 2021-915 del 4 giugno 2021, in attuazione della previsione dell'art. 28.7 del GDPR e dell'art. 29.7 del Regolamento (UE) n. 2018/1725 EUDPR. Criteri di orientamento in materia erano stati già individuati dalle Linee guida dell'EDPB in materia, adottate nel settembre 2020 (n. 7/2020).

7 Il pacchetto comprende un disegno di regolamento in materia di mercati digitali (*Digital Markets Act*), un disegno sui servizi digitali (*Digital Services Act*), il *Data Governance Act* (DGA) e la proposta di regolamento sull'intelligenza artificiale (AIR).

8 Il comitato europeo per la protezione dei dati è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE. Il comitato europeo per la protezione dei dati è composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (GEPD). Ne fanno altresì parte le autorità di controllo degli Stati EFTA/SEE per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati (GDPR), senza però che i loro rappresentanti godano del diritto di voto o di essere eletti presidente o vicepresidenti. Il comitato è istituito dal regolamento generale sulla protezione dei dati e ha sede a Bruxelles. La Commissione europea e, per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati, l'Autorità di vigilanza EFTA hanno titolo a partecipare alle attività e alle riunioni del comitato senza diritto di voto.

9 La decisione, operante dal 1° luglio 2021 al termine del periodo transitorio di tolleranza stabilito dall'Accordo di uscita della Gran Bretagna del 30 dicembre 2020, ha una validità di 4 anni e prevede un meccanismo di riesame periodico delle disposizioni autorizzative.

2. Il consolidamento della funzione del RPD.

Nell'ultimo triennio l'operatività legata all'esercizio delle funzioni del RPD si è consolidata, soprattutto nell'interazione con le diverse strutture della Banca, che fanno riferimento al RPD non solo nei processi di consultazione tipizzati dalla normativa, ma sempre più spesso allorché affrontano problematiche connesse con la normativa a tutela della *privacy* e con la partecipazione alle sedi di collaborazione in ambito nazionale ed europeo.

Anche per questo si è deciso di attribuire evidenza strutturale a questa funzione, destinata a crescere d'importanza in ragione della pervasività della disciplina sulla *privacy* e della sua diffusione pressoché in tutti i settori di attività della Banca.

Al fine di conoscere le soluzioni adottate da istituzioni comparabili all'Istituto, quali Banche Centrali Nazionali e Autorità Nazionali Competenti per la supervisione, è stata condotta un'indagine presso i *Data Protection Officer* (DPO[10]) della rete operante in ambito SEBC. L'analisi comparata delle informazioni raccolte, grazie alla collaborazione di un significativo numero di RPD interpellati, ha consentito di avere un quadro d'insieme dei diversi assetti che la funzione di assistenza di RPD assume nei differenti contesti organizzativi. Questa visione di insieme ha ispirato la soluzione infine adottata dalla Banca.

Dalla *survey* è emerso che la collocazione del RPD non è omogenea; dipende dalla specificità dei diversi assetti organizzativi ed è legata alle funzioni esercitate e alle dimensioni aziendali: in alcune rilevanti Istituzioni la collocazione è autonoma rispetto alle altre strutture, in altre il RPD è inserito in una unità che assolve anche altri compiti caratterizzati da analoga autonomia, come la *compliance,* gli affari legali, la sicurezza informatica, la gestione dei rischi. La linea di riporto del RPD è di norma diretta nei confronti degli organi di vertice, senza intermediazione di livelli decisionali.

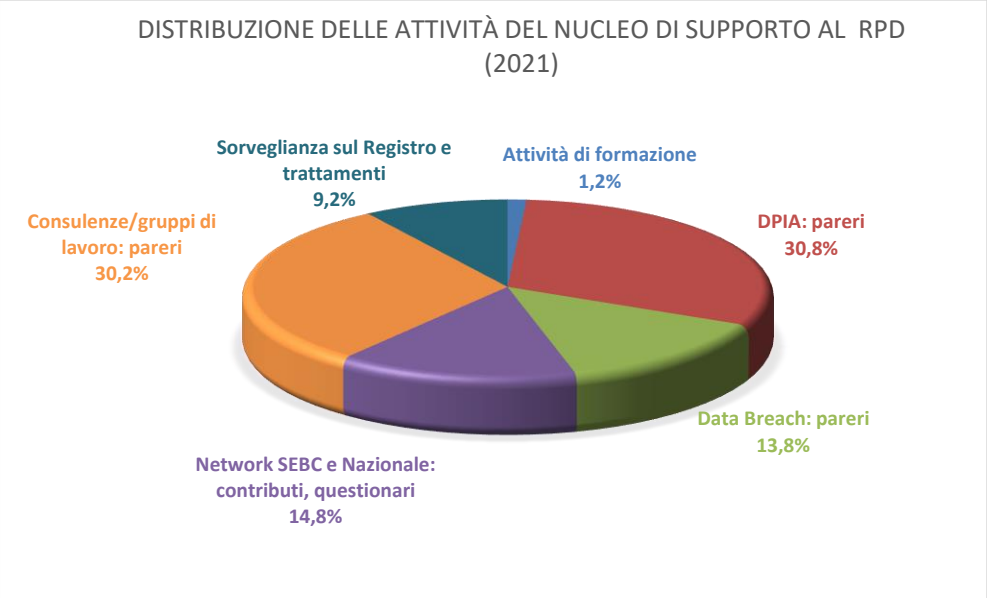
A supporto dei compiti del RPD, si riscontra in prevalenza un compendio di risorse dedicate alla sorveglianza sulla protezione dei dati che spesso ha una configurazione organizzativa autonoma. Inoltre, numerose istituzioni hanno avvertito l'esigenza di istituire "referenti *privacy*" (*data protection coordinators, data protection contact points*) presso le articolazioni organizzative o territoriali per esigenze di coordinamento d'azione.

L'istituzione nel luglio scorso di un'unità organizzativa (Nucleo) a supporto del RPD, entrata a regime nell'ultima parte dell'anno ha completato il percorso di crescita della funzione e rappresenta il riconoscimento dell'importanza dei compiti svolti e della sua autorevolezza come punto di riferimento interno ed esterno alla Banca.

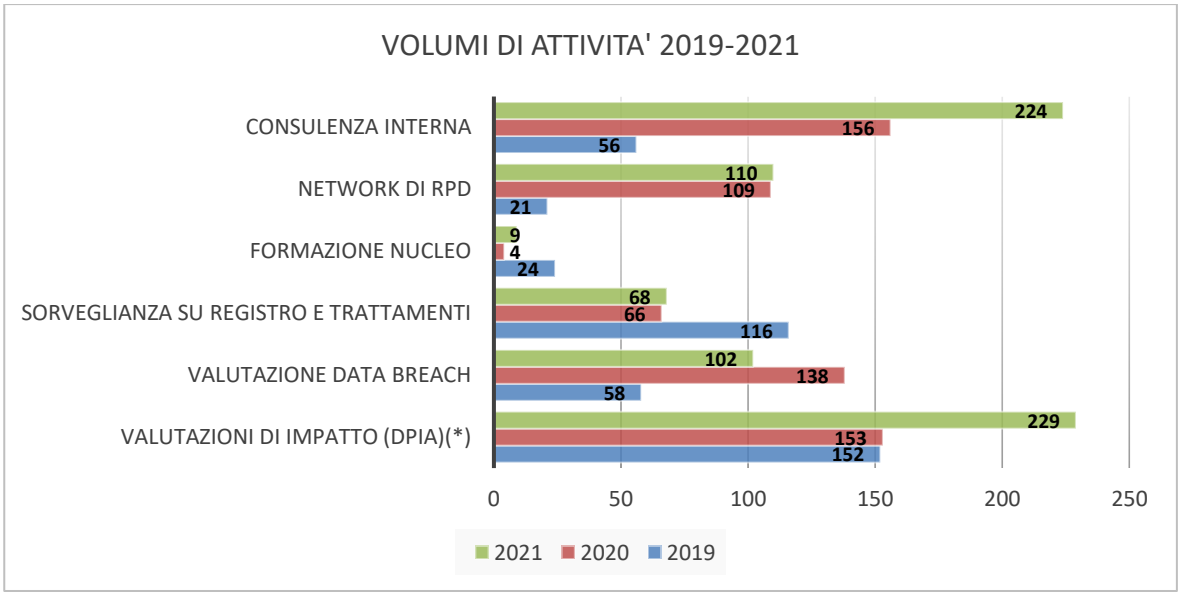
3. L'attività svolta nel 2021.

Nel corso dell'anno l'attività svolta dal RPD si è arricchita di nuove fattispecie. Alla consulenza alle strutture dell'Istituto nella quotidiana operatività e nell'avvio di progetti innovativi, quando si trovano ad analizzare problematiche connesse con il trattamento dei dati personali, si è affiancato un continuo confronto con le altre Autorità italiane ed europee.

[10] Acronimo inglese di RPD.



I pareri rilasciati sulle valutazioni di impatto sui singoli trattamenti (c.d. *assessment* DPIA [11]), che richiedono un approfondimento di analisi e di confronto con le strutture interessate, hanno assorbito una maggiore quota di attività per numero e complessità; mentre l'impegno per la ricostruzione degli eventi che hanno provocato i *data breach*[12] si è manifestato - una volta acquisite le informazioni utili dalle strutture segnalanti - nella formulazione di un parere al titolare del trattamento entro i termini previsti dal GDPR.



A seguito della costituzione del Nucleo, nell'ultima parte dell'anno ha preso avvio anche un'attività di formazione, destinata a intensificarsi in relazione al pianificato utilizzo di nuovi addetti.

[11] 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.

[12] Art. 33 GDPR.

3.1. I rapporti con il Garante.

In linea con quanto previsto dal GDPR, il RPD coopera con il Garante fungendo da figura di collegamento per tutte le questioni riguardanti il trattamento dei dati personali che coinvolgono l'Istituto.

Nel corso dell'anno gli incontri del RPD con esponenti del Garante hanno riguardato l'esame di temi di portata generale, quali la corretta valutazione delle segnalazioni di *data breach*, la disciplina condivisa del trattamento dei dati tra diversi titolari pubblici, le condizioni di liceità delle nuove tecnologie di trattamento dei dati.

Il RPD ha inoltre preso parte a incontri con il Garante nell'ambito di un procedimento di consultazione preventiva per il rilascio del parere previsto dalla normativa sulla proposta di Regolamento della Banca per la disciplina del trattamento dei dati personali nella gestione degli esposti bancari.

Nel quadro dei proficui rapporti intervenuti tra le due Autorità, il Garante ha richiesto la collaborazione della Banca per approfondire, insieme con le associazioni rappresentative dell'industria bancaria, modalità di trattamento di dati personali che presentano elementi di complessità, quali:

i) la profilazione della clientela attraverso fonti informative di ampia diffusione per ottemperare a obblighi imposti dalla normativa (es. antiriciclaggio);
ii) il contemperamento dell'esercizio del diritto di accesso degli interessati ai sensi del GDPR con le forme di accesso e di conoscenza da parte dei clienti dell'attività degli intermediari;
iii) l'interposizione di nuovi intermediari, anche non bancari, nel trattamento dei dati raccolti nelle relazioni tra banche e clienti concernenti i servizi di pagamento e quelli informativi sulla gestione dei rapporti, fenomeno legittimato dall'attuazione della seconda Direttiva europea sui servizi di pagamento.

Le modalità della collaborazione sono in via di definizione.

3.2. Consultazioni del RPD.

Lo svolgimento di compiti consultivi in materia di protezione dei dati personali nei confronti delle strutture interne ha occupato una consistente quota delle attività, mantenendo la tendenza alla crescita mostrata già negli anni precedenti.

Tale consulenza, ulteriore rispetto a quella formalizzata nei tipici pareri previsti dagli artt. 33 e 35 del GDPR (valutazione dei *data breach* e valutazioni di impatto sulla protezione dei dati) ha avuto ad oggetto, tra le attività più significative:

- un contributo alla definizione di un *Agreement* tra le *Financial Intelligence Unit* (FIU) dell'UE e la Commissione europea per la gestione da parte di quest'ultima della rete informatica FIU.net, deputata allo scambio di informazioni tra le FIU dell'Unione Europea nell'adempimento del mandato istituzionale: in particolare, riguardo ai profili di *data protection* si è convenuto che ciascuna FIU rimanga "Titolare" (*data controller*) dei trattamenti di dati personali effettuati tramite la rete FIU.net, con gli obblighi previsti dalle disposizioni del GDPR, mentre la

Commissione assume il ruolo di "Responsabile del trattamento" (*data processor*) per conto delle FIU, con i conseguenti vincoli e obblighi previsti dal EUDPR[13];

- la partecipazione alla messa a punto degli accordi tra la Banca e l'Istituto di Vigilanza sulle Assicurazioni (IVASS) per lo svolgimento da parte della Banca dei servizi di gestione della documentazione digitalizzata, della comunicazione istituzionale e dei rapporti con gli organi di stampa per conto dell'IVASS. In tale ambito per il trattamento dei dati personali inerente allo svolgimento delle funzioni affidate, di cui l'IVASS è titolare, la Banca ha assunto il ruolo di Responsabile del trattamento dei dati a norma dell'art. 28 del GDPR e i relativi obblighi, con le cautele necessarie a preservare la segregazione della sfera di autonomia delle due istituzioni[14];
- la consultazione su alcuni aspetti di *compliance* normativa riguardanti il bando di selezione e la *privacy policy* nell'iniziativa denominata *Techsprint*, lanciata dalla Banca in collaborazione con il *BIS Innovation Hub* nell'ambito della presidenza italiana del G20 per sollecitare il potenziale delle nuove tecnologie nell'innovazione finanziaria, analizzandone eventuali problemi per la regolazione e la supervisione[15];
- di seguito alla partecipazione ai lavori che hanno condotto nel 2020 alla conclusione di un *Memorandum of Understanding on joint controllership* per i dati personali trattati nel *Securities Financing Transactions Data Store* (SFTDS) dalle banche centrali del SEBC partecipanti alla costituzione di tale archivio[16], la collaborazione con il Servizio Rilevazioni ed Elaborazioni Statistiche e con il Servizio Organizzazione per gli aspetti di protezione dati relativi agli "*User Terms of Reference*" ossia le disposizioni applicative emanate per gli utenti del *Data Store*.

Va inoltre registrato il crescente coinvolgimento del RPD nelle attività preparatorie alla stipula di accordi o protocolli di collaborazione con amministrazioni dello Stato o di altri Enti pubblici per finalità di analisi statistica o ricerca economica preordinate allo svolgimento di compiti istituzionali della Banca o di servizi congiunti; le forme di collaborazione implicano nella maggior parte dei casi:

- la comunicazione e lo scambio di basi informative contenenti anche dati personali, da inquadrare nelle diverse fattispecie normative che ne possano legittimare il trattamento, determinandone ruoli *privacy* e connesse responsabilità;
- la definizione di disposizioni convenzionali atte ad assicurare l'adempimento degli obblighi di protezione dei dati personali derivanti dalle norme e dalle regole deontologiche eventualmente applicabili[17].

---

13 Regolamento UE 2018/1725 del Parlamento Europeo e del Consiglio del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle Istituzioni, degli Organi e degli Organismi dell'Unione.

14 La collaborazione si inquadra nella previsione dell'art. 13 della legge istitutiva (d.l. 6 luglio 2012, n. 95, convertito dalla legge 7 agosto 2012, n. 135) che consente all'IVASS ai fini dell'esercizio delle sue funzioni di avvalersi delle infrastrutture tecnologiche della Banca d'Italia.

15 L'iniziativa, promossa con la *Bank of International Settlement*, è consistita in un pubblico concorso di idee aperto a sviluppatori, designer, creatori, scienziati di dati, startupper, esperti di marketing digitale e comunicazione con l'obiettivo di sviluppare il potenziale delle tecnologie innovative per risolvere i problemi operativi nei settori della finanza verde e sostenibile assegnati nel bando.

16 Otre alla BCE e alla Banca d'Italia, la Nationale Bank van België, la Deutsche Bundesbank, il Banco de España, la Banque de France, la Banque centrale du Luxembourg e De Nederlandsche Bank.

17 Con particolare riguardo alla comunicazione di dati, in alternativa alla generale previsione dell'art. 2-ter del Codice *privacy*, che legittima la trasmissione dei dati personali tra istituzioni pubbliche proprio in quanto finalizzata all'adempimento di

La funzione del RPD è stata infine presente e ha fornito un proprio contributo nei lavori della *Task Force* interservizi che ha condotto analisi e approfondimenti per l'individuazione di tempi e criteri di conservazione dei dati personali trattati dall'Istituto e dalla UIF nell'esercizio delle proprie funzioni.

Nella relazione conclusiva è stato evidenziato che il principio di limitazione della conservazione dei dati personali, sancito dall'art. 5 GDPR, impone a ogni titolare del trattamento l'archiviazione dei dati trattati nell'ambito delle proprie attività per un arco di tempo non superiore al perseguimento delle finalità per cui i dati sono stati acquisiti, al termine del quale ne deve essere disposta la cancellazione o la definitiva anonimizzazione; ciascuna struttura deve sistematicamente rivalutare tempi di conservazione dei dati adeguati alle finalità e, in collaborazione con la funzione informatica, seguendo i criteri di *privacy by design* e *privacy by default*, deve individuare, al momento della progettazione o della manutenzione evolutiva di procedure che gestiscono dati personali, le misure tecnico-organizzative dirette all'eliminazione o all'anonimizzazione dei dati personali allo scadere del termine individuato.

3.3. Sorveglianza sul Registro delle attività di trattamento.

La sorveglianza del RPD sul Registro delle attività di trattamento tenuto dalla Banca nel 2021 si è focalizzata su una delle due direttrici già delineate nel corso dell'anno precedente e precisamente sul monitoraggio periodico sul complesso delle informazioni iscritte nel Registro delle attività di trattamento. Il monitoraggio del Registro[18] avviene di norma con cadenza semestrale e ha l'obiettivo di verificare la completezza e la coerenza delle descrizioni dei trattamenti censiti dalle Strutture competenti (192 al 31 dicembre).

Nell'anno in esame, il monitoraggio ha messo in evidenza la progressiva definizione delle informazioni trattate, rilevando nel contempo l'opportunità di individuare una tipizzazione armonizzata dei contenuti al fine di migliorare la sua capacità informativa.

La qualità complessiva delle informazioni iscritte nel Registro dei trattamenti ha mostrato in ogni caso un livello adeguato, in rapporto a un numero di trattamenti poco superiore a quello dell'anno precedente.

La distribuzione interna dei trattamenti pone in luce significative diversificazioni tra Dipartimenti o altre strutture, ascrivibili alla presenza variabile di dati personali nella gestione dei compiti e nelle procedure di lavoro.

La non uniforme numerosità dei trattamenti censiti nei Dipartimenti della Banca lascia però supporre che vi possa essere un diverso livello di capillarità nella loro classificazione: tale circostanza suggerisce in prospettiva di promuoverne un'individuazione omogenea.

compiti di interesse pubblico, si richiamano qui a titolo esemplificativo l'art. 5-ter D.lgs. 33/2013 che regola l'accesso per fini scientifici ai dati elementari raccolti per finalità statistiche da Enti del Sistema statistico nazionale (Sistan) o l'art. 21 Reg. UE 223/2009 che disciplina la trasmissione dati per finalità istituzionali da Enti del Sistema statistico europeo alle Banche centrali del SEBC. Tuttavia altre fattispecie possono essere introdotte da norme speciali.

18 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 valutare complessivamente l'efficacia informativa dei contenuti.

Il monitoraggio ha permesso di promuovere un miglioramento progressivo della capacità informativa del Registro – come strumento di *accountability* della Banca nella protezione dei dati - mediante una costante azione di sensibilizzazione sulla sua importanza, condotta nei confronti delle Strutture insieme con il Titolare del trattamento (Servizio Organizzazione).

Per quanto concerne la seconda direttrice di azione, costituita dall'analisi approfondita dei singoli trattamenti, sono stati rielaborati i criteri per procedere in maniera sistematica all'*assessment* dei trattamenti iscritti nel Registro, secondo metodologie più strutturate e focalizzate sul concetto di rischio.

3.4. Le valutazioni di impatto sulla protezione dei dati (DPIA)

Nel corso del 2021 il RPD ha fornito il suo parere per 19 DPIA riguardanti trattamenti di dati di complessità e ampiezza differenti, in relazione a nuovi progetti e procedure che hanno interessato la quasi totalità delle aree della Banca[19].

Nell'ambito delle funzioni istituzionali sono stati valutati gli impatti sui nuovi trattamenti di dati personali connessi con i progetti riguardanti:

- l'automazione delle attività di raccolta, elaborazione e analisi delle informazioni necessarie per la verifica dei requisiti e dei criteri di idoneità allo svolgimento dell'incarico degli esponenti (*Fit and Proper* - FAP) di tutte le banche e degli intermediari disciplinati dal TUB, in linea con la normativa comunitaria e le linee guida dell'EBA;
- l'introduzione nell'architettura della piattaforma RADAR (Raccolta e Analisi dei Dati per l'AntiRiciclaggio) di una funzionalità evoluta (c.d. *graph analysis*) per analizzare una vasta area del patrimonio informativo a disposizione dell'UIF a supporto dei suoi compiti istituzionali;
- il rinnovamento tecnologico dell'Anagrafe di tutte le tipologie di soggetti (persone fisiche e persone giuridiche) censiti dalla Banca d'Italia nell'esercizio delle funzioni istituzionali sulla base di norme di legge e regolamentari;
- la modernizzazione sul piano tecnologico della gestione, archiviazione e diffusione dei dati della Centrale dei rischi con riferimento ai servizi informativi per gli intermediari e per i cittadini, nonché del relativo trattamento per le finalità statistiche e di ricerca economica dell'Istituto;
- la revisione dei processi operativi e la nuova soluzione IT nell'ambito della procedura ICAS per la valutazione del merito di credito delle società non finanziarie italiane, delle famiglie produttrici e consumatrici;
- la rendicontazione degli incassi e dei pagamenti eseguiti per conto dello Stato o degli altri enti pubblici che rientrano nel servizio di Tesoreria dello Stato (procedura RENTERE);
- l'ammodernamento delle modalità di raccolta e gestione delle informazioni derivanti dalle segnalazioni di intermediari e imprese sulle condizioni delle operazioni di finanziamento applicate dalle banche alla propria clientela;

[19] 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 ...*».

– la raccolta e la gestione in una base dati unica delle informazioni provenienti dalla Tesoreria, dal SIOPE/SIOPE+ e da fonti statistiche interne ed esterne al fine di consentire l'analisi dell'andamento dei conti pubblici e delle principali relazioni tra flussi finanziari pubblici e variabili macroeconomiche.

Sul versante aziendale sono state esaminate le implicazioni sul trattamento dei dati:

- relativi a tutte le informazioni trattate dalla Banca in un sistema integrato di *Information Governance* («Infogov»);
- concernenti la digitalizzazione del processo a supporto del sistema aziendale di salute e sicurezza sul lavoro, nell'ambito della sorveglianza sanitaria obbligatoria;
- del personale della Banca nell'ambito del progetto di ricerca "Le donne, il lavoro e la crescita economica"[20].

Nell'anno si è reso necessario procedere da parte delle strutture responsabili a una valutazione d'impatto con un iter procedurale più snello[21] per 26 trattamenti di dati che, selezionati tra quelli privi di una valutazione specifica a partire dall'entrata in vigore del GDPR[22] (complessivamente 140 trattamenti), per caratteristiche e contenuti necessitavano di un riesame atto a confermarne l'adeguatezza in termini di compliance e di presidio del rischio per gli interessati.

In particolare, i processi analizzati hanno riguardato le procedure del sistema dei pagamenti, di gestione del personale, di assistenza fiscale, di riscontro delle operazioni finanziarie, di scambi informativi con autorità e altre istituzioni nazionali e internazionali a fini di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, per le attività del personale (accettazione doni, investimenti e operazioni finanziarie private) registrate ai fini della *compliance* per l'etica e prevenzione della corruzione.

3.5. Le segnalazioni dei *data breach*.

Nel 2021 sono state sottoposte alla valutazione del RPD 51 potenziali violazioni dei dati personali (c.d. *data breach*) a fronte delle 69 segnalate l'anno precedente: su di esse il RPD ha fornito al Servizio Organizzazione il parere sul rischio per i diritti e le libertà degli interessati, ai fini delle conseguenti determinazioni previste dal GDPR[23]. La riduzione del numero dei *data breach* è da mettere in relazione all'opera di sensibilizzazione compiuta dal RPD nei confronti della rete territoriale. Si tratta infatti, nella maggioranza dei casi, di violazioni riconducibili a errori

[20] Il progetto fa parte di uno studio generale sulle relazioni tra la crescita economica globale e una maggiore partecipazione femminile al mercato del lavoro, in rapporto alle scelte lavorative, al grado di valorizzazione delle donne nel lavoro e ad altri fattori. Esso ha costituito uno dei filoni di indagine che ha interessato un'analisi dei dati relativi ai dipendenti della Banca, realizzato dal Servizio Struttura Economica in collaborazione con il Servizio Gestione del personale, che ha richiesto particolari presidi di anonimato del trattamento e dei risultati nella stretta osservanza delle indicazioni delle Regole deontologiche in materia (Allegato A.5 al Codice *privacy* approvato dal Garante *privacy* con provvedimento n. 515 del 19 dicembre 2018, artt. 4 e 5).

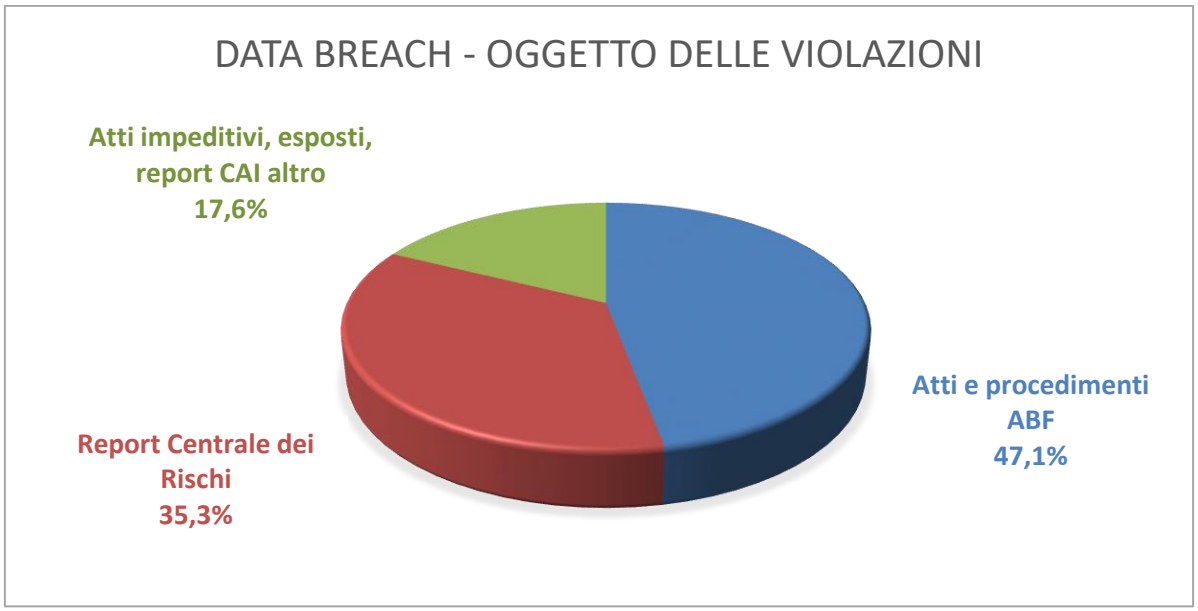
[21] Per la formalizzazione del DPIA di questo particolare novero di trattamenti, nella misura in cui non si sia avuta alcuna variazione del rischio residuo per gli interessati, sono state consentite modalità semplificate dell'iter procedurale.

[22] 25 maggio 2018.

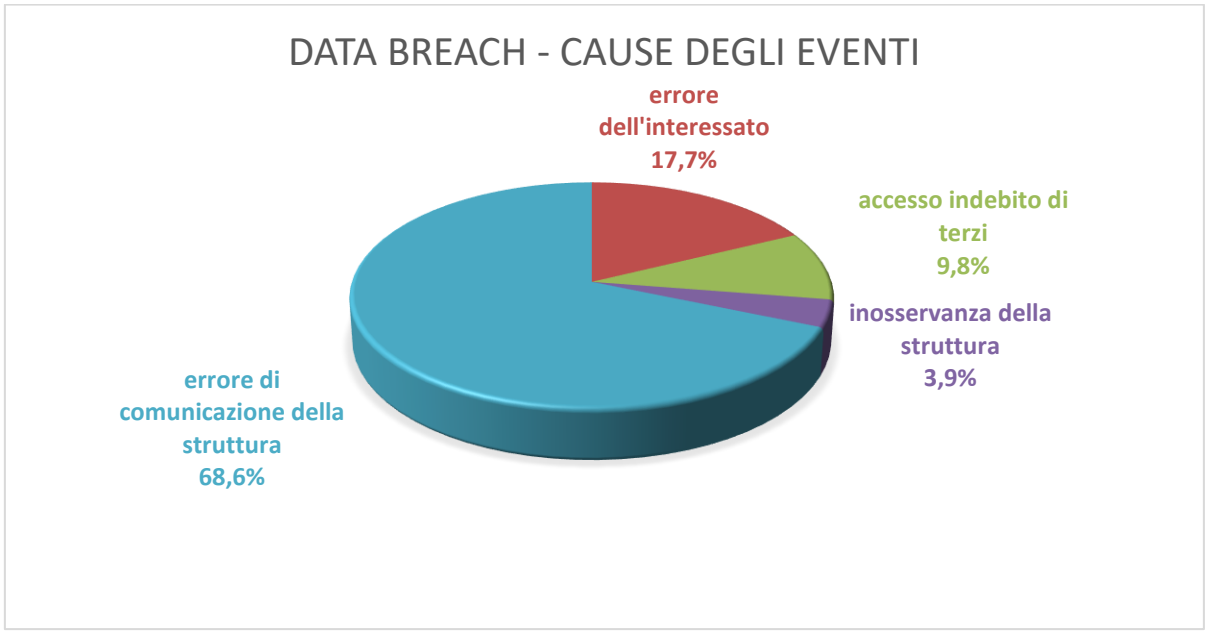
[23] Il RPD fornisce al Titolare del trattamento un parere che rafforza gli elementi di valutazione in caso di perdita, alterazione o sviamento accidentali di dati personali configurabili come *data breach*. Il GDPR (art. 33), quando si verificano i presupposti di un effettivo *data breach*, impone al 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.

operativi che possono essere mitigati con azioni di rimedio basate su un'applicazione più scrupolosa del "*four eyes principle*".

Come evidenziato dal grafico sotto riportato, gli eventi hanno riguardato prevalentemente i dati contenuti negli atti del procedimento dinanzi ai collegi dell'Arbitro Bancario Finanziario (ABF) e nei report della Centrale dei Rischi (CR).

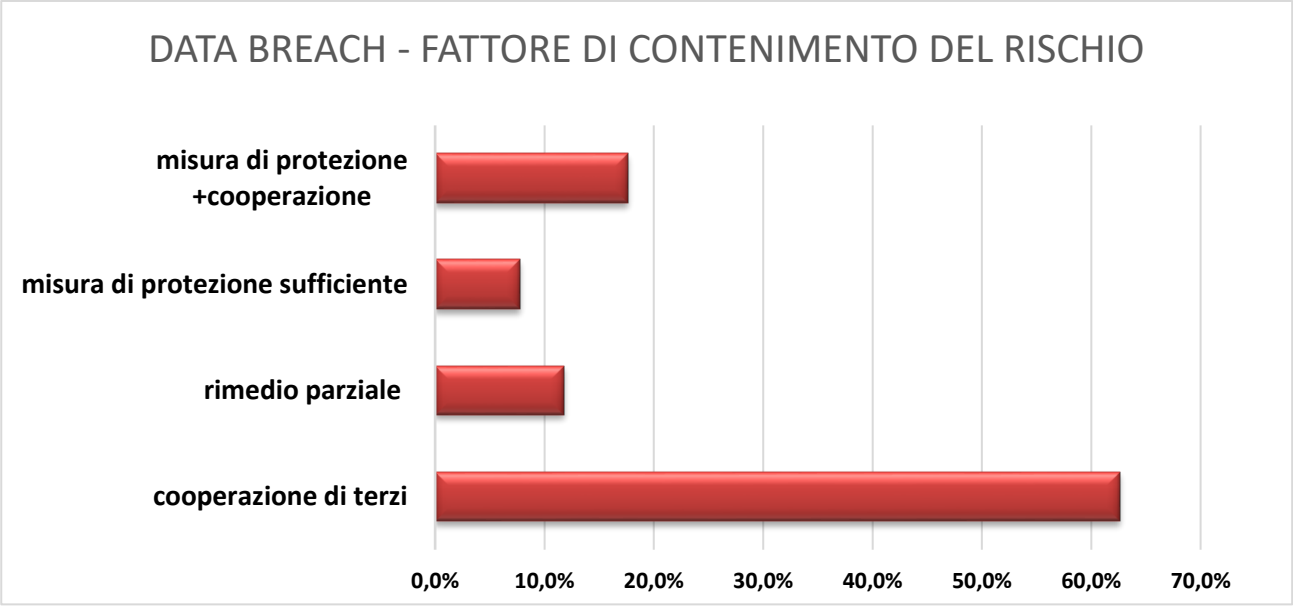


Analizzando le cause di tali eventi si rileva che essi sono dipesi prevalentemente da erronee trasmissioni di informazioni a terzi nell'ambito di taluni processi operativi della rete territoriale; in una buona parte dei casi l'incidente è stato determinato da erronea comunicazione dell'interessato e da accessi ai dati da parte di terzi privi di legittimazione, legati alla possibilità di acquisizione telematica delle informazioni.



I rischi connessi con gli eventi di *data breach* hanno indotto solo in un caso a effettuare una segnalazione al Garante, che dopo la sua istruttoria ha disposto l'archiviazione della segnalazione in relazione all'adeguatezza delle misure esistenti a tutela dell'interessato.

Tra i fattori che hanno concorso successivamente a contenere il rischio di effetti lesivi dei *data breach* risulta largamente prevalente quello della cooperazione dei terzi coinvolti accidentalmente come destinatari della comunicazione impropria dei dati, accompagnata da contromisure di protezione richieste immediatamente dalla struttura segnalante talora anche temporanee (rimedio parziale).



3.6. Le iniziative del RPD.

Nell'esercizio dei compiti di sorveglianza sull'applicazione della normativa *privacy*, il RPD sollecita anche di sua iniziativa verifiche e valutazioni per adeguare la *compliance* complessiva delle strutture.

Nell'anno, in particolare, è stata avviata l'interlocuzione con il Dipartimento Vigilanza bancaria e finanziaria per un affinamento della rappresentazione nel Registro dei trattamenti delle diverse attività di trattamento dati svolte dalla funzione[24] e per la consultazione reciproca nelle questioni riguardanti diversi ruoli rivestiti nell'attività di supervisione dalle *National Competent Authorities* e dal SSM-BCE (titolari autonomi, contitolari o responsabili del trattamento) e delle conseguenti rispettive responsabilità in materia.

[24] L'esigenza di distinguere uno specifico trattamento dati per ciascuna attività svolta nell'ambito dei compiti di supervisione, per allinearsi alla prassi sviluppata in ambito comunitario e poter gestire distintamente gli adempimenti in tema di *privacy*, è stata condivisa dal Dipartimento che si è prontamente adoperato in tal senso.

Il RPD ha fornito alla funzione del personale e alla Divisione Salute e sicurezza sul lavoro le indicazioni emergenti dalle nuove linee di indirizzo adottate dal Garante[25] sui trattamenti di dati effettuati dal datore di lavoro e dal "medico competente", derivanti dalla disciplina in materia di tutela della salute e della sicurezza nei luoghi di lavoro (d.lgs. 9 aprile 2008, n. 81). In particolare, sono stati riesaminati i ruoli *privacy* assegnati ai medici competenti e alla Banca, l'assetto delle relazioni improntate alla separatezza funzionale, l'adempimento degli obblighi del "medico competente" quale autonomo titolare del trattamento nella conduzione della sorveglianza sanitaria obbligatoria e l'adozione delle misure tecniche e organizzative adeguate alla protezione dei dati sanitari trattati.

Conformemente alle linee di indirizzo sul RPD in ambito pubblico (cfr. *supra*, par. 2), il RPD ha mantenuto costante il confronto periodico con il Servizio Organizzazione nelle funzioni di Titolare del trattamento su questioni applicative della disciplina sulla *privacy* all'interno della Banca.

Sul versante istituzionale, il RPD ha partecipato al Convegno organizzato dall'ISTAT il 23 giugno sul tema "*Protezione dei dati personali – Attività in Istat e prospettive*" nel corso del quale ha svolto un intervento e preso parte al dibattito della tavola rotonda su "Prospettive future: la parola ai Responsabili della Protezione dei Dati" assieme ai RPD dell'Agenzia delle Entrate, dell'Istituto Superiore di Sanità e dell'Istat.

L'intervento del RPD ha richiamato l'attenzione sul progetto dell'euro digitale (*euro digital currency*) e sul risultato della consultazione pubblica lanciata dalla Banca Centrale Europea, con un numero elevato mai registrato per un'iniziativa del genere della BCE, dove è emerso che cittadini e professionisti europei si aspettano da una valuta digitale innanzitutto la tutela della *privacy* (su cui converge il 43% delle risposte). Ha inoltre rappresentato l'auspicio che la normativa a protezione dai dati personali possa essere oggetto di un'azione educativa fin dalla scuola primaria: diffonderne la conoscenza attraverso iniziative ispirate al modello dell'educazione finanziaria, che le banche centrali hanno lanciato circa un ventennio fa, potrebbe essere il modo per consolidare quella cultura della legalità tanto spesso evocata nel nostro Paese.

4. La partecipazione ai network di RPD.

4.1. L'attività internazionale

Nei *meeting* dei RPD (*Data Protection Officers*) delle Banche Centrali Nazionali, della BCE e delle Autorità Nazionali Competenti per la supervisione bancaria, tenutisi nel corso dell'anno ancora in modalità a distanza, sono stati trattati e discussi argomenti di interesse comune per l'osservanza della regolamentazione europea sulla *privacy*, muovendo dalle testimonianze dell'esperienza applicativa di alcuni partecipanti al *network* o della BCE, che ha ormai assunto un ruolo stabile di coordinamento.

[25] Garante, Documento "*Il ruolo del medico competente in materia di sicurezza sul luogo di lavoro anche con riferimento al contesto emergenziale*", pubblicato il 14 maggio 2021.

Risulta inoltre che la BCE abbia deciso di adottare una soluzione organizzativa speculare a quella della Banca d'Italia, promuovendo la costituzione di una struttura specialistica di supporto all'attività del RPD.

In particolare, aspetti di *compliance* con la normativa sulla protezione dei dati personali sono stati esaminati con riferimento a:

- forme di trasferimento dei dati verso paesi terzi al di fuori dell'Unione, con particolare attenzione all'esperienza degli accordi amministrativi tra Autorità pubbliche;
- uso di piattaforme di servizi resi da fornitori statunitensi da parte di istituzioni europee in assenza di un livello di protezione adeguato[26];
- partecipazione a piattaforme per la raccolta di dati in materia antifrode e contro il finanziamento del terrorismo allestite da Autorità nazionali;
- conseguenze reputazionali della pubblicità mediatica di un *data breach*;
- ricorso a *Cloud Service Providers* nell'attività delle istituzioni partecipanti e relativi rischi;
- stato di avanzamento degli studi sull'emissione dell'euro digitale e istanze di protezione dei dati.

Per studiare le possibili forme di integrazione delle implicazioni della protezione dei dati personali nel *criticality assessment* dei progetti informatici è stato avviato al termine dell'anno, su iniziativa del RPD della BCE, un gruppo di lavoro cui partecipa un'esponente del Nucleo di supporto al RPD.

E' proseguito infine nel *network* il dibattito interno riguardante l'assetto dei ruoli *privacy* (titolari, contitolari o responsabili del trattamento) e il riparto delle responsabilità tra BCE-SSM e NCAs nei trattamenti di dati relativi alle procedure autorizzative di supervisione bancaria, nonché sui necessari *arrangements* da definire sulla materia per ottemperare al GDPR.

4.2. L'attività nazionale

Il progressivo consolidamento delle attività della rete di collegamento tra RPD delle Autorità indipendenti nazionali, costituitasi nel 2019 per finalità di confronto interistituzionale sui principali temi di protezione dei dati personali nell'ambito delle rispettive amministrazioni, è è giunto a compimento con l'approvazione delle *Regole di organizzazione e funzionamento del Network di RPD delle Autorità Amministrative indipendenti* [27].

---

[26] La Decisione della Commissione UE di adeguatezza del c.d. *Privacy Shield* UE-US, un meccanismo di autocertificazione per le società con sede negli Stati Uniti, atto a legittimare il trasferimento di dati personali dall'Unione europea verso titolari o responsabili del trattamento negli Stati Uniti, obbligati a garantire i principi stabiliti dall'UE in materia di *privacy* e assicurare agli interessati tutele paragonabili a quelle europee, è stata annullata dalla Corte di Giustizia dell'Unione Europea con sentenza del 16 luglio 2020, in quanto non idonea a garantire un livello di protezione sostanzialmente equivalente a quello richiesto dall'articolo 45, paragrafo 2, lettera a), del GDPR (in particolare per l'insufficienza dei diritti effettivi e azionabili di cui godono le persone i cui dati sono stati trasferiti verso gli USA).

[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), della Cassa per i Servizi Energetici e Ambientali (CSEA) e

Nelle riunioni tenutesi nel corso dell'anno sono stati toccati temi di interesse comune, quali i rapporti contrattuali tra Titolare e Responsabile del trattamento, la gestione dei dati personali connessi all'isolamento dei contagi e al green pass sul luogo di lavoro, le implicazioni *privacy* delle linee guida dell'AGID per la gestione documentale e la conservazione e delle linee Guida dell'ANAC in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro (*whistleblowing*), le modifiche al Codice *privacy* introdotte dal d.l. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205.

E' stato altresì completato e pubblicato un documento unitario concernente il ruolo, l'autonomia, i compiti, la collocazione organizzativa e le modalità di coinvolgimento del RPD nelle realtà pubbliche.

dell'Acquirente Unico S.p.a. (AU). Le *Regole* sono state deliberate a maggioranza assoluta nell'adunanza del 24 settembre 2021.