BANCA D'ITALIA
EUROSISTEMA

Relazione del Responsabile della Protezione dei Dati

Anno 2020

Roma, febbraio 2021

INDICE

Introduzione.

Un utilizzo corretto e trasparente dei dati personali e il riconoscimento del potere di controllo sugli stessi in capo alla persona fisica a cui si riferiscono assumono oggi crescente importanza nell'ambito della Pubblica Amministrazione, ponendo l'esigenza di trovare un giusto contemperamento con l'esercizio delle funzioni svolte nell'interesse della collettività.

La Banca si è prontamente adeguata alle previsioni normative che impongono l'istituzione del Responsabile della Protezione dei Dati (RDP)[1]; nell'organizzazione dell'Istituto, questa figura è stata identificata con il 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.

Il RPD svolge in autonomia un ruolo di confronto dialettico con le strutture e, in particolare, con quella investita dei compiti di Titolare del trattamento dei dati, che in Banca è rappresentata dal Servizio Organizzazione; riferisce sulla sua attività direttamente al Vertice aziendale, predisponendo una relazione annuale per il Direttorio.

L'anno 2020, pur nelle condizioni definite dalle normative preordinate al contenimento del rischio epidemico, ha fatto registrare un consolidamento delle attività del RPD, con un ampliamento dei contatti con le strutture per consultazioni su questioni di *privacy* e per consulenze sulle valutazioni di impatto dei trattamenti di dati collegati a nuovi progetti o procedure e sui casi di potenziale *data breach*.

Si sono moltiplicate le occasioni di confronto e di raccordo con le funzioni di protezione dei dati operanti nell'ambito del SEBC per l'espressione di opinioni o posizioni comuni sulla *compliance* con il GDPR di trattamenti di dati condivisi o collegati effettuati dalle diverse istituzioni, nonché con le *authorities* nazionali per l'approfondimento di temi e questioni di comune interesse.

Crescente è il ruolo di coordinamento assunto dal RPD della BCE e del SSM nei confronti dei RPD delle banche centrali dell'Unione nel dibattito sull'applicazione di norme e linee guida, nella promozione di accordi per disciplinare i casi di contitolarità dei trattamenti di dati e nella sollecitazione di iniziative comuni.

1. Il quadro giuridico.

Nel 2020 il quadro giuridico riguardante la tutela dei dati personali è rimasto sostanzialmente stabile.

Il Codice nazionale in materia di protezione dei dati personali (Codice *privacy*), già integralmente rivisto per l'adeguamento al GDPR, è stato modificato dalla legge 27 dicembre 2019, n. 160 prevedendo che l'attività di prevenzione e contrasto all'evasione fiscale:

- faccia parte degli ambiti di interesse pubblico rilevante nei quali è consentito il trattamento senza consenso delle cosiddette "categorie particolari di dati personali"[2];

---

[1] Regolamento UE 2016/679 (GDPR). Le funzioni del RPD, definite nell'art. 39 del GDPR, 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] Si tratta dei dati 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.

– rientri tra le fattispecie nelle quali è consentita la limitazione dell'esercizio dei diritti degli interessati.

Per quanto attiene alla normativa dell'Istituto, poiché la legislazione comunitaria e nazionale consente per finalità di interesse pubblico il trattamento di dati "particolari" (ex dati 'sensibili') e relativi a condanne penali e reati (ex dati 'giudiziari'), ma richiede l'individuazione delle modalità e delle tipologie di trattamento ammissibili nonché delle garanzie appropriate da parte di fonti normative di livello almeno regolamentare, è in corso una revisione del Regolamento, al fine di aggiornare le più articolate fattispecie di trattamento di dati "sensibili" e "giudiziari" da parte della Banca[3].

Nel corso del 2020 il Servizio Organizzazione ha rivisto la normativa interna (C. 257) attuativa delle previsioni di legge, disciplinando:

– la designazione del Responsabile del trattamento dei dati e la clausola da inserire nei contratti di affidamento di servizi a terzi che debbano assumere tale qualifica;
– il coordinamento tra la definizione delle misure di protezione dei dati personali e l'individuazione dei presidi derivanti dalle normative sulla sicurezza informatica;
– l'applicazione del GDPR nella gestione decentrata degli accessi ai dati contenuti nella Centrale dei Rischi (CR) e nella Centrale di Allarme Interbancaria (CAI).

Sul quadro della protezione dei dati a livello internazionale ha inciso significativamente la sentenza del 16 luglio 2020 (caso C-311/18, c.d. «*Schrems II*») con la quale la Corte di Giustizia dell'Unione Europea ha annullato la *Decisione di adeguatezza* del c.d. *Privacy Shield* tra UE e USA, adottata dalla Commissione Europea nel 2016 per regolare le condizioni di legittimazione del trasferimento di dati verso gli USA, in quanto insufficiente a garantire un livello di protezione sostanzialmente equivalente a quello richiesto oggi dal GDPR per i diritti delle persone i cui dati sono stati trasferiti verso gli Stati Uniti[4].

Per ripianare la lacuna creatasi con la pronuncia della Corte, la Commissione Europea ha avviato nel mese di novembre l'iter di approvazione di nuove Clausole contrattuali tipo (*Standard Contractual Clauses* - SCCs) volte a disciplinare, mediante l'uso di schemi contrattuali uniformi GDPR *compliant,* il trasferimento di dati personali verso Paesi terzi.

La disciplina dei trasferimenti di dati personali extra UE assume particolare rilevanza anche a seguito dell'uscita del Regno Unito dall'Unione Europea.

L'Accordo commerciale e di cooperazione stipulato il 30 dicembre 2020 fra Regno Unito e Unione Europea prevede che il Regno Unito continui ad applicare il GDPR per un periodo transitorio di 6 mesi nel quale qualsiasi comunicazione di dati personali verso il Regno Unito può avvenire secondo le medesime regole valevoli fino al 31 dicembre 2020 senza essere considerata un trasferimento di dati verso un Paese terzo.

2. L'attività svolta nel 2020.

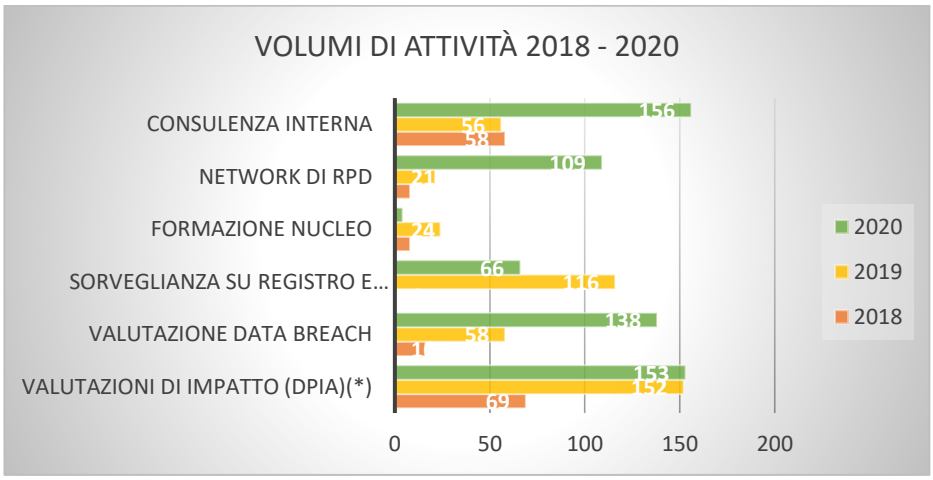
Nel corso del 2020 si è registrato un incremento complessivo del volume di attività del RPD; sono cresciuti, in particolare, gli impegni connessi con la partecipazione ai *network* dei RPD

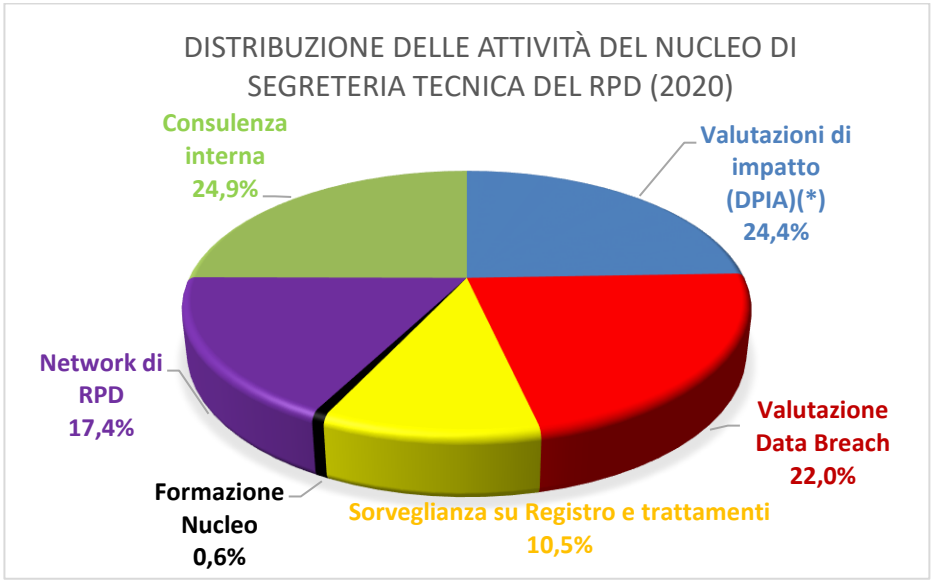
[3] Il Regolamento 6 novembre 2015 (in G.U. 20 novembre 2015, n. 271) recante *individuazione dei dati sensibili e giudiziari e delle operazioni eseguibili*, pur emanato in attuazione di norme del Codice *privacy* ormai abrogate (artt. 20 e 21), è ritenuto tuttora in vigore dal Garante *privacy* nella misura in cui è compatibile con il rinnovato quadro normativo.

[4] Il *Privacy Shield* era 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, i quali si impegnavano, certificandosi, a garantire i principi stabiliti dall'UE in materia di *privacy* e ad assicurare agli interessati tutele paragonabili a quelle europee.

delle banche centrali del SEBC e delle autorità indipendenti nazionali, nonché con le collaborazioni interne e la valutazione delle potenziali violazioni di dati (c.d. *data breach*).

Resta considerevole l'attività complessivamente dedicata allo svolgimento di DPIA(*) e alla valutazione approfondita di singoli trattamenti (c.d. *assessment*), che di norma richiede incontri e colloqui con le strutture interessate.





(*) 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 per mitigarli.

A circa tre anni dall'inizio del suo esercizio, la funzione del RPD ha assunto un carattere "trasversale", essendo chiamata a interloquire ad ampio raggio con diverse funzioni istituzionali e aziendali: la crescita dell'attività, soprattutto in termini qualitativi, e la complessità delle relazioni che si sono consolidate anche sul piano internazionale rendono non più rinviabile l'attribuzione di un'evidenza strutturale all'operatività che supporta i compiti del Responsabile.

2.1 Consulenza.

Lo svolgimento di compiti consultivi in materia di protezione dei dati personali nei confronti delle strutture interne ha costituito fin dall'avvio della sua attività una componente non trascurabile dell'operatività del RPD.

Tale funzione, distinta da quella inerente ai processi tipici disciplinati dagli artt. 33 e 35 del GDPR (valutazione dei *data breach* e valutazioni di impatto) è chiaramente individuata dalle norme e raccomandata dagli orientamenti in materia.

Nell'anno trascorso, la consulenza del RPD è stata richiesta in diversi casi, quali:

- *la revisione della normativa interna sul conflitto di interessi*, per la quale il RPD è stato consultato in merito all'individuazione, alla luce delle norme del GDPR, della base giuridica del trattamento delle informazioni rese dal dipendente sugli interessi economico finanziari potenzialmente confliggenti; è stato inoltre richiesto l'avviso del RPD circa il livello di confidenzialità da attribuire alle predette informazioni nella gestione documentale;
- *il trattamento dei casi di "omocodia" (coincidenza di codici fiscali) nella centrale dei Rischi*. Dal momento che le persone fisiche segnalate nella CR sono censite mediante la chiave identificativa del codice fiscale, è stata portata all'attenzione del RPD la questione della correttezza del trattamento e dei rischi di violazione dei dati personali nel caso di accesso di soggetti segnalati per i quali abbia avuto luogo una differenziazione di codici fiscali coincidenti[5]; si è convenuto di fornire agli interessati elementi informativi riferiti agli intermediari segnalanti che consentono l'identificazione della posizione di rischio e l'ottenimento dei soli dati personali pertinenti;
- *la revisione di un Accordo di collaborazione scientifica tra la Banca e l'Istituto Superiore di Sanità* (ISS), siglato per attività di ricerca su basi informative aggregate da parte della Banca[6], fermo restando il trattamento di dati personali esclusivamente da parte dell'ISS. La consulenza ha avuto l'obiettivo di assicurare il puntuale rispetto della normativa sulla protezione dei dati personali in una modifica dell'Accordo volta ad avvalersi della facoltà di disporre di maggiore granularità delle informazioni in sede di ricerca[7] e, attraverso un confronto diretto con il RPD dell'ISS, è pervenuta alla conclusione di un "Addendum" all'Accordo;
- *la presentazione in forma digitale completa del mod. 730 congiunto;*
- *il trattamento di dati personali nell'ambito del G7-CEG*, il *Cyber Expert Group* dei Paesi del G7[8]. Il RPD è stato consultato in ordine alle condizioni di legittimità del trasferimento dei predetti

[5] L'Agenzia delle Entrate precisa infatti che nei casi in cui l'espressione alfanumerica del codice fiscale generata sia la stessa per soggetti diversi, è necessario procedere a una differenziazione dei codici, seguendo il criterio dettato dall'art. 6 del dm 23 dicembre 1976 (sistematiche sostituzioni di una o più cifre numeriche a partire dall'ultima con corrispondenti caratteri alfabetici) rendendo inutilizzabile il codice fiscale comune generato secondo l'algoritmo standard di calcolo.

[6] Studio della diffusione dell'epidemia da Nuovo Coronavirus sul territorio nazionale finalizzato a valutare i possibili scenari evolutivi sul sistema sanitario, sull'attività economica e sulla stabilità del sistema finanziario, nonché costi e benefici di politiche alternative di contrasto alla diffusione del virus e di uscita dalla fase di emergenza.

[7] Facoltà consentita dall'emanazione di un'ordinanza governativa che ha autorizzato il trasferimento di dati pseudonimizzati in maniera non reversibile dall'ISS agli enti convenzionati per finalità di ricerca scientifica.

[8] Il CEG si occupa della prevenzione e della gestione delle crisi in caso di attacco cibernetico nel settore finanziario

dati personali verso un paese terzo di archiviazione, in relazione alle differenti modalità contemplate dal GDPR[9]. L'avviso espresso, che trova condivisione presso i RPD di altre banche centrali interessate, ha avviato un confronto tra le istituzioni partecipanti;

- *il trattamento di dati personali nel Securities Financing Transactions Data Store.* Nell'ambito della partecipazione della Banca a un progetto della BCE per la raccolta granulare di dati relativi alle operazioni di finanziamento garantite da titoli in un Archivio delle transazioni finanziarie (*Data Store)*, sulla base della specifica normativa europea (*Securities Financing Transactions Regulation, SFTR*), il RPD ha collaborato con il Servizio Rilevazioni ed Elaborazioni Statistiche e con il Servizio Organizzazione alla definizione di un *MoU on joint controllership* dei dati personali ivi trattati dalle banche centrali partecipanti[10] nonché alla revisione del *Privacy Statement* concernente tale trattamento di dati, da pubblicare sul sito dell'Istituto.

Il ruolo consulenziale del RPD, infine, si è estrinsecato nella partecipazione a gruppi di lavoro interni e nel costante confronto con il Servizio Organizzazione su questioni applicative della disciplina sulla *privacy*. In particolare:

- sono proseguiti approfondimenti congiunti sulla prevenzione di potenziali violazioni dei dati personali a fronte di episodi di accesso reiterato da parte di soggetti privati alle informazioni della Centrale dei Rischi per conto di terzi;
- è stata verificata la conformità del trattamento dati effettuato dall'Istituto, nell'adempimento dei doveri di datore di lavoro, per la gestione dei casi di contagio da Covid-19, secondo gli orientamenti del Garante *privacy*.

2.2 Sorveglianza. Registro delle attività di trattamento.

L'attività di sorveglianza del RPD nel 2020 è proseguita secondo le due direttrici di azione delineate nel corso dell'anno precedente.

A. Il monitoraggio periodico sul complesso delle informazioni iscritte nel Registro delle attività di trattamento[11]. Il RPD conduce con cadenza semestrale il monitoraggio del Registro delle attività di trattamento, che costituisce uno dei principali elementi di *accountability* del Titolare dei trattamenti, in quanto fornisce un quadro aggiornato dei trattamenti in essere all'interno dell'organizzazione ed è indispensabile per ogni attività di valutazione o analisi del rischio di violazione dei diritti delle persone.

internazionale: vi partecipano anche esperti della Banca, unitamente a quelli di altre banche centrali dell'Unione presenti nel Gruppo.

9 Le condizioni di legittimazione dei trasferimenti di dati extra UE previste dal GDPR (artt. 45-49) contemplano: l'adozione di Decisioni di adeguatezza del livello di protezione estero da parte della Commissione Europea, la stipula di accordi esecutivi di protezione tra le autorità pubbliche che esportano i dati, il recepimento nei contratti di «*Standard Contractual Clauses*» (SCCs) approvate dalla Commissione UE, l'istituzione di meccanismi di controllo basati su codici di condotta o organismi di certificazione, l'approvazione da un'autorità nazionale di controllo di *Corporate binding rules* nell'ambito di gruppi imprenditoriali trans-nazionali, l'applicazione di speciali *Derogations* per situazioni tassative.

10 Hanno preso parte al progetto, oltre 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.

11 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.

Il monitoraggio ha l'obiettivo di verificare la completezza e la coerenza delle descrizioni dei trattamenti ivi censiti (190 al 31 dicembre). Nell'anno in esame, anche per effetto dell'azione di sensibilizzazione condotta dal Servizio Organizzazione e dal RPD nei confronti delle strutture, il monitoraggio ha messo in evidenza un progressivo miglioramento dei contenuti informativi del Registro per diversi profili[12], accrescendo la capacità descrittiva dei trattamenti effettuati. Resta però l'esigenza di arricchire il Registro con una più puntuale individuazione dei termini di conservazione dei dati trattati[13].

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

B. *L'analisi approfondita (assessment) dei singoli trattamenti.* L'analisi è condotta di norma nell'ambito di incontri con i Servizi, nei quali vengono approfondite le caratteristiche dei singoli trattamenti nel contesto delle attività svolte per verificarne la corrispondenza con le informazioni dichiarate nel Registro[14].

Le attività di *assessment* si sono concentrate sui trattamenti di dati iscritti nel Registro dai Servizi del Dipartimento Immobili e Appalti.

Per la valutazione dei diversi elementi caratteristici (natura dei dati trattati, finalità e modalità di raccolta, designazione dei dipendenti autorizzati, base giuridica, esigenze di conservazione, informative agli interessati, ecc.) ci si è avvalsi di un questionario elaborato secondo le indicazioni del Manuale europeo del RPD[15].

Nell'analisi dei singoli trattamenti, nell'eventualità di accordi stipulati dalla Banca con terzi, è stato verificato in particolare, in base alle attività affidate, se tali soggetti siano stati correttamente qualificati come Responsabili del trattamento per conto della Banca o Titolari autonomi del trattamento ai fini degli obblighi di protezione dei dati; è stata inoltre promossa

12 Nell'indicazione della base giuridica, con un più aderente riferimento alle fonti di legittimazione del GDPR e nell'indicazione delle informative, con la specificazione dei modi in cui l'informativa è resa o delle eventuali cause di esonero dall'obbligo di rendere la stessa (artt. 13 e 14 del GDPR).

13 Alcune Strutture hanno avviato riflessioni per individuare tempi di conservazione coerenti col principio di minimizzazione. Sul tema della conservazione dei dati influisce la questione del coordinamento normativo tra il principio di limitazione della conservazione e quello di integrità del documento digitale che incorpora i dati: soprattutto per le Pubbliche Amministrazioni sussistono infatti incertezze sul rapporto tra vincoli *privacy* e "massimario di scarto" ancora non risolte dalle autorità di settore (Garante *Privacy* e Autorità Archivistica). Infatti l'art. 5, par. 1, lett. e) del GDPR impone che i dati personali siano conservati «*per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*»; per contro l'art. 10 del d.lgs. 42/2004 (Codice dei beni culturali) qualifica tutti i documenti della PA come "*beni culturali*" e quindi: i) *«non possono essere distrutti, deteriorati, danneggiati o adibiti ad usi non compatibili con il loro carattere storico o artistico oppure tali da recare pregiudizio alla loro conservazione»* (art. 20); ii) devono essere conservati (per i tempi previsti dai piani di conservazione) e, trascorsi 40 anni, ove ne ricorrano le condizioni (massimario di scarto), inviati all'archivio storico.

14 Linee Guida dell'Autorità europea di controllo sulla protezione dei dati (*Guidelines* 5 aprile 2017, par. 4.1 e 4.5), con riferimento all'art. 39, paragrafo 1, lettera b) del GDPR.

15 Nella conduzione dell'attività di sorveglianza del RPD si tiene conto degli indirizzi proposti nel Manuale "*Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'UE"* approvato dalla Commissione europea nel luglio 2019 allo scopo di uniformarne l'azione in ambito comunitario.

un'autovalutazione guidata dei profili di rischio inerente, a supporto della valutazione di adeguatezza nel tempo delle misure di protezione esistenti.

Per individuare i trattamenti da sottoporre prioritariamente ad *assessment* si continuerà a seguire il principio di selezione degli interventi in relazione al rischio per gli interessati, che il regolamento europeo pone alla base dell'azione di sorveglianza del RPD.

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

Nel corso del 2020 il RPD ha fornito il suo parere per 13 DPIA riguardanti trattamenti di dati di diversa complessità e ampiezza, in relazione a nuovi progetti e procedure che hanno interessato diverse aree della Banca[16].

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

- l'evoluzione della rete SWIFT, utilizzata dalle applicazioni domestiche nelle infrastrutture di pagamento per il colloquio con controparti nazionali e internazionali;
- la costituzione di piattaforme di sfruttamento dei flussi informativi delle transazioni finanziarie acquisiti in base al Regolamento UE 2012/648 (EMIR) e al Regolamento UE 2015/2365 (STFR);
- la revisione delle procedure di incasso e di pagamento della Tesoreria dello Stato;
- la gestione delle informazioni e dei dati relativi agli organi delle procedure di gestione delle crisi;
- lo sviluppo delle procedure di sportello delle Filiali e dell'Amministrazione Centrale per la gestione del comparto operativo contabile.

Sono stati altresì riesaminati alcuni aspetti di tutela dei dati personali della Piattaforma aperta sul *web* denominata Sportello del cittadino[17] e due progetti dell'U.I.F. per razionalizzare la gestione delle segnalazioni di operazioni sospette.

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

- della gestione del potenziale *whistleblowing* di lavoratori e collaboratori di imprese fornitrici di beni e servizi operanti in Banca;
- dei servizi di notifica agli utenti dei siti *web* dell'Istituto di *newsletter*, pubblicazioni e notizie;
- della registrazione di particolari dati sanitari dei dipendenti imposta alla Banca quale datore di lavoro dalla normativa sulla salute e sulla sicurezza dei lavoratori;
- della gestione dei servizi di posta ibrida;
- dell'istituzione di un Portale *web* per le dichiarazioni fiscali mod. 730.

In ordine alla valutazione delle misure tecniche di protezione dei dati, sono state promosse iniziative di semplificazione per individuare, con la collaborazione del Dipartimento Informatica, le misure di sicurezza da considerare "ricorrenti" in quanto di norma adottate in tutti i servizi offerti direttamente dalla funzione informatica della Banca, allo scopo di agevolare le strutture

[16] 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* ...».

[17] Lo Sportello consente di presentare richieste di accesso ai dati CAI, esposti della clientela, segnalazioni di irregolarità gestionali da parte di intermediari vigilati (incluse le cd. segnalazioni *whistleblowing*) e richieste di informazioni sull'attività di vigilanza, sulla CR e sulla CAI.

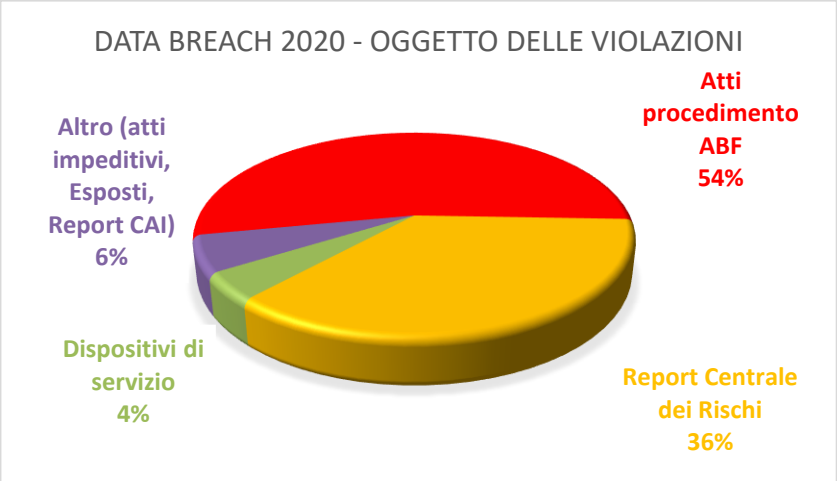
nella presentazione delle valutazioni di impatto. L'innovazione già concordata sarà recepita nella normativa interna nel 2021.

2.4 Le segnalazioni dei data breach.

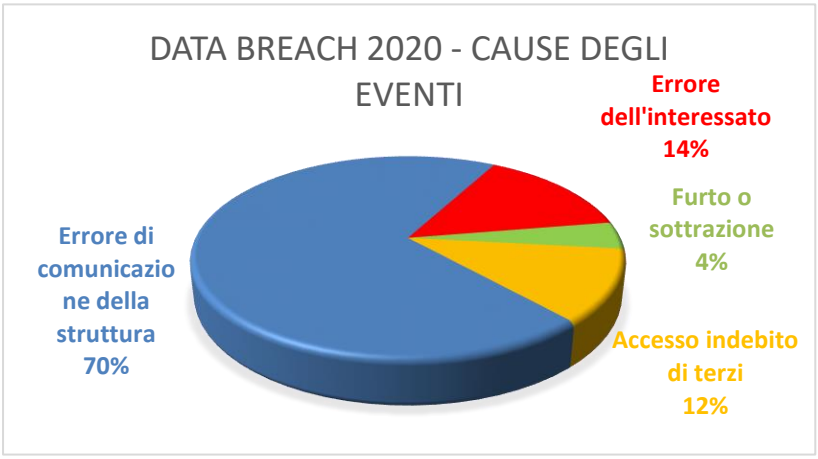
L'analisi degli eventi configurabili come *data breach* in ottemperanza al GDPR è fondamento della *accountability* del Titolare del trattamento, che ha il dovere di mettere in atto nella propria organizzazione tutte le misure atte a prevenire il rischio di trattamento non conforme dei dati personali e di responsabilità civile derivante dalla lesione della riservatezza che rechi un danno agli interessati.

Il GDPR (art. 33), quando si verifica un *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.

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



Analizzando le cause di tali eventi (cfr. grafico al lato) si rileva che essi sono dipesi prevalentemente da erronee trasmissioni di informazioni a terzi nell'ambito di taluni processi operativi della rete territoriale (errore di comunicazione della struttura); in una buona parte dei casi l'incidente è stato determinato dalla disattenzione degli stessi interessati (errore dell'interessato) e da accessi ai dati da parte di terzi privi della necessaria legittimazione (accesso indebito di terzi), legati alla possibilità di acquisizione telematica delle informazioni; residuale è la causa riconducibile ad atto criminoso (furto o sottrazione), limitato ai pochi casi di asportazione di dispositivi di lavoro (personal computer).



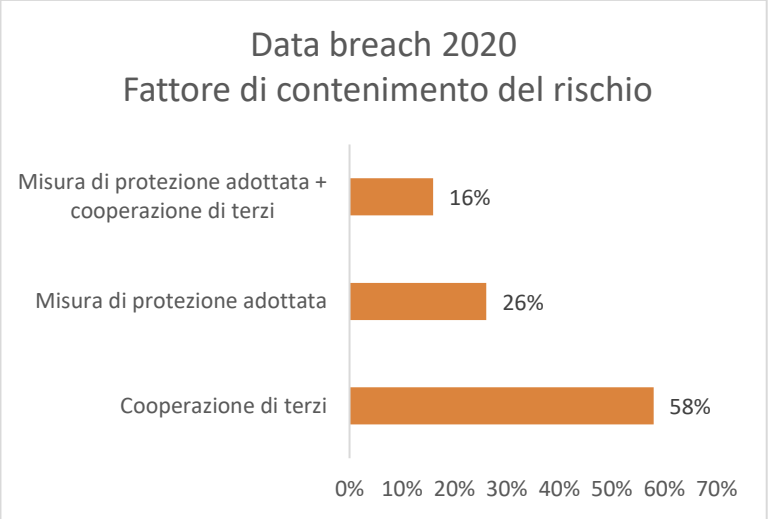
L'informazione più significativa che emerge dalla ricognizione dei *data breach* riguarda i dati contenuti nei report CR, di natura particolarmente sensibile, dei quali una consistente quota è riconducibile all'introduzione della nuova procedura di acquisizione telematica.

Dopo l'avvio dell'applicazione Sportello del cittadino, che ha consentito il rilascio *online* dei report della CR a soggetti muniti di identità digitale[18], si sono verificati reiterati casi di impropri accessi plurimi all'archivio per conto terzi, effettuati da soggetti che hanno dichiarato il possesso di requisiti con autocertificazioni risultate, ai successivi controlli, non veritiere o, in qualche caso, che hanno inoltrato la richiesta senza essere muniti di delega.

Relativamente a tali ultimi eventi di *data breach,* i rischi derivanti da dette violazioni hanno indotto a effettuare una segnalazione al Garante *Privacy* e all'adozione da parte del Servizio Rilevazioni ed Elaborazioni Statistiche, competente per la materia, di misure idonee a filtrare gli accessi per conto di altra persona fisica e a ridurre il rischio di estrazione illegittima di report.

Per quanto riguarda gli altri *data breach*, la valutazione dei fatti non ha comportato l'obbligo di segnalazione al Garante *Privacy*, dato il livello trascurabile di rischio alla luce delle cautele adottate nei casi specifici.

Inoltre, esaminando le iniziative assunte nei diversi casi per impedire il verificarsi di conseguenze dannose dell'evento, tra i fattori che hanno concorso successivamente a contenere il rischio di effetti lesivi dei *data breach,* è risultato largamente prevalente quello della cooperazione dei terzi coinvolti accidentalmente come destinatari della comunicazione impropria dei dati (cfr. grafico a lato).



3. Attività del RPD nell'ambito del SEBC e delle Autorità Indipendenti nazionali.

L'applicazione della regolamentazione comunitaria sulla protezione dei dati personali all'interno del sistema delle banche centrali facenti parte del SEBC e delle autorità di vigilanza nel contesto del SSM ha posto la questione dei ruoli rivestiti da tali autorità e delle relative responsabilità nei trattamenti di dati personali connessi con lo svolgimento di attività condivise nei rispettivi contesti istituzionali[19].

La normativa prevede che, quando le finalità e i mezzi del trattamento di dati personali sono determinati congiuntamente da due o più soggetti titolari, questi sono considerati contitolari del trattamento (*joint controllers*): ciò impone loro – in mancanza di regolazione specifica nel diritto

[18] Tale applicazione, volta ad agevolare l'accesso dell'utenza, prevede il rilascio immediato dei report relativi sia a persone fisiche sia a persone giuridiche (che possono contenere anche informazioni relative a persone fisiche) mediante accreditamento con SPID e autocertificazione di una qualifica abilitante all'acquisizione dei dati.

[19] Sebbene vi sia una sostanziale corrispondenza di previsioni, è necessario avere presente che in tema di protezione europea dei dati personali rispetto alle persone fisiche la BCE è soggetta al Regolamento (UE) 2018/1725 (detto "EUDPR") emanato per disciplinare la materia nei confronti delle istituzioni comunitarie.

dell'Unione - di determinare in modo trasparente, mediante un accordo interno di contitolarità (cd. *Memorandum of Understanding – MoU - on joint controllership for the processing of personal data*), i rispettivi ruoli e responsabilità in merito all'osservanza degli obblighi, con particolare riguardo all'informativa e all'esercizio dei diritti dell'interessato.

La definizione di tali accordi di contitolarità dei dati presuppone un'articolata attività preparatoria, diretta all'analisi dei trattamenti di dati da effettuare in relazione alle attribuzioni dei diversi attori istituzionali, e implica il coinvolgimento dei RPD delle diverse istituzioni partecipanti per un confronto congiunto sui vari aspetti della disciplina.

La centralizzazione di alcune funzioni presso la BCE-SSM e la relativa concentrazione solo presso alcune BCN incaricate della prestazione di servizi comuni per conto dell'intero SEBC implicano la definizione in materia di *privacy* di ruoli diversificati: nell'ambito del dibattito sul punto, nel quale si è fatto riferimento prevalente all'orientamento espresso dal LEGCO, nel caso di svolgimento di un trattamento di dati effettuato "per conto" dell'intero Sistema si è individuata la qualifica di "Contitolare offerente il servizio", in luogo della figura di Responsabile del trattamento per conto dei Contitolari.

Nell'anno in esame il RPD è stato interpellato per l'esame e la redazione di alcune parti dell'articolato del *MoU on joint controllership*:

- sulla disciplina del funzionamento dei servizi informatici condivisi del SEBC;
- sul trattamento dei dati del *Securities Financing Transactions - Data Store* costituito dalla BCE con altre sette banche centrali, tra cui la Banca d'Italia.

Nell'ultima parte dell'anno sono state avviate consultazioni nell'ambito dei lavori preparatori per la redazione di accordi di contitolarità dei trattamenti di dati personali in materia di procedure autorizzative di vigilanza e per il coordinamento di correlati adempimenti previsti dal GDPR: su tale argomento presumibilmente proseguiranno iniziative e consultazioni nel nuovo anno.

La sessione annuale del *network* dei RPD (DPO) in ambito SEBC/SSM si è tenuta il 30 ottobre: nel comune intento di favorire valutazioni condivise e prassi comuni da parte degli RPD nell'ambito delle istituzioni di appartenenza, la sessione ha trattato il tema delle conseguenze della Sentenza della Corte di Giustizia UE "*Schrems II*" sulla regolamentazione del trasferimento extra UE dei dati personali, lo stato dei lavori di definizione dei *Joint-Controllership agreements* nel panorama complessivo dei trattamenti comuni di dati personali e il ruolo del *network* dei DPO nel contesto del SEBC[20].

Inoltre, nel corso dell'anno si sono tenuti incontri in *streaming* del gruppo ristretto dei RPD/DPO della BCE e delle quattro BCN che gestiscono le infrastrutture comuni del sistema dei pagamenti (*Target Services* - TARGET 2, T2S, TIPS e ECMS) per la definizione di una posizione comune sulla *compliance* con il GDPR dei *Target Services*, con particolare riguardo alle misure di protezione dei dati nell'infrastruttura di pagamento TIPS-MPL[21].

[20] Nell'ambito di tale consesso va menzionata anche la partecipazione all'indagine promossa dalla Banca di Spagna per studiare il grado di attuazione del GDPR presso le banche centrali e le autorità di supervisione competenti del SEBC/SSM; il rapporto finale risultato dell'indagine, condotta nel contesto dello *Schuman Programme*, è stato pubblicato nel settembre 2020 sul sito web della Banca di Spagna.

[21] Gli incontri sono stati organizzati dalla Divisione *Market Infrastructure Management* della BCE (*Directorate General Market*

Nell'ambito del programma *Cyber Information and Intelligence Sharing Initiative* (CIISI), finalizzato a condividere informazioni, strategie, tattiche, tecniche e procedure atte a migliorare la protezione delle pubbliche istituzioni finanziarie europee contro le minacce di sicurezza informatica, il RPD è stato consultato dal RPD della BCE, unitamente ai corrispondenti Responsabili di altre banche centrali, per esprimere un'opinione sulla necessità o meno di addivenire a un accordo di contitolarità del trattamento delle informazioni scambiate. Sulla base degli elementi esaminati il RPD, coerentemente con i RPD di altre BCN, ha espresso un argomentato avviso contrario alla necessità di tale regolamentazione, in ragione della mera eventualità del carattere personale dei dati raccolti e della natura fiduciaria delle relazioni all'interno del programma.

Nel 2020 è proseguita la partecipazione alla rete di collegamento tra RPD delle autorità indipendenti nazionali, costituitasi per il confronto di esperienze e di opinioni sulle principali questioni in materia di protezione dei dati personali e sugli indirizzi operativi adottati nell'ambito delle rispettive amministrazioni[22].

Si sono tenuti incontri periodici nei quali, anche grazie ad approfondimenti di relatori interni ed esterni, sono stati trattati temi di interesse comune[23].

Di particolare importanza è stato il Seminario *on line* organizzato il 18 novembre dal RPD della Banca e dal RPD dell'ARERA, coordinatore del *network*, sul tema «*Protezione dei dati e trattamenti delle Autorità indipendenti. Focus su responsabilità e sanzioni*», che ha fatto registrare sulla piattaforma di collegamento della Banca la partecipazione di un considerevole uditorio, composto da esponenti e dipendenti di tutte le Autorità del *network*, con un soddisfacente riscontro di interesse sugli argomenti trattati (assetti organizzativi dei RPD, basi giuridiche, sanzioni, responsabilità).

Il Seminario è stato aperto dal RPD della Banca illustrando brevemente la storia dell'istituzione del Responsabile della protezione dei dati (RPD) in Banca d'Italia nata conseguentemente all'applicazione nel territorio dell'UE del GDPR che ha comportato per tutte le Amministrazioni pubbliche l'obbligo di istituire questa figura e di collocarne la funzione nell'assetto organizzativo esistente.

Il RPD ha sottolineato che vi possono essere esigenze contrastanti nello svolgimento dell'attività istituzionale della Banca d'Italia, quella di garantire la tutela della *privacy* di cittadini e imprese con i quali viene in contatto e quella di esercitare i poteri che le sono riconosciuti dall'ordinamento che prevedono in alcuni casi una forte limitazione del diritto alla riservatezza.

Infrastructure and Payments), che ha illustrato le caratteristiche tecniche e operative delle infrastrutture in modo da facilitare le valutazioni dei DPO.

[22] Il Gruppo è composto dai 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 per la protezione dei dati personali (Garante *privacy*), dell'Istituto di vigilanza sulle assicurazioni (IVASS).

[23] In particolare: modalità di conduzione delle Valutazioni di impatto sulla protezione dei dati (DPIA); ruolo e posizionamento del RPD nelle Autorità pubbliche; responsabilità amministrativa e civile delle PA per inosservanza del GDPR e del Codice privacy; trasferimento di dati extra UE; conformità dei controlli sanitari imposti dall'epidemia di Covid 19; inoltre, attraverso un incontro con la Soprintendenza dei Beni culturali del Lazio, è stato approfondito il tema della conservazione dei documenti digitali presso le Autorità amministrative indipendenti e dei riflessi del GDPR sugli archivi e sulla conservazione dei flussi documentali

Il RPD ha riconosciuto che il principio di trasparenza dell'attività amministrativa nel contesto operativo della Banca ha ormai superato precedenti impostazioni improntate a maggiore riservatezza.

Dato che il tema dell'incontro riguardava le sanzioni, il RPD ha messo in luce alcune criticità, come ad esempio la tenuta applicativa del sistema di tutela della privacy all'organizzazione pubblica, cioè la possibile qualificazione della sanzione all'ente titolare come danno erariale e la duplicazione delle responsabilità personali (del personale di vertice che risponde nei confronti dell'erario per la misura indirizzata alla PA e del responsabile del trattamento privacy destinatario diretto della sanzione) che rischia di condurre ad atteggiamenti di chiusura delle amministrazioni, con effetti su trasparenza e pubblicità dell'attività istituzionale.

4. Linee di sviluppo.

Nell'assicurare lo svolgimento di tutti i compiti tipici (monitoraggio del Registro dei trattamenti e *assessment* dei trattamenti, pareri relativi a DPIA e a *data breach*), l'impegno del RPD dovrà nel prossimo futuro tenere conto del presumibile ampliamento delle esigenze di cooperazione sul piano sovranazionale e della dinamicità dell'assetto dei trattamenti di dati che la Banca è chiamata a svolgere per l'esercizio delle sue funzioni.

Per quanto concerne il primo aspetto, occorrerà presidiare l'equilibrata definizione di ruoli e responsabilità nei trattamenti di dati personali comuni in ambito SEBC, l'efficace disimpegno delle consulenze congiunte e la partecipazione costante al *network* dei RPD/DPO.

Circa il secondo aspetto, si renderà verosimilmente necessario allargare l'azione di sorveglianza sulla conformità dei trattamenti di dati, specialmente di quelli che più possono avere riflessi sull'immagine e sulla responsabilità dell'Istituto, mediante un' opportuna selezione in base alla rischiosità intrinseca, dedicando un *focus* particolare ai trattamenti di dati che vengano affidati a terzi nell'ambito delle esternalizzazioni.

Per consolidare l'*accountability* della Banca quale Titolare dei trattamenti di dati, in ottemperanza a una specifica previsione del GDPR, occorrerà anche verificare nel tempo l'adeguatezza delle misure di protezione dei dati già messe in atto, in relazione all'evoluzione delle regole e delle procedure che ne implicano il trattamento.

Il Servizio Organizzazione ha avviato per questo una campagna di rivalutazione dei trattamenti "pregressi", ossia antecedenti all'applicazione del GDPR, che ha posto in luce l'esigenza di sottoporne un consistente numero a valutazione di impatto: la collaborazione del RPD sarà in quest'ambito orientata a individuare forme di semplificazione del processo di DPIA, per completare in un ragionevole arco di tempo la verifica di adeguatezza di tutti i trattamenti di dati.