

SENATO DELLA REPUBBLICA
XIX LEGISLATURA

Doc. CXXXVI
n. 2

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE
PER LA PROTEZIONE DEI DATI PERSONALI

(Anno 2023)

(Articolo 154, comma 1, lettera e), del codice di cui al decreto legislativo 30 giugno 2003, n. 196)

Presentata dal Presidente del Garante per la protezione dei dati personali

(STANZIONE)

Comunicata alla Presidenza il 25 luglio 2024

PAGINA BIANCA



GDPR

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Regolare il futuro

La protezione dei dati per un'innovazione antropocentrica

Relazione del Presidente Pasquale Stanzione
2023

Roma, 3 luglio 2024



Garante per la protezione dei dati personali

1. Il “cuore antico” del futuro

Signor Presidente della Camera, Autorità, Signore e Signori,

la presentazione, oggi, della Relazione annuale del Garante avviene in una congiuntura alquanto particolare. Il forum intergovernativo del G7 si è da poco interrogato sull’impatto dell’intelligenza artificiale sulla politica, sulle relazioni internazionali, sulla vita individuale e collettiva. Il 17 maggio scorso, il Consiglio d’Europa ha adottato la prima Convenzione internazionale, giuridicamente vincolante, che impegna gli Stati aderenti (non solo europei) al rispetto di alcune essenziali garanzie per i diritti umani, la democrazia e lo Stato di diritto nell’utilizzo dei sistemi di intelligenza artificiale.

Poco prima, l’Unione europea aveva approvato, in conclusione di legislatura, la prima disciplina al mondo, di taglio organico e non settoriale, dell’intelligenza artificiale, segnando una primazia che non è, affatto, soltanto cronologica ma è, soprattutto, assiologica. L’*Ai Act* – tanto più se iscritto all’interno del complessivo quadro regolatorio del digitale, definitosi nei suoi ultimi tasselli con il *Data Act* – rappresenta, infatti, assieme a ciò che fu il GDPR otto anni fa, il tentativo più avanzato dell’Europa di delineare una strategia antropocentrica di governo della tecnica.

Nel promuovere un’innovazione sostenibile sotto il profilo delle garanzie giuridiche, dell’equità sociale, della dignità personale, l’Europa ha, infatti, investito sul terreno del digitale la propria identità come Comunità di diritto, marcando la propria specificità tanto rispetto alla *deregulation* o



alla settorialità dell'approccio americano (di cui l'*Executive Order* di ottobre 2023 è espressione), quanto rispetto all'autoritarismo sino-coreano.

E pur con l'inevitabile asincronia del diritto rispetto alla tecnica, con la sua velocità incessante, i tempi della regolazione sono significativi. L'attenzione – soprattutto, ma non soltanto europea - nei confronti delle neotecnologie esprime, infatti, la consapevolezza dell'ormai piena integrazione dell'intelligenza artificiale nella nostra vita privata e pubblica. Il 2023 è stato l'anno della diffusione massiva dell'intelligenza artificiale, così estesa e veloce da aver addirittura indotto, nel marzo di quell'anno, mille esponenti delle *big tech* a suggerire, con una lettera aperta, una moratoria sullo sviluppo di questa neotecnologia, ritenuto eccessivamente rapido.

Pur limitandoci a pochi dei molti esempi che si potrebbero fare, si consideri che circa il 65% dei ragazzi utilizza oggi l'intelligenza artificiale per svolgere i compiti; due studenti su tre avrebbero preparato l'esame di maturità ricorrendo a *Chat Gpt* che peraltro, a quanto pare, non sarebbe riuscita a tradurre correttamente il Minosse, o Della legge, attribuito a Platone.

L'intelligenza artificiale è riuscita persino ad arricchire, con effetti visivi e sonori straordinari, la Turandot rappresentata alla Scala. Un'impresa su quattro, nel nostro Paese, ha già integrato l'intelligenza artificiale nei propri processi produttivi ed entro un anno – si stima – il 60% delle aziende la utilizzerà nei procedimenti assunzionali.

Si ritiene, inoltre, che l'intelligenza artificiale potrebbe sostituire, nei prossimi anni, circa 85 milioni di posti di lavoro creandone, tuttavia, 97 (milioni) di nuovi, sebbene con un rischio di nuove, ulteriori diseguaglianze, evidenziato con preoccupazione dal Fondo monetario internazionale. E non



Garante per la protezione dei dati personali

si tratta, del resto, di un rischio così peregrino, se si considerano le profonde diseguaglianze che, anche sul terreno del lavoro, il capitalismo digitale ha prodotto, rispetto ai lavoratori “invisibili” della *gig economy*.

In ambito sanitario sono moltissime e sempre più significative le applicazioni di intelligenza artificiale a fini diagnostici, sperimentali, terapeutici. Secondo una recente ricerca, le molecole farmacologiche scoperte mediante l’intelligenza artificiale mostrerebbero un tasso di successo, nella prima fase clinica, pari a circa l’80-90%: una promessa importante per la cura di molte malattie. E a dimostrazione delle straordinarie potenzialità delle neotecnologie, basti pensare che si ricorre già al Metaverso per effettuare visite mediche a detenuti, così da coniugare il diritto alla salute – che neppure in carcere può ammettere limitazione – ed esigenze di sicurezza (è il progetto della colonia penale di Mamone).

Questi esempi – e molti altri che si potrebbero addurre – dimostrano come effettivamente l’intelligenza artificiale sia ormai entrata a far parte del nostro orizzonte quotidiano di vita e sempre più ne sarà elemento costitutivo, con effetti della cui portata (in senso lato antropologica) non siamo, forse, del tutto consapevoli.

Il diritto ha il compito di colmare questo vuoto di consapevolezza, fornendoci gli strumenti per capire come porre realmente al servizio dell’uomo ciò che può rappresentare tanto uno straordinario fattore di sviluppo, benessere, promozione del pubblico interesse quanto anche, se non ben governato, una fonte di rischi tutt’altro che trascurabili, per la persona, la società, la democrazia. La sfida principale che si delinea all’orizzonte è tutta nel rendere l’evoluzione tecnologica davvero mimetica e non soltanto protesica (capace cioè di simulare l’uomo e la sua razionalità, prima e oltre che colmarne le carenze) un fattore di progresso



non solo tecnico ma sociale, temperando – per riprendere le parole del Pontefice – con l’algoretica gli eccessi dell’algocrazia.

Agli algoritmi e alla loro pretesa neutralità si affidano, infatti, decisioni sempre più significative, assecondando per ciò la svolta ingiuntiva della tecnica, sempre più demiurgica, predittiva e quindi performativa. Tra gli opposti estremi, entrambi scorretti, del soluzionismo tecnologico scienziata e del neoluddismo, si delinea dunque l’obiettivo del prossimo futuro: un governo democraticamente sostenibile della tecnica, che tracci il confine oltre il quale, per riprendere Nietzsche, non si può fare tutto ciò che *si può* fare, ponendo limiti a una volontà di potenza che, altrimenti, non ne conoscerebbe e che, anzi, tenderebbe a spostare sempre più in là la frontiera delle possibilità. Va, dunque, delineato quel “cuore antico” del futuro (parafrasando Carlo Levi) che àncori l’innovazione a un limite giuridico, politico, sociale, prima ancora etico di sostenibilità.

2. Il momento Oppenheimer

La persistenza della guerra, ai confini d’Europa e, da ottobre scorso, anche nel cuore del Mediterraneo, offre all’intelligenza artificiale un drammatico terreno di sperimentazione in contesti bellici, dove la potenza geometrica dell’algoritmo rischia di amplificare senza limiti la capacità offensiva dei conflitti, sottraendo all’uomo il controllo della violenza.

Si tratta non tanto e non soltanto dei droni - cui si è fatto ampio ricorso nel contesto russo-ucraino - quanto di sistemi, come Lavender, utilizzati nel conflitto israelo-palestinese per identificare i *target*, tuttavia con un ampio margine di tolleranza delle “*casualties*” (vittime collaterali): emblematico ossimoro del dramma della guerra. Secondo alcune fonti



citare da *The Guardian*, infatti, l'alto numero di civili rimasti vittime dei bombardamenti sulla striscia di Gaza sarebbe imputabile all'uso indiscriminato dell'intelligenza artificiale. Quella stessa intelligenza artificiale che, paradossalmente, Mosab Alì utilizza come terapia per i traumi subiti dai bambini della Striscia.

E se Lavender contempla ancora una decisione finale umana, seppur meramente estrinseca, sull'indicazione proposta dall'algoritmo, si stanno sperimentando strumenti offensivi capaci anche di prescindere, come si è chiarito alla Conferenza internazionale di Vienna di aprile. Si ritiene, non a torto, che le armi autonome possano rappresentare la nuova bomba atomica, per gli effetti dirompenti e l'assenza di regole che ne potranno caratterizzare l'utilizzo, tanto da qualificare quello attuale come un nuovo "momento Oppenheimer".

E, anche oltre il contesto bellico in senso stretto, l'intelligenza artificiale alimenta quella "cognitive warfare" – realizzata con la manipolazione e monopolizzazione dell'informazione, su cui lo stesso Presidente della Repubblica ha stimolato una riflessione – capace di rappresentare, secondo alcuni, la nuova guerra fredda, spintasi in quello che la Nato ha definito il sesto dominio della conflittualità.

La stessa vice-Presidente della Commissione UE ha espresso preoccupazione rispetto all'utilizzo massivo e con metodi algoritmici, a fini di competizione geopolitica, dei dati personali da parte di alcuni Stati: il bando statunitense dei prodotti Kaspersky è, del resto, in tal senso significativo. Essa ha infatti sottolineato come i "tempi nervosi" in cui viviamo inducano a una crescente domanda di sicurezza da parte dei cittadini, che va dunque – aggiungiamo – filtrata e analizzata, dalla politica,



Garante per la protezione dei dati personali

con la necessaria lungimiranza, tanto più alla luce delle potenzialità dell'intelligenza artificiale, per essere più efficaci, non meno liberi.

La continua espansione ed evoluzione dell'intelligenza artificiale impone dunque di tracciare (e questo è il massimo compito della politica) un limite di sostenibilità, delle colonne d'Ercole da non varcare perché il progresso non divenga, paradossalmente, socialmente regressivo.

Si pensi, a titolo meramente esemplificativo, ai progetti di utilizzo dell'intelligenza artificiale in campo neuroscientifico, con la realizzazione di *decoder* "semantici" dell'attività neurale, combinando scansione cerebrale e database di modelli linguistici, come quelli usati da *Chat Gpt*. A gennaio, negli Stati Uniti, è stato applicato per la prima volta, a un paziente tetraplegico, un dispositivo in grado di decodificare i segnali neurali per far eseguire a un robot ciò che i suoi arti non possono fare.

Si tratta di un'innovazione potenzialmente rivoluzionaria, capace di apportare benefici senza precedenti per la cura di stati neurodegenerativi e, per ciò, meritevole di sviluppo, purché tuttavia non si giunga alla trasparenza del pensiero: il più illiberale e pericoloso degli esiti possibili. La possibilità di traduzione dell'attività neurale in impulsi algoritmici è, infatti, una conquista preziosa a condizione che non venga utilizzata per leggere il pensiero, rendendo dunque accessibile anche quel foro interno la cui riservatezza è presupposto necessario per la libertà di coscienza.

Quello del limite e dello scopo (o, meglio, di uno scopo diverso dalla mera volontà di potenza) è, dunque, il principale obiettivo da perseguire nel governo della tecnica, perché l'uomo non divenga, paradossalmente, egli stesso strumento della macchina anziché suo *dominus*, al "servizio della manovella", come nell'icastica immagine pirandelliana di Serafino Gubbio operatore.



3. Territorio di frontiera

Se il Garante è potuto intervenire su molti sistemi di intelligenza artificiale (nell'ultimo anno *ChatGPT*, *Sora*, *Replika*) è perché la disciplina di protezione dei dati regola (e continuerà a farlo anche dopo l'*AI Act*) il fulcro dell'intelligenza artificiale: il trattamento di dati personali funzionale a processi decisionali automatizzati e all'addestramento dell'algoritmo.

Rispetto a questo nucleo fondativo dell'intelligenza artificiale, la disciplina di protezione dei dati ha introdotto infatti, non da ora, alcune garanzie essenziali: dal principio di conoscibilità al divieto di discriminazione algoritmica; da un generale principio di trasparenza, che impone precisi obblighi informativi nei confronti dell'utente a un criterio di qualità ed esattezza dei dati da utilizzare, particolarmente rilevante per evitare i *bias* propri di un addestramento dell'algoritmo sulla base di informazioni inesatte o non sufficientemente rappresentative.

Le garanzie particolari accordate nel trattamento dei dati dei minori si sono, inoltre, rivelate determinanti nell'assicurare il controllo sull'accesso degli infraquattordicenni ad alcuni dei contenuti offerti da sistemi di intelligenza artificiale generativa e *chatbot* tra cui *Replika* e *ChatGpT*, spesso inadeguati (ad esempio perché sessualmente espliciti) per il corretto sviluppo cognitivo, etico, personologico dei minori. L'attenzione posta dal Garante sulle carenze di *chatbot* come *ChatGpT* ha stimolato, peraltro, anche il Comitato europeo per la protezione dei dati a trattare il tema ad ampio raggio e su scala appunto europea, con una *task force* costituita *ad hoc*.

Particolare rilievo assume anche il provvedimento sul *webscraping*, recante alcune garanzie essenziali (e, per converso, adempimenti a carico



dei titolari) per impedire che le nostre vite si traducano – come si è detto - in alimento per gli algoritmi. I limiti del *webscraping* sono stati sottolineati anche rispetto alla riforma fiscale, nel cui ambito il ricorso all'intelligenza artificiale esige requisiti stringenti di affidabilità ed esattezza dei dati utilizzati per la profilazione del contribuente. Se addestrato su dati anche soltanto parzialmente inesatti, infatti, l'algoritmo restituirà risultati errati in proporzione geometrica, con *bias* che dalla base informativa si propagano lungo tutto l'arco della decisione algoritmica. Per questo, ad esempio, nel parere sul decreto legislativo, sul concordato preventivo, è stato richiesto di espungere un riferimento che avrebbe potuto legittimare analisi del rischio fiscale fondate anche sul *webscraping*.

Basare le procedure accertative su informazioni "rastellate" dal web – come tali in larga misura inesatte – è, infatti, estremamente rischioso, potendo avere effetti fortemente distorsivi sulla corretta rappresentazione della capacità fiscale dei contribuenti. Le garanzie di protezione dei dati rappresentano quindi, anche in quest'ambito, presupposti di efficacia dell'azione di contrasto dell'evasione fiscale.

Riguardo al settore sanitario, caratterizzato dal ricorso qualitativamente e quantitativamente crescente all'intelligenza artificiale, con lo specifico "decalogo" adottato lo scorso ottobre si è inteso rimarcare i principi che presiedono al corretto utilizzo dei dati personali mediante sistemi d'intelligenza artificiale, riconducibili in estrema sintesi ai principi di trasparenza e supervisione dei processi decisionali automatizzati, nonché di non discriminazione algoritmica.

La disciplina del GDPR sulla decisione algoritmica è funzionale anche ad evitare che il legittimo controllo del territorio, a fini di sicurezza, degeneri, sia pur preterintenzionalmente, in sorveglianza massiva. Per



Garante per la protezione dei dati personali

questo, ad esempio, si è inteso verificare la legittimità del sistema di videosorveglianza “intelligente” adottato dal Comune di Trento, la cui incidenza sui diritti e le libertà dei cittadini avrebbe comportato l’adozione di garanzie significative.

Queste iniziative (e molte altre che si potrebbero richiamare) dimostrano la ragione per cui l’*AI Act*, nel delineare il sistema di *governance* dell’intelligenza artificiale, sancisca una specifica riserva di competenza in favore delle Autorità di protezione dei dati, in particolare in settori (immigrazione, attività di contrasto, giustizia, processi democratici) nei quali la potenza algoritmica rischia di amplificare la strutturale asimmetria del rapporto in cui si iscrive o le vulnerabilità proprie, per condizione soggettiva o circostanza, degli interessati. Ed è anche questa la ragione per cui, come rappresentato più volte al Parlamento e al Governo, l’individuazione nel Garante dell’Autorità competente per l’*AI Act* sarebbe la più coerente con l’incidenza, profonda e trasversale, dell’intelligenza artificiale, sui diritti fondamentali (cui, significativamente, si rivolge la stessa valutazione d’impatto prescritta per i sistemi ad alto rischio). Essa suggerisce, infatti di attribuirne la competenza ad Autorità caratterizzate da requisiti d’indipendenza, in ragione dei “limiti e delle aporie” che la regola maggioritaria presenta, come insegnava Norberto Bobbio, di fronte a quel “territorio di frontiera” rappresentato dai diritti di libertà; la sfera dell’indecidibile, appunto.

4. La giustizia e il digitale

L’anno trascorso è stato determinante per la piena realizzazione del processo di digitalizzazione della giustizia, cui il Garante ha fornito un



contributo significativo soprattutto in sede consultiva, rispetto sia al processo (ordinario) telematico, sia alla costituzione delle infrastrutture digitali per le intercettazioni. I flussi informativi funzionali alla giurisdizione presentano, infatti, caratteristiche tali da esigere cautele peculiari e garanzie rafforzate nella loro utilizzazione, per la tutela dei soggetti interessati e degli stessi interessi pubblicistici sottesi (si pensi, per tutti, al segreto investigativo o all'autonomia e indipendenza della magistratura).

Ma con questi presidi offerti, anche, dalla disciplina di protezione dei dati, la capacità trasformativa del digitale può rappresentare uno straordinario fattore di progresso e miglioramento dell'attività giurisdizionale, a beneficio di tutti gli attori coinvolti. E' dunque opportuna la valorizzazione, operata tanto dalla riforma Cartabia in entrambi i settori della giustizia ordinaria, quanto dal PNRR, delle risorse digitali in ambito giurisdizionale.

Gli aspetti più delicati, dal punto di vista della protezione dei dati, comuni a questi progetti, pur nella loro diversità, possono ricondursi a due macroaree: la sicurezza e la riservatezza in senso stretto. Con riferimento al primo aspetto, va ricordato - come peraltro rilevato in sede di audizione sul disegno di legge sulla cybersicurezza - che ogni ipotesi di digitalizzazione determina rischi in termini di sicurezza cibernetica. L'esposizione al mezzo telematico comporta, infatti, delle vulnerabilità da cui i dati e i sistemi che li ospitano vanno protetti, per la salvaguardia non soltanto della privacy dei soggetti coinvolti, ma anche della stessa efficienza dell'amministrazione della giustizia, come recenti casi di cronaca dimostrano.

Questo aspetto è centrale nei pareri resi, anche quest'anno, dal Garante sui vari provvedimenti che hanno disciplinato la telematizzazione



Garante per la protezione dei dati personali

di alcuni flussi informativi o la costituzione di nuovi sistemi digitali, con l'esigenza di garantire misure tecniche e organizzative realmente adeguate al grado di rischio connesso al trattamento.

Peraltro, la digitalizzazione non tocca il solo profilo organizzativo e strumentale della giurisdizione, ma anche quello più strettamente processuale, investigativo e probatorio. Soprattutto su questo terreno, il ricorso alla tecnologia e alle sue potenzialità crescenti lascia intravedere l'esigenza di una più puntuale regolazione, come plasticamente emerso in relazione alla *data retention* e ai criptofonini: temi sui quali la giurisprudenza, europea e interna, ha dovuto svolgere un'azione per certi versi di supplenza, per altri di monito al legislatore.

Si dovrebbero, peraltro, rafforzare ulteriormente (secondo direttive già suggerite dal Garante in audizione) le garanzie per le intercettazioni mediante captatore, la cui applicazione sta mostrando tutti i limiti della delega, alla tecnica, di uno strumento potenzialmente "onnivoro" quale il trojan, tanto più se utilizzato "a strascico".

Un altro profilo ricorrente nei processi di digitalizzazione concerne il bilanciamento tra pubblicità degli atti processuali (amplificata esponenzialmente dal mezzo telematico) e garanzia della riservatezza delle parti e dei terzi coinvolti. Un profilo peculiare è emerso a seguito dell'estensione, con la riforma Cartabia del ricorso, nel processo penale, alla riproduzione audiovisiva e fonografica come modalità generale di documentazione, che è destinata ad affiancare il verbale per gli atti del procedimento, quale modalità preferenziale di documentazione dell'interrogatorio di garanzia dell'indagato *in vinculis* o forma di documentazione dell'assunzione dibattimentale dei mezzi di prova.



Garante per la protezione dei dati personali

Tale innovazione - in ragione del suo impatto sul trattamento dei dati personali delle parti e dei terzi coinvolti, a vario titolo, nel procedimento, benché volta a garantire una rappresentazione più accurata dell'atto - ha indotto il Garante a suggerire l'introduzione di un regime speciale di pubblicità degli atti così documentati. Esso dovrebbe, in particolare, bilanciare le esigenze di pubblicità, espressione del principio di cui all'art. 101, I c., Cost., il diritto alla riservatezza e il principio di minimizzazione dei dati trattati.

E' chiaro, infatti, che l'applicabilità a tali atti, documentati digitalmente nella loro integralità, del regime ordinario di pubblicità, potrebbe determinare l'indiscriminata diffusione di dati eccedenti, talora anche appartenenti alle categorie particolari cui l'ordinamento accorda una tutela rafforzata, sino al divieto di diffusione per i dati sanitari, genetici, biometrici. Si tratta, peraltro, di un bilanciamento coerente con quello sotteso anche a innovazioni normative recenti, quali l'oblio per i soggetti destinatari di provvedimenti giudiziari favorevoli (rispetto al quale il Garante ha chiarito doversi operare un bilanciamento tra gli interessi in gioco, senza presunzioni assolute di prevalenza) e le nuove disposizioni sulla trascrizione delle intercettazioni introdotte dal d.l. 105 del 2023. Esse si inseriscono, peraltro, all'interno del più ampio disegno di revisione della disciplina delle intercettazioni - in parte ancora in itinere - volto a rafforzare (ulteriormente rispetto a quanto disposto dalle riforme del 2017 e del 2019 e in linea con le indicazioni del Garante) le garanzie in favore dei terzi, indirettamente intercettati.

Come si è avuto modo di sottolineare in audizione, il ddl governativo, in particolare, rafforza sensibilmente, le garanzie di riservatezza dei terzi e, per altro verso, circoscrive l'ambito circolatorio (endo- ed extra-



Garante per la protezione dei dati personali

processuale) dei contenuti captati, a tutela della privacy di tutti i soggetti (parti e terzi) le cui conversazioni siano acquisite. Se si limita la pubblicabilità delle intercettazioni ai soli contenuti riprodotti dal giudice in propri provvedimenti, si circoscrive notevolmente il novero dei dati suscettibili di circolazione al di fuori del giudizio, ammettendola soltanto per le informazioni rilevanti a fini processuali.

Queste modifiche sottendono, ovviamente, un bilanciamento tra privacy e diritto di (e all') informazione, la cui definizione è riservata alla discrezionalità del legislatore. Ciò che si può auspicare - anche rispetto alla delega legislativa sul divieto di pubblicazione integrale o per estratto dell'ordinanza di custodia in fase di indagini - è che si contenga la tendenza a scambiare l'interesse sociale della notizia con il gossip.

La sfida della democrazia è, infatti, proprio nel coniugare la "pietra angolare" del diritto di (e all') informazione con la dignità personale (di cui la protezione dei dati è peculiare espressione): tanto più in un ordinamento, come il nostro, dalla vocazione intrinsecamente personalista.

5. **Biologia e biografia**

La sfida della digitalizzazione riguarda anche - e non senza analogia complessità - il settore sanitario, rispetto al quale la protezione dei dati ha dimostrato di poter rappresentare un fattore di efficienza della *governance* sanitaria ma, anche, di fiducia dei cittadini nella sanità. Sulla sinergia tra innovazione, sanità e protezione dei dati si giocherà, infatti, una sfida sempre più determinante per le nostre società, che dobbiamo impegnarci a vincere nel segno, ancora una volta, della centralità della persona e della



Garante per la protezione dei dati personali

sua dignità: quei vincoli che, spiegò Aldo Moro in Assemblea costituente, neppure l'interesse collettivo alla sanità pubblica può superare.

I dati sulla salute sono, infatti, prezioso strumento di garanzia del diritto alla salute e alle cure (che, con lungimirante affermazione, la nostra Costituzione assicura anche "agli indigenti"), anche nella componente solidaristica della destinazione a fini di ricerca ma, al tempo stesso, prezioso frammento della vita più intima di ciascuno, da proteggere da indebite ingerenze o strumentalizzazioni. Non a caso, tra le prime norme dell'ordinamento sulla riservatezza si annoverano proprio quelle inerenti i dati sanitari, da proteggere per evitare fughe dalla diagnosi e dalla terapia, così da costruire, sulla base dell'affidamento riposto nel segreto professionale, il rapporto strettamente fiduciario tra medico e paziente che costituisce l'architrave della disciplina odierna e della giurisprudenza sull'autodeterminazione terapeutica.

Queste garanzie vanno assicurate anche – a maggior ragione – in un contesto di sempre più marcata digitalizzazione della sanità e di promozione della ricerca scientifica che va, tuttavia, inscritta all'interno di un progetto organico e lungimirante di *governance* sanitaria. Esso deve, in particolare, minimizzare i rischi cibernetici e promuovere una condivisione selettiva dei dati, ammettendone anche (come prevede il Regolamento sullo spazio europeo dei dati sanitari) la destinazione solidaristica, anche a fini di ricerca, ma con le dovute cautele per evitare ogni indebita reidentificazione degli interessati e discriminazione per gruppi (rischio tanto più elevato ove i *dataset* sui quali si fonda la decisione algoritmica non siano rappresentativi o sottendano comunque pregiudizi di genere, etnia, condizioni sociali o appunto di salute e così via).



Garante per la protezione dei dati personali

Da questo punto di vista, la recente riforma della disciplina dell'uso dei dati personali a fini di ricerca scientifica, nell'escludere la previa consultazione del Garante anche in assenza del consenso dell'interessato, responsabilizza notevolmente i ricercatori, che saranno tenuti a verificare autonomamente le condizioni di legittimità del trattamento, anche alla luce delle specifiche regole deontologiche, oltre che del parere del comitato etico.

Con riguardo alla digitalizzazione della sanità, sono particolarmente rilevanti le criticità segnalate al Governo rispetto alle difformità riscontrate, tra le varie Regioni, nella realizzazione del FSE 2.0, concepito invece proprio per assicurare omogeneità nelle garanzie di fruizione tra le varie aree del Paese. Diritti fondamentali come quello alla salute – e, per altro verso, la protezione dei dati – non possono, infatti, tollerare garanzie a geometria variabile, con le diseguaglianze *ratione loci* suscettibili di derivarne.

E'quanto, del resto, ha recentemente ribadito la Corte costituzionale nel dichiarare illegittima, per violazione del riparto di attribuzione della potestà legislativa tra Stato e Regioni, una legge regionale volta a legittimare la videosorveglianza nelle strutture di cura, in assenza di norme legislative statali in materia.

Quest'esigenza di uniformità è tanto maggiore in ragione della progressiva integrazione dei sistemi (soprattutto) informativi in ambito sanitario prevista dal Regolamento sullo spazio europeo dei dati sanitari. Esso, infatti, pur promuovendo la destinazione a fini solidaristici dei dati sanitari (in linea con l'idea dei dati come beni comuni sottesa già al *data altruism* del *Data Governance Act*), introduce tuttavia significative garanzie anche per la c.d. *group privacy*, con specifici divieti di utilizzo



discriminatorio dei dati sanitari nei confronti di singoli o gruppi di persone, anche per quanto riguarda offerte di lavoro o condizioni contrattuali.

Analoga esigenza non discriminatoria è sottesa alla disciplina dell'oblio oncologico, condivisa – anche in fase attuativa – con il Garante, volta a impedire che la persona sia risolta nella sua malattia e che la biografia sia schiacciata, ineludibilmente, sulla biologia.

Non del tutto dissimile, almeno nel suo significato più profondo, l'esigenza di riservatezza che ha indotto il Garante ad intervenire, anche sul piano sanzionatorio, rispetto alla vicenda del "cimitero dei feti", ovvero dell'indicazione dei nomi delle donne che avevano praticato un'interruzione volontaria di gravidanza su targhette apposte sulle sepolture dei feti presso un cimitero romano.

In gioco qui vi erano non tanto e non "soltanto" dati sulla salute come, pure, sono quelli sull'aborto quanto, piuttosto, informazioni relevantissime (e per ciò soggette alla massima riservatezza) su scelte di ordine esistenziale, etico, per certi aspetti persino religioso, tra le più delicate. Come spesso accade, anche in questo caso una questione che coinvolge il corpo giunge, ben al di là - dalla biologia alla biografia, appunto - al cuore di quelle "scelte tragiche" che meritano il massimo riserbo.

6. Asia e le altre

La vicenda di Asia, la ragazza insultata in rete perché (!) malata, così come quella, di pochi mesi precedente, della ristoratrice toltasi la vita per non aver retto alla "condanna" dello spietato tribunale di internet, simboleggiano, drammaticamente, le aberrazioni cui può giungere l'odio digitale.



Garante per la protezione dei dati personali

Preoccupa l'uso offensivo del web, la diffusione anche tra i giovani di messaggi istigativi, discriminatori nei confronti, generalmente, di minoranze, delle donne o di chiunque sia percepito come "altro-da-noi", con rivendicazioni identitarie in forma aggressiva. Le stesse caratteristiche socio-tecniche (c.d. *affordances*) delle piattaforme sono, spesso, non neutrali rispetto al genere e tali, dunque, da agevolare o, quantomeno, normalizzare atteggiamenti sessisti.

E se la rete esprime la morfologia sociale dell'oggi, questa sua degenerazione non può non interrogarci con la drammaticità dei problemi epocali, a partire dagli episodi, susseguitisi la scorsa estate e sui quali il Garante è più volte intervenuto, di diffusione sui social di immagini di stupri commessi da ragazzi, in gruppo, su ragazze, sole. Le interrelazioni tra il web e la violenza sono, infatti, più profonde e ambivalenti di quanto una drammatica contabilità delle loro aberrazioni possa restituire.

La rete mostra infatti – accanto a innegabili, straordinarie, potenzialità di progresso anche sociale – sempre più un lato oscuro, un suo prestarsi a logiche di sopraffazione che finiscono con il tradirne l'originaria promessa inclusiva. Internet rappresenta così non soltanto il "teatro" della violenza (e di violazioni varie come l'impersonificazione e le frodi, oggi in netto aumento) ma anche, spesso, un suo fattore propulsivo, capace di mutarne, profondamente, forme di manifestazione e implicazioni, per persistenza, pervasività, emulazione, difficile contenibilità del danno.

Si pensi al *revenge porn*, rispetto a cui l'indiscriminata pubblicità, lo *shaming effect* indotti dalla diffusione in rete di immagini intime rendono possibile una forma nuova e del tutto singolare di violenza, appunto digitale. Il tradimento della fiducia sottesa a quell'intimità e dell'aspettativa di riservatezza che le è propria, si realizza infatti proprio per effetto



Garante per la protezione dei dati personali

dell'ampia diffusività assicurata dal web ai contenuti che vi sono immessi. L'esercizio, da parte del Garante, della specifica competenza attribuitagli in materia di *revenge porn* (consistente nella decisione sulle istanze di blocco del caricamento non consensuale di contenuti intimi: in quest'anno, 299), ha consentito all'Autorità di verificare la vastità e pervasività del fenomeno, che in tal modo si può almeno in parte arginare.

Ma la violenza digitale assume anche le tragiche vesti della riedizione, *on line*, della violenza inferta *off-line*, nella sua immane concretezza. L'amara cronaca dell'estate scorsa ci ha mostrato come la barbarie degli stupri, commessi da ragazzi - in gruppo - su ragazze, sole, possa superare ogni limite di atrocità venendo filmata, condivisa e irrisa, come fosse il frammento di un'ordinaria quotidianità. La violenza fisica viene così, con se possibile persino maggiore sprezzo, perpetuata nella violenza rappresentata e poi divulgata, con gli effetti drammatici della vittimizzazione secondaria, che il Garante con i suoi interventi ha cercato di contenere.

E vittime e autori di questo dramma sono, troppo spesso, coloro i quali - i ragazzi, appunto - intessono con le nuove tecnologie un rapporto quasi osmotico, ancorché spesso inconsapevole. La micro-celebrità che assicura il web, con il mito di *influencer* seguiti da milioni di *follower*, sembra così poter assicurare l'identità che si fatica altrimenti a costruire, giungendosi al paradosso di voler riprodurre *on line* la propria vita, anche al prezzo di quella degli altri.

Se quest'alienazione dal reale è il frutto della virtualizzazione della vita, dell'intersezione costante, fin quasi alla sovrapposizione, delle dimensioni reale e virtuale, si rischia di confondere la vita con la sua rappresentazione, la persona con l'*avatar*, il corpo con la sua immagine,



riducendo anche la percezione del “male”, di cui la rete offre spesso una narrazione pornografica. La stessa diffusione dei *deep fake*, espressiva della capacità della tecnica di rendere imitabile, riproducibile, “falsificabile” ciascuno, induce a sottovalutare l’irripetibile unicità della persona.

Il malinteso anonimato del web, come la defisicizzazione dei rapporti (l’altro ridotto a immagine, profilo, *avatar*) alimentano così, soprattutto nei giovani, quell’aggressività che spesso nella vita *offline* incontra il limite dell’inibizione e la deterrenza del controllo sociale. Ma si può – e si deve - interrompere la mimesi della violenza e illuminare il lato oscuro della rete, rendendola quello strumento di libertà, pluralismo e democrazia che ben potrebbe essere. Per questo, va anzitutto difesa l’unicità della persona (con tutta la sua fragilità e fallibilità) e, con essa, la solidarietà verso l’altro, contro gli effetti deleteri di quella che Lacan definiva, con lucidità, “iocrazia”.

In questo percorso è indispensabile – molto più dei divieti - la pedagogia digitale cui il Garante ha dedicato, soprattutto ma non soltanto quest’anno, una parte significativa della propria attività, nella consapevolezza della sua necessità per costruire un futuro democraticamente sostenibile.

7. Lo sguardo presbite del diritto

La promozione, tra i cittadini, di un’adeguata “coscienza digitale” (anche rispetto all’uso di dispositivi IOT o al ricorso alla telemedicina) è una delle funzioni cui il Garante ha riservato, anche nell’anno trascorso, una particolare attenzione. Molte altre e di segno diverso, tuttavia, sono state le iniziative che hanno consentito al Garante di intervenire sui vari ambiti



Garante per la protezione dei dati personali

rimessi alla sua competenza, trasversale e, come tale, tangente ogni ambito della vita e della società. La peculiarità di questa Autorità è, anzi, proprio la poliedricità degli ambiti e delle funzioni che le sono ascritti consentendole così, in una strategia integrata, sul piano interno e internazionale, di offrire una tutela ad ampio spettro a un diritto, come quello alla protezione dei dati, tipicamente "d'avanguardia".

Così, la funzione consultiva consente al Garante di fornire, a Parlamento e Governo - con audizioni o pareri, oltre 70 nell'anno - un contributo utile a delineare, sin dall'origine, norme coerenti con le garanzie richieste dalla disciplina di protezione dei dati. Nel 2023, particolarmente significativa è stata l'attività consultiva svolta rispetto all'attuazione delle riforme processuali o in materia d'istruzione, soprattutto in ragione della piena realizzazione della piattaforma "Unica".

Ancora, nell'ambito dell'istruttoria legislativa, il Garante è stato auditato dalle Camere, in varie occasioni, anche (ma non soltanto) sulla disciplina dell'intelligenza artificiale, nella molteplicità delle sue implicazioni, con confronti tanto più proficui quanto più hanno determinato, come spesso accaduto, la revisione dei testi normativi o l'inclusione, nelle relazioni conclusive delle indagini conoscitive, delle indicazioni fornite.

Hanno svolto una rilevante funzione preventiva anche gli "avvertimenti", rivolti ad alcuni titolari di trattamenti suscettibili di determinare - in assenza di tempestive modifiche - violazioni della disciplina di protezione dei dati. Tra i provvedimenti adottati, rileva in particolare l'avvertimento rivolto a *Worldcoin* relativamente al progetto di scansione dell'iride in cambio di cryptovalute, che avrebbe potuto legittimare una raccolta di dati biometrici in assenza delle dovute garanzie e della necessaria consapevolezza da parte degli utenti. Inoltre sul tema, a



questo tangente, dello scambio di servizi contro dati, su cui pure si fonda l'architettura della *data economy*, il Comitato europeo per la protezione dei dati – in linea con la nostra giurisprudenza di legittimità - ha chiarito che il modello “*consent or pay*”, per le grandi piattaforme, può ammettersi soltanto in quanto contempra alternative equivalenti non patrimoniali. Perché, appunto, la monetizzazione del consenso non divenga un modo per rendere la privacy un lusso per pochi.

La cooperazione internazionale – realizzata pure attraverso la partecipazione ai lavori del Comitato europeo per la protezione dei dati – ha offerto anche quest'anno l'occasione di confronti particolarmente utili, come quelli funzionali alla decisione di 1.595 procedure “Imi” e quelli che, certamente, si svilupperanno nell'ambito dei lavori del G7 dei Garanti per la protezione dei dati, organizzato per ottobre prossimo proprio dall'Autorità italiana.

La funzione di controllo e decisoria ha consentito anche – ben prima che d'irrogare sanzioni, nel 2023 riscosse per quasi 8 milioni di euro - di ingiungere misure prescrittive o inibitorie, tali da attenuare o, se possibile, prevenire gli effetti pregiudizievoli delle violazioni (soprattutto per i *data breach*, notificati nell'ordine di 2.037). La tutela remediale caratterizza, in modo particolare, l'ambito della libertà di manifestazione del pensiero, rispetto al quale le misure “correttive” rappresentano spesso l'esito elettivo di controversie sui limiti delle esigenze informative o, anche, il particolare ambito del diritto all'oblio.

Rilevante è stata anche, nell'anno trascorso, l'attività funzionale all'approvazione di due importanti codici di condotta, quali quelli, rispettivamente, per le agenzie per il lavoro e sul *telemarketing*. Il primo, in particolare, introduce alcune significative garanzie per i candidati a



Garante per la protezione dei dati personali

posizioni lavorative, volte anche a impedire discriminazioni nell'accesso al mercato del lavoro. Le Agenzie aderenti al Codice si impegnano, in particolare, a trattare soltanto dati strettamente necessari all'instaurazione del rapporto di lavoro, senza svolgere indagini sulle opinioni politiche, religiose o sindacali dei lavoratori o effettuare preselezioni, neppure con il consenso dei candidati, sulla base di informazioni relative a scelte o condizioni di vita come stato matrimoniale, gravidanza, disabilità, non potendo neppure utilizzarsi informazioni su illeciti disciplinari o procedimenti giudiziari.

Il secondo codice di condotta potrà svolgere una funzione rilevante nella promozione del principio di responsabilizzazione, anche favorendo standard uniformi di conformità delle condotte dei vari attori coinvolti nella filiera delle attività promozionali, non realizzabili forse neppure con la deterrenza esercitata dal quadro sanzionatorio, pur elevato.

Tra le attività di promozione della consapevolezza delle esigenze di protezione dei dati, vanno segnalate anche le Linee guida per la conservazione delle *password*, adottate d'intesa con l'Agenzia per la cybersicurezza nazionale, volte a fornire raccomandazioni sulle funzioni crittografiche ritenute attualmente più sicure per la conservazione delle *password*, per evitarne la violazione e il conseguente utilizzo per furti di identità, richieste di riscatto o altri tipi di attacchi (la cui criticità raggiunge oggi la soglia dell'81% del totale, contro il 47% del 2019).

Questi pochi esempi testimoniano, almeno in parte, la complessa articolazione dei compiti del Garante che, combinando funzioni consultive, regolatorie, decisorie, di controllo e di *advocacy*, può offrire una tutela davvero integrata alla persona, nel suo rapporto altrimenti impari con la tecnologia. E può farlo contando sul costante impegno di un contingente di



Garante per la protezione dei dati personali

personale ristretto (e meritevole di ampliamento, proporzionalmente alle crescenti competenze dell’Autorità) ma qualificato, che voglio qui, unitamente al Collegio e al Segretario generale, sinceramente ringraziare. E ringrazio anche le Autorità che hanno inteso offrirci, in vario modo, sostegno, nonché il corpo della Guardia di Finanza, per la ormai consueta collaborazione.

La collaborazione istituzionale, la relazione costante con i cittadini, la sinergia delle varie forme di tutela offerte, la cooperazione internazionale, l’alto senso di responsabilità nello svolgimento dei compiti affidati al Garante consentono di renderne la prospettiva lungimirante quanto necessaria a comprendere, prima ancora che regolare, una realtà in costante evoluzione (quasi l’eterna velocità marinettiana), come quella digitale. Soltanto guardando oltre lo stretto orizzonte del contingente si può, infatti, tutelare un diritto – come quello alla protezione dei dati – “inquieto”, perché in costante dialettica con l’evoluzione tecnologica - e necessariamente mite, perché mai tiranno. E’, in fondo, lo sguardo presbite che deve avere il diritto per poter regolare un futuro.

Solo con uno sguardo presbite si può regolare un futuro che, per riprendere le parole di Rainer Maria Rilke, *“entra in noi, per trasformarsi in noi, molto prima che accada”*.

Vi ringrazio.



| **GPDP** |

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

RELAZIONE ANNUALE 2023



GPDP

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Pasquale Stanzione, *Presidente*
Ginevra Cerrina Feroni, *Vice Presidente*
Agostino Ghiglia, *Componente*
Guido Scorza, *Componente*

Fabio Mattei, *Segretario Generale*

Piazza Venezia, 11
00187 Roma
Tel. 06 696771
e-mail: protocollo@gdp.it
www.gdp.it



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Relazione annuale 2023

Indice

Provvedimenti collegiali

634

59

Pareri su atti normativi
e amministrativi

263

Decisioni su reclami
e segnalazioni

1.595

Procedure IMI

2.037

Violazioni dei dati
personali notificate

9.281

Riscontri a reclami
e segnalazioni

506

Riscontri a quesiti

€ 7.977.343
Sanzioni riscosse

**I numeri
del 2023**

144

Ispezioni

235

Riunioni
internazionali

7

Comunicazioni
all'Autorità giudiziaria

15.048

Contatti SRP

79

Comunicati e
Newsletter

4.263.357

Accessi al
sito web

I - STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Indice

1. Introduzione	3
2. Il quadro normativo in materia di protezione dei dati personali	16
2.1. Le leggi	16
2.2. I decreti-legge	19
2.3. I decreti legislativi	23
3. I rapporti con il Parlamento e le altre istituzioni	26
3.1. L'attività consultiva del Garante	26
3.1.1. <i>La consultazione del Garante nell'ambito del procedimento legislativo o dell'esercizio delle funzioni conoscitive, di indirizzo e controllo delle Camere</i>	26
3.1.2. <i>La consultazione del Garante su atti normativi statali di rango primario: i pareri al Governo su progetti di legge e schemi di decreto legislativo</i>	27
3.1.3. <i>I pareri sugli atti regolamentari o amministrativi in generale</i>	27
3.1.4. <i>La consultazione del Garante sugli atti normativi regionali o di province autonome</i>	29
3.1.5. <i>Segnalazioni</i>	30
3.1.6. <i>Quesiti</i>	30
3.2. Consultazione attraverso la piattaforma IMI	30
3.3. Il contributo al Governo ai fini del riscontro ad atti di sindacato ispettivo	31
3.4. L'esame delle leggi regionali al vaglio di costituzionalità del Governo	31

II - L'ATTIVITÀ SVOLTA DAL GARANTE

4. Il Garante e le amministrazioni pubbliche	35
4.1. L'attività fiscale, tributaria e in materia di antiriciclaggio	35
4.1.1. <i>La dichiarazione dei redditi precompilata</i>	35
4.1.2. <i>Antiriciclaggio</i>	37
4.2. Previdenza, assistenza sociale e altri benefici economici	38
4.3. La protezione dei dati personali in ambito scolastico e universitario	39
4.4. Trasparenza e pubblicità dell'azione amministrativa	42
4.4.1. <i>La pubblicazione di dati personali online da parte delle pubbliche amministrazioni</i>	42
4.4.2. <i>Accesso civico</i>	43
4.5. Trattamenti di dati personali effettuati dalle amministrazioni centrali, regioni ed enti locali	47
4.5.1. <i>Trattamenti di dati personali effettuati dalle amministrazioni centrali</i>	47
4.5.2. <i>Trattamenti di dati personali effettuati presso regioni ed enti locali</i>	49
4.5.2.1. <i>Ambiente</i>	49
4.5.2.2. <i>Mobilità e trasporti</i>	50
4.5.3. <i>Esercizio dei diritti</i>	50
4.6. Trattamenti per finalità amministrative	51
4.7. Servizi <i>online</i> e misure di sicurezza	52
4.8. Il RPD in ambito pubblico	53
4.9. Ordini professionali	53

Indice

4.10. Digitalizzazione della pubblica amministrazione	54
4.11. La materia anagrafica ed elettorale	57
4.12. Trattamenti di dati personali in ambito pubblico mediante dispositivi video	58
5. La sanità	60
5.1. La sanità digitale	60
5.1.1. <i>Il Fascicolo sanitario elettronico</i>	60
5.1.2. <i>Il dossier sanitario</i>	63
5.1.3. <i>La telemedicina</i>	64
5.2. L'uso dell'intelligenza artificiale in sanità	65
5.3. Trattamenti di dati personali nell'ambito dei sistemi informativi sanitari centrali	67
5.4. Trattamenti per finalità di cura e amministrative correlate alla cura	70
5.4.1. <i>Provvedimenti derivanti da data breach</i>	70
5.4.2. <i>Provvedimenti derivanti da reclami e segnalazioni</i>	74
5.4.3. <i>Provvedimenti derivanti da istruttorie attivate d'ufficio</i>	79
5.4.4. <i>Provvedimenti relativi al trattamento di dati personali effettuato nell'ambito dell'emergenza sanitaria</i>	80
5.5. Trattamenti per finalità ulteriori rispetto a quelle di cura e/o amministrative correlate alla cura	81
5.6. Esercizio dei diritti	84
6. La ricerca scientifica	86
6.1. Provvedimenti adottati ai sensi dell'art. 110 del Codice	86
6.2. Chiarimenti in merito all'art. 110-bis, comma 4, del Codice	92
6.3. Altri provvedimenti in materia di trattamenti per scopi di ricerca scientifica	93
7. La statistica	96
7.1. La statistica ufficiale	96
8. I trattamenti in ambito giudiziario e di sicurezza	99
8.1. Trattamenti in ambito giudiziario	99
8.2. Trattamenti da parte di forze di polizia	101
8.3. Pareri resi su schemi di decreti in ambito giudiziario o in relazione ad attività di polizia	101
8.4. Il controllo sul CED del Dipartimento della pubblica sicurezza	103
8.5. Il controllo sul Sistema di informazione Schengen	103
8.5.1. <i>Follow up della valutazione Schengen relativa all'Italia</i>	103
8.5.2. <i>L'attività di controllo e monitoraggio sul SIS II</i>	104
9. L'attività giornalistica	105
9.1. Dati statistici e aspetti procedurali	105
9.2. Trattamento di dati nell'esercizio dell'attività giornalistica	106
9.2.1. <i>Dati giudiziari</i>	106
9.2.2. <i>Illecita diffusione di dati sanitari</i>	106
9.2.3. <i>Dati relativi a minori</i>	107
9.2.4. <i>Dati di personaggi noti</i>	108
9.2.5. <i>Notizie di rilevante interesse pubblico e rispetto dell'essenzialità dell'informazione</i>	109
9.2.6. <i>Istanze di cancellazione rivolte agli editori</i>	111
9.3. Trattamento di dati da parte dei motori di ricerca	112

10. Cyberbullismo e revenge porn	117
11. Marketing e trattamento di dati personali	118
11.1. Il fenomeno del <i>telemarketing</i> indesiderato e l'azione di contrasto	118
11.1.1. Il telemarketing <i>illegale</i> nel settore telefonico	120
11.1.2. Il telemarketing <i>illegale</i> nel settore energetico	121
11.1.3. Attivazione <i>illecita</i> di schede telefoniche	122
11.1.4. Utilizzo di call-center ubicati fuori dall'Unione europea	123
11.1.5. Scenari evolutivi nel settore del telemarketing <i>illegale</i> : il codice di condotta	123
11.1.6. Marketing e profilazione	123
11.1.7. Marketing attraverso modelli oscuri (dark pattern) e banche dati <i>illecite</i>	124
11.1.8. Attività svolte nell'ambito della tutela del consumatore nei servizi di comunicazione elettronica	125
12. Servizi di comunicazioni elettroniche e internet	126
12.1. Meta Election Day Information (EDI)	126
12.2. Conservazione di dati di traffico	126
12.3. <i>Data retention</i> per finalità giudiziarie	126
12.4. <i>Cookie</i> e altri strumenti di tracciamento di dati personali	127
12.5. Trattamento di dati personali in rete	127
12.6. Trattamento di dati personali mediante dispositivi connessi	128
12.7. Attività in materia di trattamento dati mediante sistemi di intelligenza artificiale	129
12.8. Schemi di decisione finale ai sensi dell'art. 60, parr. 7 o 8, del RGPD	130
12.9. Procedure di cooperazione europea relative a trattamenti transfrontalieri di dati personali effettuati da fornitori di servizi della società dell'informazione	130
13. La protezione di dati personali nel rapporto di lavoro privato e pubblico	135
13.1. Trattamento di dati mediante la posta elettronica	135
13.2. Esercizio dei diritti	140
13.3. Trattamento di dati biometrici	146
13.4. Trattamento di dati sanitari	147
13.5. Videosorveglianza nei luoghi di lavoro del settore privato	148
13.6. Pubblicazione di dati in internet	151
13.7. Trattamento di dati mediante dispositivi tecnologici	151
13.8. Trattamento di dati nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti (cd. <i>whistleblowing</i>)	152
13.9. La protezione di dati nell'ambito del rapporto di lavoro pubblico	153
13.9.1. <i>Trattamento di dati per finalità di instaurazione e gestione del rapporto di lavoro</i>	154
13.9.1.1. <i>Trattamento di dati nell'ambito di procedure concorsuali</i>	154
13.9.1.2. <i>Trattamento di dati effettuato in occasione dell'accertamento del requisito vaccinale per i professionisti sanitari</i>	156
13.9.1.3. <i>Comunicazione di dati a soggetti terzi e circolazione di informazioni nei contesti lavorativi</i>	156
13.9.1.4. <i>Diffusione online di dati dei lavoratori</i>	157
13.9.2. <i>Dati personali di lavoratori in banche dati pubbliche</i>	159

Indice

Indice

14. Le attività economiche	162
14.1. Trattamento di dati in ambito assicurativo	162
14.2. Trattamento di dati in ambito bancario-finanziario e sistemi di informazioni creditizie	163
14.3. Imprese	170
14.4. Concessionari di pubblici servizi	174
14.5. Procedure IMI relative a trattamento di dati in ambito economico-produttivo	176
15. Altri trattamenti in ambito privato	178
15.1. Trattamento di dati personali nell'ambito del condominio	178
15.2. Trattamento di dati da parte di associazioni e fondazioni	180
15.3. Videosorveglianza nel settore privato	184
16. Intelligenza artificiale e diritto alla protezione dei dati personali	187
17. Violazioni dei dati personali	193
18. Il trasferimento dei dati personali all'estero	194
19. L'attività ispettiva	195
19.1. L'attività ispettiva fra programmazione e contingenze	195
19.2. Controlli <i>online</i> sulle cd. linee guida in materia di <i>cookie</i>	196
19.3. La collaborazione con la Guardia di finanza	196
20. Il contenzioso giurisdizionale	198
20.1. Considerazioni generali	198
20.2. Le opposizioni ai provvedimenti del Garante e le decisioni giudiziali di maggior rilievo	198
20.3. Il contributo del Garante nei giudizi in materia di protezione dati	209
21. Le relazioni comunitarie e internazionali	210
21.1. La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati	211
21.2. La cooperazione delle autorità di protezione dati nel settore libertà, giustizia e affari interni	220
21.2.1. Comitato di controllo coordinato	220
21.2.2. Gruppo di supervisione del sistema EUODAC	222
21.2.3. Gruppo di coordinamento della supervisione del Sistema informativo doganale	223
21.3. La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali	223
21.4. Le Conferenze internazionali ed europee	226
21.5. Le domande pregiudiziali davanti alla Corte di giustizia dell'Unione europea	227
21.6. I progetti per l'applicazione del RGPD finanziati dall'Unione europea	228
22. Attività di normazione tecnica internazionale e nazionale	230

23. L'attività di comunicazione, informazione e di rapporto con il pubblico	233
23.1. La comunicazione del Garante: profili generali	233
23.2. I prodotti informativi	235
23.3. Il sito istituzionale, i prodotti multimediali e le pubblicazioni	236
23.4. Le manifestazioni e i convegni	237
23.5. L'attività internazionale	238
23.6. L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi	238

Indice

III - L'UFFICIO DEL GARANTE

24. Attività di studio e documentazione	243
--	-----

25. La gestione amministrativa e dei sistemi informatici	244
---	-----

25.1. Il bilancio e la gestione economico-finanziaria dell'Autorità	244
25.2. L'attività contrattuale, la logistica e la manutenzione dell'immobile	245
25.3. L'organizzazione dell'Ufficio	247
25.4. "Amministrazione trasparente" e adempimenti relativi alla disciplina anticorruzione	250
25.5. Il settore informatico-tecnologico e la transizione digitale	251

IV - I DATI STATISTICI

Elenco delle abbreviazioni e degli acronimi più ricorrenti

ARERA	Autorità di regolazione per energia reti e ambiente
AGCM	Autorità garante della concorrenza e del mercato
AGCOM	Autorità per le garanzie nelle comunicazioni
AgID	Agenzia per l'Italia digitale
all.	allegato
ANAC	Autorità nazionale anticorruzione
art.	articolo
BCR	<i>Binding corporate rules</i>
c.c.	codice civile
cfr.	confronta
cons.	considerando
C.d.S.	Consiglio di Stato
c.p.	codice penale
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
CAD	codice dell'amministrazione digitale
cap.	capitolo
CDFUE	Carta dei diritti fondamentali dell'Unione europea
cd.	cosiddetto/i
CEDU	Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali
CEPD o Comitato	Comitato europeo per la protezione dei dati
cfr.	confronta
CGUE	Corte di giustizia dell'Unione europea
cit.	citato
Codice	Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101)
Corte EDU	Corte europea dei diritti dell'uomo
Cost.	Costituzione
d.d.l.	disegno di legge
d.l.	decreto-legge
d.lgs.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
doc.	documento

es.	esempio
FAQ	<i>Frequently Asked Questions</i>
FSE	Fascicolo sanitario elettronico
GEPD	Garante europeo per la protezione dei dati
Gruppo Art. 29	Gruppo dei garanti europei istituito dall'art. 29 della direttiva 95/46/CE
G.U.	Gazzetta ufficiale della Repubblica italiana
GUUE	Gazzetta ufficiale dell'Unione europea
IA	Intelligenza artificiale
IMI	<i>Internal Market Information System</i>
IVASS	Istituto per la vigilanza sulle assicurazioni
IWGDPT	<i>International Working Group on Data Protection in Telecommunications</i>
l.	legge
lett.	lettera
MEF	Ministero dell'economia e delle finanze
n.	numero
p.	pagina
p.a.	pubblica amministrazione/pubbliche amministrazioni
par.	paragrafo
PEC	posta elettronica certificata
PNRR	Piano nazionale di ripresa e resilienza
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
RGPD o Regolamento	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
RPD	Responsabile della protezione dei dati
RPO	Registro pubblico delle opposizioni
RSPP	Responsabile del servizio prevenzione e protezione
SEE	Spazio economico europeo
sez.	Sezione
SPID	Sistema pubblico dell'identità digitale
SSN	Servizio sanitario nazionale
tab.	tabella
T-PD	Comitato consultivo della Convenzione del Consiglio d'Europa n. 108/1981
t.u.	testo unico
TFUE	Trattato sul funzionamento dell'Unione europea
UE	Unione europea
URL	<i>Uniform resource locator</i>
v.	vedi



GPDP

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Stato di attuazione del Codice in materia di protezione dei dati personali

**RELAZIONE ANNUALE
2023**

PAGINA BIANCA

I - Stato di attuazione del Codice in materia di protezione dei dati personali

1 Introduzione

L'attività del Garante nel 2023 si è svolta in un contesto caratterizzato da elementi con una componente fortemente innovativa, ma è proseguita anche secondo una linea di continuità. Tre sono quelli più rappresentativi fra i primi, in estrema sintesi: digitalizzazione, intelligenza artificiale, Piano nazionale di ripresa e resilienza. Si tratta di elementi che hanno comportato, a livello nazionale, una consistente spinta alla velocizzazione di tutti i processi, compresi quelli amministrativi e, quindi, anche della risposta del Garante alle istanze provenienti dai soggetti pubblici e privati che, ciascuno per la propria parte, sono stati coinvolti in tali processi. Tuttavia, alcune costanti hanno caratterizzato il lavoro dell'Autorità nello scorso anno, confermandosi, quindi, come tratti essenziali dello scenario di protezione dati nazionale; anche in questo caso, possiamo individuare una triade: contrasto al *marketing* aggressivo, attenzione particolare ai soggetti vulnerabili, crescente internazionalizzazione dei processi. Su entrambi i versanti, che sono naturalmente reciprocamente connessi, il Garante ha sempre ricercato il difficile, talora arduo componimento degli interessi e dei diritti in gioco tenendo dritta la barra della propria missione di autorità cui è

1 Executive Summary

In 2023, the Garante carried out its activities in a scenario featuring highly innovative components, although work continued according to well-established patterns as well. Out of the former, three are especially significant. In a nutshell, they include digitalisation, artificial intelligence, and the national recovery and resilience plan. All of them entailed, at domestic level, a substantial drive towards speeding up all processes including administrative ones; this impacted the Garante's response vis-à-vis the different requests and claims from the public and private bodies that have been participating in those processes in their respective capacities. Nevertheless, there were some well-known patterns in the Garante's work as well, which confirmed their being key features in Italy's data protection scenario. Again, those features are three-fold: countering aggressive marketing, a special focus on vulnerable individuals, and the growing internationalisation of all processes. On both counts, which are clearly mutually related, the Garante has consistently aimed at the difficult, sometimes daunting objective of balancing the interests and rights at stake; in so doing, it has pursued its course unwaveringly whilst being fully aware that it is tasked with

1

demandata la tutela di diritti che sono veramente fondativi della libertà personale e sociale. Una missione che necessita di adeguate risorse umane e materiali, tuttora insufficienti nonostante i molti interventi messi in campo dal Garante nello scorso anno per potenziare le proprie strutture.

Un contributo essenziale è quello che il Garante ha fornito attraverso i pareri obbligatori resi al Parlamento e al Governo su atti normativi, di rango primario e secondario, poiché ciò ha da sempre consentito all’Autorità di indicare tempestivamente, ove necessario, aggiustamenti e correzioni di rotta. Fra i molti testi normativi esaminati (cfr. parr. 2.1, 3.1), merita ricordare la l. 7 dicembre 2023, n. 193 che mira a prevenire le discriminazioni e garantire la tutela dei diritti delle persone guarite da malattie oncologiche, sancendo il diritto al cd. oblio oncologico e attribuendo al Garante il compito di vigilare sulla sua attuazione concreta. Particolarmente utile si è dimostrato anche nel 2023 il ricorso all’audizione parlamentare, per la possibilità di instaurare un dialogo diretto fra parlamentari e Garante su tematiche di grande attualità; le audizioni del Presidente dell’Autorità dinanzi alle competenti Commissioni di Camera e Senato, ovvero le memorie presentate in rapporto a indagini conoscitive, hanno riguardato ambiti assai diversi e rilevanti – dalla legge annuale per il mercato e la concorrenza all’impiego delle intercettazioni, e finanche alle iniziative per contrastare le sfide di resistenza (*challenge*) nelle reti sociali telematiche. Peraltro, l’Autorità non ha mancato di ricordare, attraverso le proprie segnalazioni al Governo, alcune lacune della legislazione secondaria che da tempo attendono di essere colmate, in particolare con riguardo alla ricognizione dei trattamenti di dati personali nelle attività giudiziarie e di polizia, anche ai fini dell’esercizio dei diritti da parte degli interessati (cfr. par. 3.1.5).

Se è vero che i processi di digitalizzazione caratterizzano da tempo il panorama

the protection of rights underpinning our personal and social freedoms. To discharge those tasks, adequate human and financial resources are needed, which is not yet the case in spite of the multifarious steps taken by the Garante in the past year to strengthen its own organisation.

A fundamental contribution was provided through the opinions the Garante is required to issue to Parliament and the Government on primary and secondary draft legislation; in fact, this has proven consistently helpful in order to timely flag any necessary adjustments and rectifications. Out of the many legislative drafts taken into consideration (see paras. 2.1 and 3.1), reference can be made to Law No 193 of 7 December 2023, to prevent discrimination and protect the rights of individuals that have recovered from cancer-related diseases, as it set out the so-called right to oncological oblivion and tasked the Garante with supervising its enforcement. Parliamentary hearings were especially helpful in 2023 as well, since they allowed setting up a dialogue directly between MPs and the Garante on very topical issues. The President of the Garante was heard by the competent Committees at both the Chamber of Deputies and the Senate, and briefings were submitted as part of fact-finding inquiries carried out by Parliament on highly diverse as well as important topics – from the annual market and competition law to the use of wiretapping records, up to measures aimed at countering challenges on social media. On the other hand, the Garante did not fail to draw the Government’s attention to loopholes in secondary legislation that have long been in need of being cured – with particular regard to processing operations in law enforcement activities, also in order to regulate exercise of data subject rights (see para. 3.1.5).

Digitalisation has become since long a feature in Italy’s economic and social landscape; however, it is unquestionable that the pace of its development gained

economico e sociale del nostro Paese, è altrettanto vero che essi hanno subito una forte accelerazione nell'ultimo anno per una serie di fattori concomitanti – *in primis* la necessità di utilizzare i fondi messi a disposizione dal PNRR e il ricorso pervasivo a tecnologie genericamente etichettabili come di intelligenza artificiale. In questo contesto, il Garante ha esercitato la funzione consultiva che gli pertiene rispetto all'introduzione di nuove funzionalità nell'erogazione dei servizi *online* ai cittadini. Tali funzionalità perseguono in buona sostanza l'obiettivo di semplificare e accorpare le modalità di accesso ai servizi della pubblica amministrazione, e con ciò sollevano numerosi questioni in tema di proporzionalità e necessità dei trattamenti di dati personali ovvero di allocazione delle rispettive responsabilità: menzioniamo qui, a titolo esemplificativo, la gestione centralizzata delle credenziali dell'identità digitale CIE (CIEId), il *Single digital gateway* (SDG) per lo scambio transfrontaliero di prove, la Piattaforma unica per le notifiche digitali di atti amministrativi (cfr. par. 4.10). Sullo stesso versante, sono proseguite le attività connesse ai trattamenti dell'Agenzia delle entrate che, anche in omaggio al principio dell'*once only*, prevedono l'interscambio di informazioni fra amministrazioni al fine di garantire l'esattezza e completezza della dichiarazione dei redditi precompilata (cfr. par. 4.1.1), così come quelle legate all'operatività dell'Anagrafe nazionale dei residenti nelle sue molteplici articolazioni.

In questo contesto, merita di essere ricordato il provvedimento di ammonimento e correttivo nei confronti dell'ISTAT (cfr. par. 7.1) per non avere implementato alcune delle misure precedentemente individuate dall'Autorità attraverso un provvedimento del 2020 con riguardo alla realizzazione del censimento permanente (v. Relazione 2020); tali misure miravano a garantire l'attuazione di tecniche di pseudonimizzazione in grado di assicurare la minimizzazione dei dati e il rispetto del principio di

momentum over the past year due to several concurrent reasons – first and foremost, the need to make use of the funds made available through the national recovery and resilience plan along with the pervasive reliance on technology that partakes, generally speaking, of 'artificial intelligence'. Within this framework, the Garante played the advisory role it is called upon to discharge as for the introduction of new functions in delivering online services to citizens. Those functions are basically intended to simplify and streamline access to public administration services, which raises, in turn, several questions as to proportionality and necessity of the processing of personal data as well as regarding allocation of competence. By way of example, reference can be made to the centralised management of digital identity credentials (CIEId), the single digital gateway (SDG) enabling cross-border transfer of evidence, and the unified platform for the digital service of administrative instruments (see para. 4.10). Still from this perspective, the Garante continued working on processing activities by the Italian Revenue Agency, which are grounded generally speaking in the once-only principle and accordingly envisage the exchange of information between public administrative bodies to ensure that pre-completed tax returns contain accurate as well as complete information (see para. 4.1.1); the national Index of residents including its multiple components was also the subject of in-depth assessment.

It is worth mentioning here that the Garante imposed a reprimand along with corrective measures on ISTAT, the Italian statistics agency (see para. 7.1), since it was found not to have implemented some of the measures the Garante had previously set out in a decision of 2020 concerning the national census survey. Those measures were aimed at having pseudonymisation techniques in place that could ensure compliance with data minimisation and purpose limitation requirements in handling the huge

1

1

limitazione della finalità nella gestione dell'enorme mole di informazioni affidate all'Istituto.

Anche in ambito sanitario, la riforma del Fascicolo sanitario elettronico 2.0 e la realizzazione del sistema nazionale di telemedicina, che sono parte delle azioni di attuazione della Missione 6 (salute) del PNRR e presuppongono l'interconnessione tra sistemi informativi sanitari in un'ottica di digitalizzazione, hanno condotto il Garante a ribadire la necessità di coordinare le misure tecniche e organizzative da introdurre a tutela dei diritti fondamentali e dei principi generali del trattamento. Significativa anche la pubblicazione di un decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di intelligenza artificiale (cfr. par. 5.2), con cui sono state fornite indicazioni in ordine ai profili giuridici ed etici da tenere in considerazione nella realizzazione di servizi sanitari nazionali che prevedano l'utilizzo di soluzioni di IA (cfr. cap. 16). Il Garante ha ricordato che le applicazioni di IA comportano attività di profilazione e possono generare decisioni sulla base di processi esclusivamente automatizzati che, in un contesto di interesse pubblico quale quello che contraddistingue la sanità, necessitano di una base giuridica nel diritto nazionale che assicuri il rispetto dei diritti e delle libertà degli interessati. Peraltro, questi stessi principi sono stati richiamati anche con riguardo ad alcuni dei progetti inseriti nel Programma statistico nazionale (cfr. par. 7.1) sui quali il Garante ha espresso il previsto parere, in quanto essi prefigurano il ricorso a tecniche di *machine learning* per l'analisi dei dati che non possono prescindere, in particolare, da un intervento umano di supervisione qualificata dei risultati algoritmici e non devono comportare forme di discriminazione ad opera di questi ultimi.

Nell'ottica dell'attenzione costantemente posta dal Garante ai soggetti vulnerabili e alle tutele che devono essere prestate, assumono particolare rilevanza le indicazioni fornite rispetto ad alcune iniziative di matrice governativa assunte

amount of information ISTAT is empowered to access.

Turning to the health care sector, the reformation brought about in 2023 regarding the electronic health record 2.0 and the implementation of the national telemedicine infrastructure led the Garante to reiterate the need for consistent technical and organisational measures so as to protect fundamental rights and key processing principles. Both initiatives are part of the implementing activities within Mission 6 (Health) of the national recovery and resilience plan and are grounded in the interlinking of health care information systems for digitalisation purposes. A significant milestone in this connection was the publication of a decalogue for AI-based national health care systems (see para. 5.2), which provided guidance on the legal and ethical issues to be considered when setting up national health care systems that rely on AI solutions (see Chapter 16). The Garante recalled in this connection that AI applications entail profiling activities and may result into fully automated decision-making processes, which must be grounded in national law and ensure respect for data subjects' rights and freedoms in the light of the public interest underpinning the delivery of health care services. These principles were also recalled in the opinions rendered by the Garante with regard to some of the research projects that were included in the 2023 national statistics plan (see para. 7.1). Those projects envisaged use of machine learning techniques for data analysis, which made it indispensable, in the Garante's view, to include qualified human supervision of algorithmic results and to prevent discrimination on account of such algorithms.

From the perspective of the unrelenting attention paid by the Garante to vulnerable individuals and the safeguards to be afforded, special importance can be attached to the guidance made available in respect of several actions undertaken by the Italian government in 2023 – such as the 'Platform for families and

nel 2023, quali la Piattaforma famiglie e studenti, che mira a rendere disponibili appositi servizi digitali al fine di garantire il sostegno del diritto allo studio e semplificare l'erogazione delle prestazioni a favore di famiglie e studenti, ovvero l'introduzione dell'assegno di inclusione e del supporto per la formazione e il lavoro, che hanno sostituito precedenti misure di sostegno economico per le persone in difficoltà quali il reddito e la pensione di cittadinanza (cfr. par. 4.3). In una linea di continuità con pregressi pronunciamenti, il Garante è intervenuto indicando, nei singoli casi, le correzioni e le migliorie necessarie per assicurare il rispetto dei principi fondamentali di necessità e proporzionalità delle informazioni oggetto di trattamento nonché una corretta *governance* dei dati, anche attraverso una più granulare definizione dei ruoli rivestiti dai molti attori che intervengono nei processi finalizzati all'erogazione degli specifici benefici, a favore di soggetti che sono ritenuti meritevoli di particolare tutela e sostegno. A tale riguardo, merita ricordare fra le attività che rappresentano costanti dell'operato del Garante, da un lato quelle connesse alla trasparenza e alla pubblicità delle attività amministrative, con particolare riferimento alle richieste di accesso civico e ai sempre più numerosi pareri resi ai difensori civici o ai Responsabili della prevenzione e corruzione nei quali (in conformità con le linee guida pubblicate dal Garante e dall'ANAC nel 2016) si è ricercato il bilanciamento fra obblighi di trasparenza amministrativa e tutela di diritti alla riservatezza variamente declinati (cfr. par. 4.4.2); dall'altro, alcune decisioni nelle quali il Garante ha potuto perseguire violazioni della normativa in materia di protezione dei dati particolarmente gravi e odiose perché perpetrate da soggetti pubblici e pubbliche amministrazioni nei riguardi di soggetti estremamente vulnerabili: ci si riferisce, in particolare, alle misure assunte a seguito della diffusione dei dati di donne che si erano sottoposte a un'interruzione di gravidanza, indicandoli su

students', which is aimed to provide ad-hoc digital services to uphold the right to education and simplify the granting of benefits to families and students, or the newly introduced benefits for people in need of financial support (i.e., the 'assegno di inclusione' and 'supporto per la formazione e il lavoro') which superseded the so-called 'citizenship income' and 'citizenship pension' minimum income schemes (see para. 4.3). Consistently with previous decisions, the Garante stepped in to lay out such adjustments and improvements as were found to be necessary in the individual cases to ensure compliance with fundamental proportionality and necessity requirements as to the information to be processed along with adequate data governance measures; the latter included a more granular allocation of responsibilities among the many stakeholders that are involved in the processes to grant those benefits to individuals deserving protection and support.

In this connection, one of the areas the Garante has consistently covered is related to transparency and openness of administrative activities with particular regard to FOIA-type access requests and the increasing number of opinions issued to ombudspersons and managers of anti-corruption measures. In those opinions, indeed throughout those activities, the Garante has aimed to strike a balance between administrative openness requirements and protection of the right to privacy in its multifarious configurations (see para. 4.4.2) – in line with the guidelines that were published jointly by the Garante and ANAC (the national anti-corruption authority) in 2016. Reference should also be made to a few decisions in which the Garante addressed especially heinous as well as serious infringements of data protection legislation which had been committed by public bodies and administrative agencies to the detriment of highly vulnerable individuals. This is particularly the case with the decisions issued following dissemination of information

1

1

targhette apposte sulle sepolture dei feti (cfr. par. 4.6 e 5.5), ma anche ai molti casi di *data breach* nel settore sanitario che hanno visto la diffusione di volumi anche considerevoli di informazioni particolarmente delicate a causa dell'omessa o negligente attuazione di misure tecniche e organizzative adeguate in termini di sicurezza (cfr. par. 5.4.1). Per altro verso, numerosissime istruttorie sono state chiuse nel corso del 2023 in riferimento a reclami e segnalazioni presentati da interessati ultracinquantenni che erano stati oggetto di sanzioni amministrative per non aver osservato gli obblighi vaccinali connessi alla pandemia da Covid-19, individuando modalità idonee a evitare, sia nei confronti dell'Agenzia delle entrate sia nei confronti del Ministero della salute, la comunicazione di informazioni eccedenti sullo stato di salute degli interessati (cfr. par. 5.4.4).

Assai rilevante in questo stesso ambito, focalizzato sui soggetti vulnerabili, l'attività tesa ad assicurare la tutela dei dati personali nel contesto lavorativo, pubblico e privato. Numerosi, come in passato, i provvedimenti assunti in riferimento ai trattamenti svolti nelle fasi propedeutiche all'instaurazione del rapporto di lavoro nonché durante la vigenza di tale rapporto, soprattutto con riguardo all'utilizzo della posta elettronica sul luogo di lavoro e all'impiego di sistemi di videosorveglianza (cfr. par. 13.1); in tutti questi casi l'Autorità è intervenuta tenendo conto della stretta connessione esistente fra lo svolgimento dell'attività lavorativa e lo sviluppo della personalità del lavoratore, nonché delle difficoltà nel tracciare, soprattutto alla luce della pervasività dell'impiego di tecnologie digitali in ambito pubblico e privato, una vera e propria linea di confine fra ambito lavorativo o professionale e ambito strettamente privato. Su tale fondamento, il Garante ha indicato la necessità, da parte dei titolari-datori di lavoro, di un'attenta considerazione dei principi di responsabilizzazione e necessità del trattamento soprattutto ove possa configurarsi il controllo a distanza del

identifying women that had undergone abortion procedures, whose names had been tagged to the burial places of the respective foetuses (see paras. 4.6 and 5.5), or with the many data breach cases in the health care sector that led to the dissemination of at times substantial sets of highly sensitive information because of the flawed or missing implementation of adequate technical and organisational security measures (see para. 5.4.1). On the other hand, a considerable number of proceedings could be finalised in 2023 regarding complaints and alerts by data subjects aged above 50 who had been fined on account of their non-compliance with COVID-19 vaccination obligations; in particular, arrangements could be set out to prevent excessive information on those complainants' health from being communicated to the Revenue Agency or the Ministry of Health (see para. 5.4.4.) Still with regard to the focus on vulnerable individuals, one should not fail to mention the important steps taken to ensure personal data protection by both public and private employers. Many decisions were adopted – as was the case in the past – to address processing issues that had arisen both before and after entering an employer-employee relationship with particular regard to the use of emails in the workplace and the deployment of video surveillance systems (see para. 13.1). The Garante's action was grounded in the consideration that a close link exists between work and the development of the individual worker's personality, whilst a clear-cut boundary between one's professional/working life and one's personal sphere can hardly be set – especially in view of the pervasiveness of digital technologies in all the walks of life. Accordingly, the Garante emphasized the need for employers to carefully consider accountability and necessity of processing – especially if such processing may give rise to remote surveillance of workers. Mention should be made here of two guidance documents that were published last year – namely,

lavoratore. Merita ricordare in questa sede due documenti di indirizzo elaborati nel corso dell'anno – l'uno dedicato alla gestione della posta elettronica nel contesto lavorativo e al trattamento dei metadati (cfr. par. 13.7), l'altro elaborato con ANAC e dedicato alla gestione delle procedure connesse al cd. *whistleblowing* (cfr. par. 13.8) – poiché entrambi coniugano l'attenzione alla tutela dei soggetti vulnerabili (quali i lavoratori dipendenti) con l'impiego corretto degli strumenti digitali. Per altro verso, ancora una volta nella prospettiva dell'innovazione digitale, il parere reso dall'Autorità (in via d'urgenza) sulle modalità operative del portale unico per il reclutamento che tutte le pubbliche amministrazioni sono tenute a utilizzare dal 2023 (cfr. par. 13.9.2) ha permesso al Garante di indicare una serie di puntuali misure tecniche e organizzative in grado di mitigare i rischi elevati per i diritti e le libertà degli interessati che l'impiego del portale in questione comporta, visto che possono confluirci anche dati appartenenti a categorie particolari o relativi a condanne penali e reati.

Pur in presenza di una certa polverizzazione delle casistiche con riguardo ai molti reclami e alle segnalazioni riferentisi a trattamenti svolti da imprese e soggetti privati in genere, si possono comunque individuare anche in questo campo alcune costanti nel senso delineato nei paragrafi iniziali. In molti casi le doglianze hanno riguardato, secondo una consolidata tradizione, il parziale o negato riscontro a richieste di accesso formulate dagli interessati, particolarmente nei settori bancario e assicurativo, talora anche in rapporto a questioni successive ovvero a contenziosi di varia natura – riscontro rivelatosi erroneo perché i presupposti per limitare l'accesso sono spesso risultati inesistenti (cfr. parr. 14.1, 14.2). Peraltro, il Garante ha avuto modo di esaminare anche questioni complesse legate alla difficile interazione fra la disciplina a tutela degli interessi finanziari e di contrasto del riciclaggio e quella a tutela della riservatezza (cfr.

a guidance paper addressing the use of emails in the workplace along with the processing of metadata (see para. 13.7), and a paper drafted jointly with ANAC to regulate whistleblowing-related procedures (see para. 13.8). Both papers try to reconcile the protection of vulnerable individuals (such as employees) with the appropriate use of digital tools. From a digital innovation perspective, the Garante issued an urgent opinion on the operating arrangements of the unified recruitment portal all public administrative bodies have been required to rely upon since 2023 (see para. 13.9.2), where detailed technical and organisational measures could be laid down to mitigate the high risks to data subjects' rights and freedoms arising from use of the portal; indeed, special category data along with data concerning sentences and criminal offences may be fed into the portal in question.

Despite a somewhat motley set of cases arising from the many complaints and alerts filed with the Garante in connection with processing activities by private bodies, there is a pattern to be identified also in this sector along the lines we recalled in the foregoing paragraphs. In many cases, the complaints had to do with the failure to grant access, partially or in full, to data subjects' personal information – especially in the banking and insurance sectors. This is part of a long-standing tradition and includes cases arising from litigation on the estate of deceased individuals as well as on multifarious issues. The complaints in question were mostly found to be substantiated since there were no grounds for refusing access (see paras. 14.1 and 14.2). The Garante also addressed complex issues relating to the difficult *Interplay* between the legislation protecting financial interests and countering money-laundering and the legislation protecting personal data (see para. 14.2); here the Garante reaffirmed the importance of striking the right balance between preventing money laundering in accordance with the due dil-

1

1

par. 14.2), ribadendo l'importanza di trovare un giusto equilibrio tra l'interesse a prevenire il riciclaggio di denaro nella logica della *due diligence* e gli interessi sottesi ai diritti fondamentali alla protezione dei dati e alla vita privata – in questo caso, applicando un identico grado di diligenza attraverso verifiche incrociate e puntuali nell'accertare la riferibilità a un determinato interessato di informazioni negative pubblicamente disponibili. Significativi poi, in una prospettiva più generale, i numerosi interventi dell'Autorità, comprendenti anche accertamenti ispettivi, nei confronti di concessionari di pubblici servizi nel mercato energetico, in una fase storica caratterizzata dalla transizione verso il mercato libero e, per tale motivo, dal palesarsi di pratiche illecite a opera di alcuni fornitori per l'acquisizione di contratti non richiesti mediante trattamento di dati personali inesatti e non aggiornati (cfr. par. 14.4). In molti casi il Garante ha potuto evidenziare che il fenomeno era frutto dell'inadeguatezza delle misure tecniche e organizzative adottate dai fornitori al fine di garantire il rispetto delle prescrizioni impartite ai rispettivi responsabili di trattamento – ossia, del mancato rispetto dei requisiti di *accountability* fissati nel RGPD.

Si inserisce in questa stessa linea di persistente inosservanza delle norme a tutela degli interessati l'attività di contrasto del *telemarketing* aggressivo che, anche nel 2023, non ha mostrato sensibili ridimensionamenti. L'Autorità è intervenuta su più piani e a più livelli (cfr. par. 11.1), analizzando l'attività di intermediari e *call center* in quanto anelli essenziali, e talora deboli, di una catena in cui l'assenza di strumenti di controllo che impediscano alle imprese di utilizzare contatti acquisiti in violazione delle norme si è confermata una delle cause primarie delle violazioni riscontrate. Tuttavia, due elementi positivi in questo panorama sono rappresentati da un lato dall'approvazione del codice di condotta per le attività di *telemarketing* e *teleselling*, che vuole promuovere l'*accountability* del

igence paradigm and the protection of the fundamental rights to privacy and data protection – in particular, by applying the same measure of diligence in cross-checking whether publicly available negative information did relate to an individual data subject. From a broader perspective, special importance should be attached to the many decisions adopted by the Garante – at times following on-site inspections – vis-à-vis utility suppliers on the energy market. Against the backdrop of the ongoing transition towards a deregulated energy market, one is faced with unlawful practices by some suppliers which attempt to execute unsolicited contracts by processing inaccurate and/or obsolete personal data (see para. 14.4). Evidence could be found in many such cases of the inadequate technical and organisational measures put in place by suppliers in order to achieve compliance with the instructions they were supposed to give to their processors – in short, non-compliance with the accountability requirements set out in the GDPR was the key factor.

The fight against aggressive telemarketing is yet another example of the areas where data subjects continue to be in sore need of protection; indeed, there were no major breakthroughs in this area during 2023. The Garante carried on its action according to a multi-layered approach (see para. 11.1) by addressing the activities of data brokers and call centres which act as indispensable – sometimes weak – links in a chain of actors lacking effective tools to prevent suppliers from relying on contact information that was acquired unlawfully – in fact, this proved to be one of the main reasons underlying the infringements found by the Garante. Nevertheless, there were two positive developments in this scenario – namely, the approval of the telemarketing and tele-selling code of conduct, which is aimed at fostering accountability, along with the full deployment of the automated system to report unlawful telemarketing via the

settore; dall'altro, dalla piena operatività del sistema automatizzato di segnalazioni in materia di *telemarketing* implementato attraverso il portale web dell'Autorità (v. Relazione 2022), che ha consentito di ricavare preziose informazioni incrociando i dati raccolti con altri provenienti da attività ispettive o di altra natura e, quindi, di promuovere accertamenti ancor più mirati e completi (cfr. par. 11.1.5). Le molteplici istruttorie condotte dall'Autorità in questo ambito hanno riguardato anche soggetti operanti in chiave transfrontaliera e, pertanto, hanno richiesto attività di cooperazione nel quadro del meccanismo di sportello unico di cui all'art. 60 del RGPD (cfr. par. 12.5).

Ancor più pregnante si è dimostrato il livello di cooperazione internazionale richiesto nella gestione di casi, taluni di alto profilo, riguardanti la tutela dei dati personali nelle comunicazioni elettroniche e, in generale, in rete. In una percentuale importante di tali casi si è potuta raggiungere una composizione degli interessi in gioco attraverso procedure più snelle che hanno consentito di fornire un rimedio efficace ai reclamanti in tempi relativamente contenuti (cfr. par. 12.9). Per altro verso, nel 2023 vi sono stati alcuni significativi interventi dell'Autorità nei confronti di grandi *player* internazionali, anche non stabiliti nell'Unione europea, che hanno sollevato interrogativi importanti sull'utilizzo delle tecniche di intelligenza artificiale nelle loro molteplici articolazioni e, al contempo, hanno funto da stimolo per una riflessione a livello europeo su approcci coordinati ed efficaci nell'ottica di una tutela equilibrata e tempestiva (cfr. par. 12.7).

Come si è ricordato in più occasioni nelle pagine che precedono, è proprio la ricerca di un punto di equilibrio fra innovazione e regolazione che ha caratterizzato da sempre, e soprattutto negli ultimi anni, l'attività del Garante. In nessun ambito questo si dimostra più necessario che in quello legato all'intelligenza artificiale, e in questo senso il 2023 ha visto il conseguimento di un

Garante's web portal (see also the 2022 Report). The latter allowed obtaining valuable information by cross-checking the information contained in the alerts with the data collected in the course of inspections or other activities, which made it possible to plan increasingly targeted as well as thorough investigations (see para. 11.1.5). The many proceedings the Garante set up in this area also concerned cross-border processing situations and required accordingly the Italian authority to pursue cooperation via the one-stop-shop mechanism under Article 60 of the GDPR (see para. 12.5). International cooperation proved all the more necessary in handling (high-profile) cases concerning the protection of personal data in electronic communications and more generally on the Internet. A substantial number of these cases could be settled by way of expeditious procedures that allowed complainants to vindicate their rights with a relatively short turnaround time (see para. 12.9). On the other hand, the past year also witnessed some significant steps taken by the Garante vis-à-vis major international players, also outside the EU, which raised key questions on the use of AI techniques from multifarious standpoints; at the same time, this worked as a driver for European-level brainstorming initiatives aimed to devise co-ordinated, effective approaches and achieve balanced as well as timely protection (see para. 12.7).

As recalled more than once in the preceding paragraphs, it is exactly the attempt to reconcile innovation and regulation that has been a standing feature of the Garante's action – never more so than over the past few years. In no area did this prove more necessary than in the AI-related one. From this standpoint, a major achievement at supranational level in 2023 was the pre-finalisation of the EU regulation on AI, which is intended to ensure the reconciliation mentioned above. Work also continued relentlessly within the Council of Europe to lay down a framework Convention, which

1

1

importante risultato a livello sovranazionale con la sostanziale definizione del regolamento dell'UE che mira a garantire proprio tale equilibrio, nonché con i lavori proseguiti in seno al Consiglio d'Europa per la definizione di una Convenzione quadro significativamente dedicata all'IA e "ai diritti umani, la democrazia e lo stato di diritto" (cfr. cap. 16). In questo quadro, pur facendo espressamente salva la disciplina in materia di protezione dei dati personali, non si può non rilevare che il futuro regolamento europeo sull'IA lascia aperta la questione (largamente rimessa ai legislatori nazionali) delle autorità nazionali competenti e del loro coordinamento nelle funzioni di controllo. Da tempo, il Garante (v. Relazione 2022) ha rappresentato le ragioni della preminenza dell'Autorità in tale ambito alla luce della stretta connessione fra il funzionamento dei sistemi di IA e l'utilizzo di dati personali, nonché della necessità di disporre di un controllo pienamente indipendente (quale il Garante) ai fini di una supervisione efficace di questi sistemi.

Le tematiche dell'IA e della digitalizzazione sono state oggetto e spunto di numerose attività in *forum* europei e internazionali ai quali il Garante ha sempre costantemente e attivamente partecipato. Non è un caso che il G7 delle autorità di protezione dei dati (fra cui il Garante), tenutosi a Tokyo nel 2023, abbia adottato una dichiarazione congiunta proprio sul tema dell'IA e della necessità di approcci di *privacy by design* in tale ambito (cfr. par. 21.4), e che le nuove tecnologie e i flussi di dati transfrontalieri figurino in modo prominente nel programma di lavoro di questo consesso (che nel 2024 sarà ospitato a Roma e presieduto dal Garante). Lo stesso dicasi per le attività del Garante in ambito OCSE e Consiglio di Europa e, soprattutto, per le attività di cooperazione in ambito UE, attraverso i lavori del Comitato europeo per la protezione dei dati (CEPD). Quest'ultimo si è confrontato più volte, nello scorso anno, con i riflessi della strategia digitale dell'Unione nelle

is significantly addressing AI and 'human rights, democracy and the rule of law' (see Chapter 16). One should not fail to highlight in this connection that the (future) EU AI regulation leaves it largely to national law-makers to determine national competent authorities and how they should co-ordinate supervisory efforts – although it explicitly leaves personal data protection legislation unprejudiced. The Garante had already pleaded (see the 2022 Report) for recognising the primacy of data protection authorities in this area, given the close link existing between operation of AI-based systems and use of personal data as well as in the light of the need to engage with a fully independent body (such as the Garante) in order to ensure effective supervision of those systems.

AI and digitalisation were both the subject and the driver of several activities in European and international forums to which the Garante has always provided its active contribution. It is no chance that the 2023 G7 Roundtable of data protection authorities (including the Garante) held in Tokyo adopted a joint statement exactly on AI and the need for privacy by design approaches in this area (see para. 21.4), whilst new technologies are quite prominent on the agenda of the G7 DPA's roundtable – which in 2024 will be hosted in Rome under the Garante's chairpersonship. The same goes for the activities carried out by the Garante within the OECD and the Council of Europe, and even more so for cooperation activities at EU level within the framework of the European Data Protection Board (EDPB). The latter repeatedly tackled the data protection impact of the EU's digital strategy over the past year by having regard to the many instruments involved (from the DMA to the DGA); additionally, the EDPB through its many subgroups dealt with the increasingly frequent interactions between the data protection legal framework and other legal domains including, in particular, consumer protection and the risks aris-

sue molteplici sfaccettature (dal DMA al DGA), che hanno tutte impatti sulle questioni di protezione dei dati; inoltre, attraverso il lavoro dei molti sottogruppi in cui si articola, il CEPD si è occupato delle sempre più frequenti istanze di interazione fra il quadro giuridico in materia di protezione dei dati e altri ambiti quali, in particolare, la tutela dei consumatori e i rischi inerenti all'utilizzo degli strumenti digitali (compresi *social media*). Quanto ai flussi di dati personali, merita ricordare in questa sede il contributo fornito dal Garante ai lavori del CEPD per il parere obbligatorio sulla progettata decisione di adeguatezza ai fini dei trasferimenti di dati fra UE e USA, poi adottata dalla Commissione europea con riguardo al nuovo *Data Privacy Framework* (cfr. par. 21.1). Per altro verso, il 2023 ha visto anche la proposta della Commissione europea (2023/348) di un nuovo regolamento che dovrebbe integrare il RGPD al fine di potenziare e facilitare la cooperazione fra autorità di controllo nei casi di trattamenti transfrontalieri (cfr. par. 21.1). La proposta è stata oggetto di un importante parere congiunto di CEPD e Garante europeo per la protezione dei dati, redatto con il coordinamento del Garante italiano, e rappresenta la spia della sempre maggiore volontà di armonizzazione e cooperazione europea e internazionale che, come si è detto, caratterizza le attività delle autorità di protezione dati e, *in primis*, anche del Garante.

Sempre in quest'ottica, è necessario osservare che l'anno trascorso ha visto anche un aumento consistente degli interventi interpretativi della Corte di giustizia dell'UE a seguito di richieste di rinvio pregiudiziale in relazione a disposizioni del RGPD e della direttiva polizia e giustizia (cfr. par. 21.5). Con questi interventi, per i quali il Garante ha sempre fornito memorie e contributi di analisi ai competenti organismi nazionali, la Corte ha di fatto delineato importanti elementi applicativi in tema, per esempio, di risarcimento del danno immateriale conseguente al trattamento

ing from the use of digital tools such as social media. As for personal data flows, the contribution provided by the Garante to the EDPB's work on the draft adequacy decision concerning EU-US data transfers should be mentioned here along with the decision the Commission subsequently adopted to set up the new Data Privacy Framework (see para. 21.1). On the other hand, 2023 also marked the tabling of a proposal by the European Commission (2023/348) for a new regulation that is intended to supplement the GDPR in order to enhance and facilitate cooperation among data protection authorities in cross-border processing cases (see para. 21.1). The proposal was addressed in a major joint opinion by EDPB and EDPS, which was drafted under the Garante's coordination; it is a token of the increasingly stronger drive towards harmonisation and cooperation at both European and international level, which is actually – as already pointed out – a feature of the activities carried out by data protection authorities in general, and by the Garante in particular.

Still from this standpoint, one should mention that there was a substantial increase in the preliminary rulings by the Court of Justice of the EU in 2023 concerning interpretation of provisions in both the GDPR and the law enforcement directive (see para. 21.5). Those rulings, for which the Garante consistently provided briefings and contributions to the competent national bodies, actually led the Court to outline key implementing approaches regarding, for instance, compensation for non-material damage resulting from the processing of personal data, exercise of access rights, controllership and joint controllership, and the exercise of the powers conferred on data protection authorities.

Two areas where the trends mentioned in the above paragraphs are especially prominent include the handling of cases related to journalism and freedom of expression (see Chapter 9), on the one hand, and to revenge porn, on the other

1

1

di dati personali, di esercizio del diritto di accesso, di titolarità e contitolarità dei trattamenti, e dell'esercizio dei poteri da parte delle stesse autorità.

Due settori nei quali le linee di tendenza sopra ricordate emergono con particolare evidenza sono quelli concernenti i casi in materia di giornalismo e libertà di manifestazione del pensiero (cfr. cap. 9), da un lato, e quelli in materia di *revenge porn* per i quali, come è noto, l'art. 144-bis del Codice conferisce all'Autorità specifici poteri (cfr. cap. 10). Per i primi, il costante bilanciamento fra libertà di informazione e rispetto dell'identità personale si è estrinsecato nell'esame di un elevato numero di reclami e segnalazioni che lamentavano violazioni per la diffusione di notizie in rete e sui *social media*, quasi equamente suddivise fra istanze rivolte ai motori di ricerca al fine di ottenere la deindicizzazione principalmente di contenuti ritenuti obsoleti (in omaggio al cd. diritto all'oblio) e istanze rivolte a organi di informazione, queste ultime primariamente finalizzate a ottenere la rimozione di dati ritenuti eccedenti e non conformi al principio di essenzialità delle informazioni oggetto di pubblicazione. Mentre su questo versante l'Autorità si è mossa secondo principi di equo bilanciamento degli interessi in gioco, sanciti peraltro da una copiosa giurisprudenza nazionale e sovranazionale, nel caso degli interventi in materia di *revenge porn* il Garante ha operato, come previsto dalle norme, per prevenire e contrastare un fenomeno di particolare violenza e odiosità, anche attraverso l'implementazione di un'apposita procedura di segnalazione *online* che ha comportato un incremento consistente delle segnalazioni ricevute nel corso dell'anno. In quasi la metà di tali segnalazioni è stata adottata in via d'urgenza una determinazione dirigenziale per ottenere il blocco preventivo dei contenuti sessualmente espliciti dei quali si paventava la diffusione. Si tratta di misure che hanno natura para-emergenziale e che non possono, evidentemente, costituire l'unica risposta istituzionale al problema.

hand; concerning the latter, it should be recalled that Section 144-a of the data protection Code does confer specific powers on the Garante (see Chapter 10). As to the former, the balancing exercise between freedom of the press and respect for an individual's identity was carried out by dealing with a substantial number of complaints and alerts alleging violations due to the dissemination of information on the Internet and social media. Those cases involved, to an almost identical extent, delisting requests to search engines mainly in respect of allegedly obsolete information – in accordance with the so-called right to be forgotten – and requests submitted to media outlets mostly in order to have contents removed because of their being allegedly excessive and in breach of the principle of materiality of the information to be published. In all these instances the Garante pursued the equitable balancing of the interests at issue, also in the light of the wealth of case-law on this subject matter; conversely, as for revenge porn, the Garante took action as required by the law in order to prevent and counter an especially violent as well as disreputable crime. To that end, an ad-hoc online alerting procedure was implemented, which resulted into a steep increase in the number of alerts received over the past year. In almost half of those cases, an urgent decision by the competent department was issued to block the sexually explicit contents that were allegedly about to be disseminated. Needless to say, these steps are taken in an emergency situation and they are certainly not enough to tackle the issue from a public interest perspective.

Key importance should be attached in this context also to the information and awareness-raising initiatives by the Garante, which included both an information campaign addressing consumers and citizens in general (see para. 23.1) and targeted awareness-raising actions concerning aggressive marketing, the risks of generative AI, or the measures to protect children online. Public events

In questo senso, continuano a rivestire importanza primaria anche le attività di comunicazione e sensibilizzazione condotte dall’Autorità, che hanno visto sia una campagna di informazione istituzionale generalista rivolta ai consumatori e ai cittadini in genere (cfr. par. 23.1), sia attività mirate alla sensibilizzazione su temi quali il *marketing* invasivo, i rischi dell’intelligenza artificiale generativa, le misure a tutela dei minori nelle attività *online*. Eventi pubblici ad ampia partecipazione, quali lo “*State of Privacy 2023*” (cfr. par. 23.1), hanno permesso di veicolare in modo quanto più possibile capillare il messaggio della necessaria sinergia e consapevolezza di istituzioni e cittadini per individuare soluzioni anche innovative e creative, che consentano di navigare il mondo della digitalizzazione e delle tecnologie innovative senza perdere di vista quell’approccio antropocentrico che caratterizza l’intera disciplina europea in materia di protezione dei dati e *privacy*.

Non è certo un caso che il RGPD affermi al suo cons. 4 che “il trattamento dei dati personali dovrebbe essere al servizio dell’uomo”. Questo è l’obiettivo che il Garante ha da sempre perseguito, e che ha acquistato ulteriore rilevanza e risonanza negli ultimi tempi. La Relazione che segue, supportata dalle informazioni statistiche di dettaglio che, come di consueto, forniscono in forma tabellare un puntuale riscontro numerico, dà conto del lavoro svolto, un lavoro complesso, talora difficile, ma sempre appassionante, del quale questa breve introduzione ha cercato di schematizzare le linee di tendenza e i contenuti principali.

such as the ‘2023 State of Privacy’ conference organised by the Garante (see para. 23.1) had a large audience discussing ways to ensure that public authorities and citizens work jointly and knowledgeably as required in order to devise innovative, creative solutions to navigate digitalisation and new technologies – which is ultimately aimed to uphold the human-centered approach underpinning the whole European legal framework on privacy and data protection.

Recital 4 GDPR states that ‘the processing of personal data should be designed to serve mankind.’ This is certainly no chance statement. Indeed, this is the objective the Garante has consistently pursued, and this has taken on further significance and importance over the past few years. The Report contained in the following sections is supported by detailed statistical information providing – as is customary – in-depth numerical evidence in tabled format of the work carried out by the Garante. Our work is a complex, at times a daunting task – however, it is work performed with passion, and this short executive summary has barely scratched its surface by pointing to key trends and highlights in the past year.

1

2 Il quadro normativo in materia di protezione dei dati personali

Nel 2023 sono stati approvati numerosi provvedimenti normativi rilevanti (pur in diversa misura), in termini di protezione dei dati personali. Nell'impossibilità di descriverli tutti, si analizzano di seguito gli atti normativi maggiormente incidenti sulla materia.

2.1. Le leggi

Legge di bilancio 2024

La legge 30 dicembre 2023, n. 213, recante il bilancio di previsione dello Stato per l'anno 2024 e bilancio pluriennale per il triennio 2024-2026 prevede alcune disposizioni di interesse in materia di protezione dei dati personali tra le quali si segnalano, in particolare, le seguenti:

- il comma 60 dell'art. 1, che, al fine di contrastare l'evasione nel settore del lavoro domestico, legittima l'Agenzia delle entrate e l'INPS a realizzare – con modalità definite d'intesa – la piena interoperabilità delle banche dati per lo scambio e l'analisi dei dati, anche attraverso l'utilizzo di tecnologie digitali avanzate;

- il comma 86 dell'art. 1, in materia di variazione dello stato dei beni immobiliari, che legittima l'Agenzia delle entrate e della riscossione a verificare, sulla base di specifiche liste selettive elaborate con l'utilizzo delle moderne tecnologie di interoperabilità e analisi delle banche dati, la presentazione, ove prevista, della dichiarazione di variazione dei beni (art. 1, commi 1 e 2, d.m. 19 aprile 1994, n. 701), ai fini degli eventuali effetti sulla rendita dell'immobile presente in atti nel catasto dei fabbricati;

- il comma 100 dell'art. 1, che, nel predisporre misure di contrasto all'evasione e razionalizzazione delle procedure di compensazione dei crediti, prevede modifiche al d.P.R. n. 602/1973, recante disposizioni sulla riscossione delle imposte sui redditi. In particolare viene aggiunto al decreto l'art. 75-ter, il quale, al fine di assicurare la massima efficienza dell'attività di riscossione, legittima l'agente della riscossione ad avvalersi, prima di avviare l'azione di recupero coattivo, di modalità telematiche di cooperazione applicativa e degli strumenti informatici per l'acquisizione di tutte le informazioni necessarie, da chiunque detenute.

È previsto il parere del Garante sulla definizione, da parte del Ministero dell'economia e delle finanze (MEF), delle soluzioni tecniche in grado di assicurare l'utilizzo di tali strumenti informatici per l'accesso alle informazioni necessarie ai fini della riscossione.

Legge concorrenza

La legge annuale per il mercato e la concorrenza, 30 dicembre 2023, n. 214, comprende varie disposizioni particolarmente rilevanti sotto il profilo della protezione dei dati personali. Esse sono state oggetto di analisi, da parte del Garante, nell'ambito dell'audizione tenuta presso la 9^a Commissione del Senato il 5 settembre 2023 oltre che nella memoria inviata alla X Commissione della Camera dei deputati il 29 novembre 2023 (cfr. par 3.1.1).

Il Garante, in tali sedi, ha rimarcato il fatto che la disciplina dettata dalla legge interessa la protezione dei dati sotto un duplice profilo; da un lato, interviene sul rapporto, sempre più stretto, tra protezione dei dati e tutela consumeristica (art. 2); dall'altro, adeguando l'ordinamento interno al *Digital Markets Act*, delinea un quadro regolatorio denso di interrelazioni tra protezione dati e disciplina, appunto, dei mercati digitali (art. 18).

2

Il Garante si è quindi soffermato sulle norme di cui all'art. 2 che, nel disciplinare l'utilizzo dei contatori intelligenti di seconda generazione, regolano l'accesso ai dati di consumo tramite il Sistema informativo integrato.

In particolare l'art. 2 - novellando il d.lgs. 4 luglio 2014, n. 102, di recepimento della direttiva 2012/27/UE - prevede che Acquirente unico S.p.A., in qualità di gestore del Sistema informatico integrato, metta i dati del contatore di fornitura a disposizione del cliente finale o, su sua richiesta formale, di un soggetto terzo univocamente designato, in un formato facilmente comprensibile che possa essere utilizzato per confrontare offerte comparabili ovvero per l'erogazione di servizi da parte di tali soggetti terzi. Ciò avverrà tramite il Portale dei consumi di energia elettrica e di gas naturale e "nel rispetto della normativa in materia di protezione dei dati personali". Il medesimo articolo stabilisce altresì che venga istituito presso Acquirente unico S.p.A. un registro informatico recante l'elencazione dei soggetti terzi che accedono ai dati del cliente finale, teso a garantire a titolo gratuito la messa a disposizione dei clienti finali di ciascuna informazione concernente gli accessi ai dati da parte dei soggetti terzi, compresa la loro cronologia e la tipologia di dati consultati.

Nei suoi interventi il Garante, dopo aver ricordato il coinvolgimento del Garante nel quadro dell'istituzione, nel 2019, da parte di ARERA, del Portale consumi, aveva suggerito alcune precisazioni da introdurre nel testo - tuttavia non recepite dal legislatore - tese a definire i limiti di ordine oggettivo e soggettivo dell'accesso al Portale, specificando il novero delle "terze parti" abilitate a fruire della messa a disposizione dei dati di consumo dei clienti finali, nonché le tipologie di dati "relativi all'immissione" e al "prelievo" di energia elettrica e di gas naturale.

Il Portale consumi contiene infatti una molteplicità di dati personali (es. dati anagrafici, POD e PDR, pratiche di *switching*, dati contrattuali, ecc.) la cui ampia disponibilità, da parte di soggetti diversi dall'interessato, potrebbe determinare implicazioni importanti sulla riservatezza (si pensi al fenomeno diffuso dell'attivazione fraudolenta di utenze nel mercato libero dell'energia).

Si è sottolineata, inoltre, l'esigenza di individuare in maniera più dettagliata le finalità dell'accesso, con una formulazione più circoscritta rispetto a quella relativa al confronto tra "offerte comparabili" o "all'erogazione di servizi da parte dei predetti soggetti terzi", di per sé inadeguata a escludere scopi ulteriori (es. profilazione dei clienti, elaborazione di dati statistici, ecc.) rispetto a quelli più strettamente connessi alla valutazione dell'impronta energetica del cliente finale o del confronto di offerte comparabili perseguite dalla normativa (v. in merito anche le dir. 2019/944/UE e 2012/27/UE).

Ulteriori considerazioni svolte hanno riguardato l'art. 18, che adegua l'ordinamento interno al reg. (UE) 2022/1925 (cd. *Digital Markets Act*), individuando quale autorità designata per l'esecuzione l'AGCM. La norma fa correttamente salve le competenze generali di supervisione e controllo del Garante, con particolare riguardo ad alcuni dei profili disciplinati dal regolamento, di maggiore rilievo per la protezione dei dati personali (art. 18, comma 8).

L'esplicitazione di tale clausola di salvaguardia, pur ricavabile dall'ordinamento sovranazionale, si rende necessaria - come sottolineato dal Garante nelle interlocuzioni preliminari avute con il Governo in materia - al fine di evitare, sul piano interno, potenziali conflitti e sovrapposizioni di competenze tra le autorità coinvolte. Come pur ricordato nel corso dell'audizione, infatti, l'esigenza di un adeguato coordinamento e, quindi, della leale collaborazione tra autorità per la concorrenza e per la protezione dei dati è stata affermata in linea generale dalla CGUE nella sentenza 4 luglio 2023 (C-252/21), osservando anche come le prime debbano consultare le seconde laddove, nell'ambito di proprie istruttorie, vengano in rilievo profili incidenti sulla protezione dei dati.

Oblio oncologico

Particolarmente rilevante è la legge 7 dicembre 2023, n. 193 che, nel dettare le disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone guarite da malattie oncologiche, recepisce le istanze della risoluzione del Parlamento europeo 16 febbraio 2022 sul rafforzamento dell'Europa nella lotta contro il cancro – verso una strategia globale e coordinata (2020/2267(INI)).

Nel definirne l'oggetto e le finalità, l'art. 1 della legge effettua un espresso richiamo agli artt. 2 (riconoscimento dei diritti inviolabili dell'uomo), 3 (eguaglianza e pari dignità sociale) e 32 (diritto fondamentale alla tutela della salute) della Costituzione e agli artt. 7 (rispetto della vita privata e della vita familiare), 8 (protezione dei dati di carattere personale), 21 (non discriminazione), 35 (protezione della salute) e 38 (protezione dei consumatori) della Carta dei diritti fondamentali dell'Unione europea, oltre che all'art. 8 (diritto al rispetto della vita privata e familiare) della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. In aggiunta, il comma 2 del suddetto articolo definisce il diritto all'oblio oncologico quale "diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica".

Il secondo articolo della legge disciplina l'accesso ai servizi finanziari, bancari, d'investimento e assicurativi, oltre che nell'ambito della stipulazione di ogni altro tipo di contratto, anche esclusivamente tra privati, quando le informazioni di salute siano suscettibili di influenzarne condizioni e termini. Tale articolo stabilisce dunque che il consumatore non sia tenuto a fornire informazioni relative a pregresse condizioni di salute concernenti patologie oncologiche trascorsi dieci anni dalla fine del trattamento terapeutico, ovvero cinque anni qualora la diagnosi sia stata formulata prima del compimento dei diciotto anni d'età e che gli operatori finanziari in tutte le fasi di accesso dei consumatori a tali servizi, ivi compresi le trattative precontrattuali e la stipula o il rinnovo di contratti, devono fornire alla controparte adeguate informazioni circa tale diritto.

Il medesimo articolo prevede, inoltre, che le informazioni sullo stato di salute non possano essere acquisite neanche da fonti diverse dal contraente e, qualora siano comunque nella disponibilità dell'operatore o dell'intermediario, non possano essere utilizzate per la determinazione delle condizioni contrattuali.

Il comma 7 dell'art. 2, dispone che sui provvedimenti (delibera CICR e provvedimento IVASS) tesi ad individuare le modalità di attuazione delle garanzie di riserbo nei confronti di società finanziarie e assicurative venga acquisito il parere del Garante.

Analoghe garanzie di riserbo vengono previste poi all'art. 4, il quale prevede il divieto di richiedere – ai fini dell'accesso a procedure concorsuali – informazioni relative allo stato di salute degli interessati concernenti patologie oncologiche se trascorsi 10 o 5 anni a seconda dell'età.

Particolare interesse assume, infine, l'art. 5 della legge che detta le disposizioni transitorie e finali, attribuendo al Garante la funzione di vigilanza sulla corretta applicazione delle disposizioni di cui al provvedimento in oggetto (comma 4).

La legge 9 agosto 2023, n. 111, recante delega legislativa per la riforma fiscale, ha indicato in particolare, tra i criteri direttivi per l'esercizio della delega, la predisposizione di strumenti per prevenire, contrastare e ridurre l'evasione e l'elusione fiscale, anche attraverso:

1) la piena utilizzazione dei dati che affluiscono al sistema informativo dell'Anagrafe tributaria, il potenziamento dell'analisi del rischio, il ricorso alle tecnologie digitali e alle soluzioni di intelligenza artificiale, nel rispetto della disciplina dell'UE sulla tutela dei dati personali, nonché il rafforzamento del regime di adempimento collaborativo ovvero l'aggiornamento e l'introduzione di istituti, anche premiali, volti

Delega fiscale

a favorire forme di collaborazione tra l'amministrazione finanziaria e i contribuenti;

2) la piena utilizzazione dei dati resi disponibili dalla fatturazione elettronica e dalla trasmissione telematica dei corrispettivi nonché la piena realizzazione dell'interoperabilità delle banche di dati, nel rispetto della disciplina dell'UE sulla tutela dei dati personali.

L'art. 16 della legge indica, tra i principi e criteri direttivi relativi alla revisione generale degli adempimenti tributari, l'introduzione di misure per la semplificazione degli obblighi dichiarativi e di versamento.

In tale quadro prevede che si incentivino, con sistemi premiali, l'utilizzazione delle dichiarazioni precompilate, ampliando le categorie di contribuenti interessate e facilitando l'accesso ai servizi telematici per i soggetti con minore attitudine all'utilizzo degli strumenti informatici (lett. g); che si semplifichino le modalità di accesso dei contribuenti ai servizi messi a disposizione dall'amministrazione finanziaria (lett. h) anche incrementando il numero dei servizi digitali a disposizione dei cittadini (lett. i).

La disposizione stabilisce inoltre che si provveda al potenziamento di strumenti e modelli organizzativi che favoriscano la condivisione dei dati e dei documenti, in via telematica, tra l'Agenzia delle entrate e i competenti uffici dei comuni, anche al fine di facilitare e accelerare l'individuazione degli immobili non censiti e degli immobili abusivi.

L'art. 17, infine, indica principi e criteri direttivi specifici per la revisione dell'attività di accertamento, di adesione e di adempimento spontaneo.

Si prevedono specificamente misure di semplificazione del procedimento accertativo, anche mediante l'utilizzo delle tecnologie digitali, con conseguente riduzione degli oneri amministrativi a carico dei contribuenti, oltre che un'applicazione generalizzata del procedimento del contraddittorio.

È previsto inoltre che vengano razionalizzate e riordinate – in conformità alla normativa in materia di protezione dati e di accesso – le norme in materia di analisi delle posizioni di rischio fiscale e l'utilizzo sempre maggiore delle tecnologie digitali (anche supportate dall'intelligenza artificiale), al fine di ottenere, attraverso la piena interoperabilità tra le banche dati, la disponibilità delle informazioni necessarie per prevenire gli errori dei contribuenti e i conseguenti accertamenti.

2.2. I decreti-legge

La legge 13 novembre 2023, n. 159 ha convertito, con modificazioni, il d.l. 15 settembre 2023, n. 123, recante misure urgenti per il contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale.

Il testo contiene numerose norme di interesse tra le quali, in particolare, si segnalano le seguenti:

- l'art. 12 procede a un riordino della disciplina in materia di vigilanza sull'adempimento dell'obbligo di istruzione di cui all'art. 114, d.lgs. 16 aprile 1994, n. 297 (testo unico delle disposizioni legislative vigenti in materia di istruzione, relative alle scuole di ogni ordine e grado), ridefinendo i compiti del sindaco e del dirigente scolastico. In particolare si prevede che il sindaco, mediante accesso all'Anagrafe nazionale dell'istruzione (ANIST), possa individuare i minori non in regola con tale obbligo, provvedendo ad ammonire "senza ritardo" il responsabile" e invitandolo ad ottemperare (comma 2).

In tale ambito, nelle more dell'attivazione dell'ANIST, la disposizione prevede che i dirigenti scolastici possano trasmettere al sindaco i dati relativi ai suddetti minori

2

Disagio giovanile

2

Intercettazioni

demandando ad atti attuativi, sentito il Garante, l'indicazione delle procedure e tutele a tal fine necessari;

- l'art. 13 introduce disposizioni – sulla cui corretta applicazione vigilerà AGCOM – volte ad assicurare ai genitori la gratuita fruizione di applicazioni per il controllo parentale nei dispositivi di comunicazione elettronica. Il comma 6 dell'art. 13 prevede poi che i dati personali raccolti o generati durante l'attivazione delle applicazioni non possono essere utilizzati per scopi commerciali e di profilazione;

- l'art. 13-*bis* prescrive il generale divieto per i minori di accedere ai contenuti a carattere pornografico e impone ai gestori dei siti web, con il medesimo contenuto, l'obbligo di verificare la maggiore età degli utenti, attraverso modalità tecniche che saranno individuate dall'AGCOM, sentito il Garante;

- l'art. 15 designa l'AGCOM coordinatore dei servizi digitali ai sensi dall'art. 49, comma 2, reg. (UE) 2022/2065, prevedendo anche che l'AGCOM, il Garante e ogni altra autorità nazionale competente assicurino ogni necessaria collaborazione ai fini dell'esercizio delle relative funzioni. Si prevede altresì che le autorità possano disciplinare con protocolli di intesa gli aspetti applicativi e procedurali della reciproca collaborazione (art. 15, comma 2).

La legge 9 ottobre 2023, n. 137, reca la conversione, con modificazioni, del d.l. 10 agosto 2023, n. 105, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione.

Del provvedimento rilevano, in particolare, le disposizioni in materia di intercettazioni.

L'art. 1 estende l'ambito di applicazione della disciplina di cui all'art. 13, d.l. n. 152/1991, derogatoria rispetto alla normativa codicistica, ai procedimenti per i delitti, consumati o tentati, di attività organizzate per il traffico illecito di rifiuti e sequestro di persona a scopo di estorsione, ovvero commessi con finalità di terrorismo, o avvalendosi delle condizioni previste dall'art. 416-*bis* del c.p. o al fine di agevolare l'attività delle associazioni previste dallo stesso articolo. Per effetto di tale disposizione, anche per tali procedimenti le intercettazioni possono essere disposte quando necessarie (e non assolutamente indispensabili) per lo svolgimento delle indagini, in relazione a un delitto in ordine al quale sussistano sufficienti (invece che gravi) indizi di reità.

Tale disposizione reca inoltre ai suoi commi da 2-*bis* a 2-*quinqües* talune modifiche di rilievo al c.p.p., riguardanti in particolare:

- la modifica dell'art. 267 c.p.p., volta a precisare che il decreto autorizzatorio di intercettazioni ambientali mediante captatore informatico deve esporre con autonoma valutazione le specifiche ragioni che rendono necessarie in concreto, per lo svolgimento delle indagini, il ricorso a tale modalità (comma 2-*bis*);

- la modifica dell'art. 268 c.p.p., secondo cui nel verbale deve essere trascritto anche sommariamente soltanto il contenuto delle comunicazioni intercettate rilevanti, ai fini delle indagini, anche a favore della persona sottoposta a indagine. Il contenuto non rilevante ai fini dell'indagine non sarà invece trascritto, neppure sommariamente, e nessuna menzione ne verrà riportata nei verbali e nelle annotazioni della polizia giudiziaria, nei quali sarà apposta l'espressa dicitura "la conversazione omessa non è utile alle indagini" (comma 2-*ter*);

- l'ulteriore modifica del medesimo art. 268, concernente l'esclusione dai verbali di fatti e circostanze afferenti alla vita privata degli interlocutori, se non rilevanti (comma 2-*ter*);

- la modifica dell'art. 270 c.p.p., che limita la possibilità di utilizzo dei risultati delle intercettazioni, in procedimenti diversi da quelli nei quali sono state disposte, ammettendola nei soli casi in cui risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza (comma 2-*quater*).

L'art. 2 prevede l'istituzione di apposite infrastrutture digitali interdistrettuali, dirette a realizzare, per le attività d'intercettazione, più elevati ed uniformi livelli di sicurezza, un aggiornamento tecnologico adeguato, una maggiore efficienza, economicità e capacità di risparmio energetico dei sistemi informativi.

Il comma 4 stabilisce poi che i requisiti tecnici delle infrastrutture garantiscono l'autonomia delle funzioni del Procuratore della Repubblica di direzione, organizzazione e sorveglianza sulle attività di intercettazione e sui relativi dati, nonché sugli accessi e sulle operazioni compiute sui dati stessi. Fermi il segreto investigativo e le garanzie di riservatezza e sicurezza dei dati, viene ribadito che il Ministero della giustizia, pur nell'ambito delle suddette attività, non può avere accesso ai dati in chiaro.

Il comma 5 demanda a un decreto del Ministro della giustizia la disposizione dell'attivazione dell'archivio digitale di cui agli artt. 269, comma 1, c.p.p. e 89-bis delle disposizioni di attuazione del c.p.p.; quindi si autorizza al comma 6 la migrazione dei dati dalle singole procure e il conferimento dei nuovi dati.

Il comma 9 dispone che i decreti attuativi dell'art. 2 vengano adottati sentito il Consiglio superiore della magistratura, il Garante e il Comitato interministeriale per la cybersicurezza.

La legge 10 agosto 2023, n. 112, recante la conversione del d.l. 22 giugno 2023, n. 75, in materia di organizzazione delle pubbliche amministrazioni, di agricoltura, di sport, di lavoro e per l'organizzazione del Giubileo della Chiesa cattolica per l'anno 2025, istituisce al suo art. 21 la piattaforma "Famiglie e studenti".

Come previsto al suo comma 4-ter, il Ministero dell'istruzione e del merito promuove la progettazione, lo sviluppo e la realizzazione della suddetta piattaforma, quale canale unico di accesso al patrimonio informativo detenuto dal Ministero medesimo e dalle istituzioni scolastiche ed educative statali. Essa è costituita da un'infrastruttura tecnica che rende possibile l'interoperabilità dei sistemi informativi esistenti e funzionali alle attività del Ministero, al fine di semplificarne l'accesso e l'utilizzo. Il Ministero dell'istruzione e del merito e le istituzioni scolastiche ed educative utilizzano i dati presenti sulla piattaforma limitatamente – si precisa – ai trattamenti strettamente connessi agli scopi di quest'ultima e per il perseguimento delle rispettive finalità istituzionali.

Il comma 4-quater stabilisce invece che – al fine di semplificare l'erogazione delle prestazioni a favore delle famiglie e degli studenti, di ottimizzare le attività del Ministero e delle istituzioni scolastiche ed educative statali e di alimentare la piattaforma – il Ministero è autorizzato ad acquisire dall'INPS (previamente trasmessi al fine dell'individuazione degli studenti) i dati in forma aggregata e privi degli elementi identificativi, suddivisi per fasce, relativi all'Indicatore della situazione economica equivalente (ISEE) delle famiglie di cui fanno parte studenti iscritti presso le istituzioni suddette, al fine di ripartire le risorse tra queste ultime. Prevede altresì – sempre nel rispetto della normativa in materia di protezione dati – che le istituzioni scolastiche ed educative statali, in qualità di enti erogatori, per il tramite della piattaforma, effettuano altresì i controlli sul sistema informativo dell'ISEE relativi alla veridicità delle dichiarazioni sostitutive concernenti i dati delle famiglie che abbiano richiesto il riconoscimento del contributo.

Il comma 4-quinquies demanda infine la definizione dei servizi digitali inclusi nella piattaforma (comma 4-ter), degli standard tecnologici e dei criteri di sicurezza, accessibilità, di disponibilità e di interoperabilità, dei limiti e delle condizioni di accesso volti ad assicurare il corretto e lecito utilizzo dei dati a uno o più decreti, di natura non regolamentare, del Ministro dell'istruzione, sentito il Garante.

La legge 3 luglio 2023, n. 85 recante la conversione del d.l. 4 maggio 2023, n. 48, nell'ambito delle misure urgenti in materia di inclusione sociale e accesso al mondo del lavoro, ha introdotto, quale misura nazionale di contrasto alla povertà, l'assegno di inclusione: una integrazione al reddito in favore dei nuclei familiari che

2

Organizzazione
delle pubbliche
amministrazioni

Accesso al mondo del
lavoro

2

comprendano una persona con disabilità, un minorenni o un ultrasessantenne e che siano in possesso di determinati requisiti. La norma prevede che il beneficio mensile venga erogato dall'INPS attraverso uno strumento di pagamento elettronico, per un periodo massimo di 18 mesi continuativi, con la possibilità di un rinnovo per ulteriori 12 mesi (art. 1).

Tra le disposizioni di interesse si segnalano, oltre all'art. 2 che individua la platea dei beneficiari dell'assegno, anche il successivo art. 3 che delinea il percorso di attivazione della misura, attuato attraverso l'invio automatico, mediante piattaforma, dei dati del nucleo familiare al servizio sociale del comune di residenza ai fini dell'analisi, della presa in carico dei componenti con bisogni complessi e dell'attivazione degli eventuali sostegni.

L'art. 4 disciplina invece le modalità di richiesta dell'assegno. In particolare si prevede che la domanda venga presentata per via telematica all'INPS, che potrà riconoscere il beneficio previa verifica del possesso dei requisiti, sulla base delle informazioni disponibili sulle proprie banche dati o tramite quelle messe a disposizione dai comuni, dal Ministero dell'interno attraverso l'Anagrafe nazionale della popolazione residente, dai Ministeri della giustizia, dell'istruzione e del merito, dall'Anagrafe tributaria, dal PRA e dalle altre p.a. detentrici dei dati necessari per la verifica dei requisiti, attraverso sistemi di interoperabilità.

Il medesimo articolo prevede al suo primo comma che l'INPS informi il richiedente del fatto che, per ricevere il beneficio economico, dovrà effettuare l'iscrizione presso il Sistema informativo per l'inclusione sociale e lavorativa (SIISL), che gli permetterà di sottoscrivere un patto di attivazione digitale e che dovrà espressamente autorizzare la trasmissione dei dati relativi alla domanda ai centri per l'impiego, alle agenzie per il lavoro e agli enti autorizzati all'attività di intermediazione.

Il comma 3 specifica che, tramite la piattaforma, il percorso di attivazione viene attuato attraverso l'invio automatico dei dati del nucleo familiare al servizio sociale del comune di residenza ai fini dell'analisi, della presa in carico dei componenti con bisogni complessi e dell'attivazione degli eventuali sostegni.

Il comma 7 del presente articolo prevede, infine, che tutta la procedura di richiesta della misura venga definita con uno o più decreti del Ministro del lavoro e delle politiche sociali, sentiti il Garante e l'Agenzia nazionale per le politiche attive del lavoro.

L'art. 5 prevede l'istituzione, presso il Ministero del lavoro e delle politiche sociali, del SIISL, realizzato dall'INPS al fine di consentire l'attivazione dei percorsi personalizzati per i beneficiari, nonché per finalità di analisi, monitoraggio, valutazione e controllo dell'assegno. Tale sistema informativo consentirà l'interoperabilità di tutte le piattaforme digitali dei soggetti accreditati al sistema sociale, secondo quanto previsto con uno o più decreti del Ministro del lavoro e delle politiche sociali, sentiti il Garante, l'INPS e l'ANPAL.

L'art. 7 disciplina invece i controlli ispettivi sull'assegno di inclusione, svolti dal personale ispettivo dell'Ispettorato nazionale del lavoro (INL) e dal Comando carabinieri per la tutela del lavoro, dal personale ispettivo dell'INPS, nonché dalla Guardia di finanza nell'ambito delle ordinarie funzioni di polizia economico-finanziaria.

La disposizione prevede al suo comma 2 che, al fine di consentire un efficace svolgimento dell'attività di vigilanza, il personale ispettivo dell'INL e della Guardia di finanza abbiano accesso a tutte le informazioni e le banche dati, sia in forma analitica che aggregata, trattate dall'INPS, già a disposizione del personale ispettivo dipendente dal medesimo Istituto e, in ogni caso, alle informazioni e alle banche dati contenenti informazioni collegate ai requisiti e alle condizioni per accedere e conservare il beneficio. Il medesimo comma 2 prevede altresì che l'INPS e la Guardia di finanza, sentito il Garante, stipulino apposita convenzione, al fine del conseguimento delle predette finalità.

Il comma 3 demanda a un decreto del Ministro del lavoro e delle politiche sociali, sentito il Garante, l'individuazione delle categorie di dati, le modalità di accesso, le misure a tutela degli interessati e i tempi di conservazione dei suddetti dati.

L'art. 12 istituisce poi il supporto per la formazione e il lavoro consistente in un'indennità mensile riconosciuta in favore dei soggetti di età compresa tra 18 e 59 anni che partecipano a progetti di politiche attive del lavoro o a progetti utili alla collettività, anche in questo caso demandando ad apposito decreto del Ministro del lavoro e delle politiche sociali, sentiti il Garante e l'ANPAL, l'individuazione delle sue procedure e le misure per la sua attivazione.

Con l'art. 15, infine, in tema di vigilanza, viene richiesto agli enti pubblici e privati di condividere gratuitamente le informazioni di cui dispongono – individuate sentito il Garante, ai sensi dell'art. 2-ter, comma 1, del Codice – all'INL e alla Guardia di finanza, per meglio orientarne l'azione ispettiva, in particolare nei confronti delle imprese che evidenziano fattori di rischio in materia di salute e sicurezza sui luoghi di lavoro, lavoro irregolare o evasione od omissione contributiva.

2.3. I decreti legislativi

Tra i numerosi decreti legislativi adottati nel 2023 e rilevanti, in varia misura, in materia di protezione dei dati personali, si segnalano, in particolare, i seguenti:

Il decreto legislativo 26 luglio 2023, n. 106, reca l'attuazione della delega di cui all'art. 2 della l. 5 agosto 2022, n. 118, per la mappatura e la trasparenza dei regimi concessori di beni pubblici.

Il decreto, sul cui schema il Garante ha reso parere favorevole il 10 novembre 2022 istituisce, presso il MEF, il sistema informativo di rilevazione delle concessioni di beni pubblici, al fine di promuovere la massima pubblicità e trasparenza dei principali dati e delle informazioni relative a tutti i rapporti concessori, tenendo conto delle esigenze di sicurezza.

Tale sistema informativo è alimentato dalle informazioni, relative alla concessione di beni pubblici, detenute dalle amministrazioni pubbliche aventi la proprietà o la gestione del bene (che deve appartenere al demanio o al patrimonio indisponibile dello Stato). Tra le informazioni minime con le quali è alimentato il sistema figurano anche quelle relative alle generalità del concessionario.

Tra gli obblighi di pubblicità previsti in ottemperanza del criterio di delega, si include la pubblicazione dei dati comunicati e rilevati dalle amministrazioni su apposita sezione dedicata del sito web del MEF, anche in forma aggregata e nel rispetto della normativa di protezione dati, salvo si tratti di beni destinati alla difesa nazionale o siano rappresentate motivate esigenze di tutela della sicurezza pubblica e dell'ordine pubblico da parte dell'amministrazione competente.

Il decreto legislativo 10 marzo 2023, n. 24 reca l'attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, relativa alla protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Il decreto, sul cui schema il Garante ha reso parere l'11 gennaio 2023, (cfr. par. 3.1.2) è stato adottato nell'esercizio della delega legislativa conferita, al Governo, dall'art. 13 della l. 4 agosto 2022, n. 127 (legge di delegazione europea 2021) che, tra i principi e criteri direttivi, prevede l'esigenza di operare gli opportuni adattamenti delle disposizioni vigenti al fine di conformare la normativa nazionale a quella europea, anche in relazione a violazioni di diritto interno riconducibili a reati o comportamenti impropri che compromettono la cura imparziale dell'interesse pubblico o la regolare organizzazione e gestione dell'ente.

2

Mappatura e
trasparenza dei regimi
concessori

Whistleblowing

2

L'ambito oggettivo di applicazione è esteso, dall'art. 1, anche alle segnalazioni relative a violazioni del diritto interno, in virtù della facoltà prevista dall'art. 2, par. 2, della direttiva.

Per converso, lo stesso art. 1 disciplina i casi di esclusione dell'applicazione della nuova disciplina tra i quali si annoverano, in particolare, contestazioni o rivendicazioni di carattere personale nei rapporti individuali di lavoro o di impiego pubblico e le segnalazioni di violazioni in materia di sicurezza nazionale o di appalti relativi ad aspetti di difesa o sicurezza nazionale, salvo che tali aspetti siano riconducibili al diritto derivato unionale.

L'art. 3, identifica l'ambito soggettivo di applicazione della disciplina, individuando quali soggetti interessati dalla tutela per la segnalazione degli illeciti, suscettibili di eventuali atti ritorsivi, tutti i lavoratori dei settori pubblico e privato in qualità di dipendenti o collaboratori, lavoratori subordinati e autonomi, liberi professionisti ed altre categorie, tra le quali quelle dei volontari e dei tirocinanti anche non retribuiti, degli azionisti e delle persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche laddove tali ruoli siano esercitati in via di mero fatto.

Gli artt. 4 e 5, che introducono il Capo II (segnalazioni interne, segnalazioni esterne, obbligo di riservatezza e divulgazioni pubbliche), disciplinano rispettivamente le modalità di presentazione delle segnalazioni interne, volte a garantire la riservatezza dell'identità del segnalante e l'iter procedurale successivo alla segnalazione.

Gli artt. 7 e 8, disciplinano le caratteristiche del canale di segnalazione esterna attivato presso ANAC per quanto concerne sia il settore pubblico sia quello privato, con obbligo di garanzia (anche mediante il ricorso alla crittografia) della riservatezza del segnalante, delle persone coinvolte e menzionate nella segnalazione, nonché del contenuto della stessa. Anche in tali casi, le segnalazioni sono effettuate tramite piattaforma informatica messa a disposizione da ANAC, oppure in forma scritta od orale (attraverso linee telefoniche e altri sistemi di messaggistica vocale), nonché, qualora la persona lo richieda, anche attraverso un incontro diretto.

L'art. 8 sancisce, in capo ad ANAC, oltre all'obbligo di fornire riscontro al segnalante, anche quello di trasmissione delle segnalazioni relative a violazioni esulanti dalle proprie attribuzioni alle competenti autorità, amministrative o giurisdizionali – ivi compresi gli enti dell'Unione europea – le quali sono parimenti tenute, nell'attività successiva, a garantire la riservatezza degli interessati.

L'art. 9, disciplina le informazioni sulle segnalazioni esterne e sul relativo seguito, sancendo in capo ad ANAC l'obbligo di illustrazione del regime di riservatezza applicabile alle segnalazioni.

L'art. 10, demanda ad ANAC l'adozione – previo parere del Garante – di linee guida relative alle procedure di presentazione e gestione delle segnalazioni esterne, che promuovano anche il ricorso a strumenti di crittografia per garantire la riservatezza degli interessati e il contenuto delle segnalazioni.

L'art. 12, sotto la rubrica "Obbligo di riservatezza", sancisce il principio generale secondo cui le segnalazioni non possano essere utilizzate se non per darvi seguito, con espresso divieto di rivelazione – a persone diverse da quelle specificamente autorizzate anche ai sensi degli artt. 29 e 32, par. 4, del RGPD e 2-*quaterdecies* del Codice – dell'identità del segnalante, in assenza del suo consenso espresso.

L'art. 13, disciplina il trattamento dei dati personali, indicandone i ruoli soggettivi e precisando che i diritti sanciti dagli artt. da 15 a 22 del RGPD possono essere esercitati nei limiti di cui all'art. 2-*undecies* del Codice.

L'art. 14, consente la conservazione delle segnalazioni interne ed esterne e della relativa documentazione, per il tempo necessario alla loro definizione e, comunque, per non più di cinque anni a decorrere dalla data della comunicazione dell'esito

finale della procedura di segnalazione. L'articolo reca un'ulteriore precisazione sulle modalità di documentazione della segnalazione, in ragione della sua effettuazione con l'utilizzo di linee telefoniche o altro sistema di messaggistica vocale registrata o meno o, ancora, nel corso di un incontro diretto.

2

3 I rapporti con il Parlamento e le altre istituzioni

3.1. *L'attività consultiva del Garante*

La previsione del parere obbligatorio dell'Autorità sugli atti normativi anche di rango primario con profili di interesse in materia di protezione dei dati personali ha determinato un notevole incremento, di tipo qualitativo oltre che quantitativo, nell'attività consultiva del Garante (artt. 36, par. 4, e 57, par. 1, lett. c), cons. 96, RGPD art. 28, par. 2, dir. UE 2016/680; art. 24, comma 2, d.lgs. n. 51/2018).

Attraverso tale potenziata consultazione del Garante si è realizzata, in linea generale, l'individuazione di un più corretto bilanciamento tra diritti (spesso in opposizione) in rapporto alle sempre più numerose norme che prevedono trattamenti di dati personali.

3.1.1. *La consultazione del Garante nell'ambito del procedimento legislativo o dell'esercizio delle funzioni conoscitive, di indirizzo e controllo delle Camere*

Numerosi sono stati i casi di consultazione del Garante su atti normativi primari, anche in sede di conversione di decreti-legge, soprattutto in relazione alle misure adottate per contrastare l'attuale situazione di crisi internazionale, economica ed energetica. Sempre più frequente è il ricorso in questo ambito allo strumento, particolarmente duttile, dell'audizione parlamentare, che offre anche la possibilità di un dialogo diretto, mediante il dibattito successivo alla relazione, tra i singoli parlamentari e il Garante.

Tra le audizioni (o, comunque, le richieste di contributi) del Garante nell'ambito del procedimento legislativo si segnalano, in particolare, per il periodo di riferimento, le seguenti:

a) audizione dinanzi alla 9^a Commissione del Senato nell'ambito dell'esame del decreto legislativo recante attuazione della dir. (UE) 2019/2161 che modifica la dir. 93/13/CEE e le dir. 98/6/CE, 2005/29/CE e 2011/83/UE per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori - 12 gennaio 2023 (doc. web n. 9843160);

b) audizione dinanzi alla 9^a Commissione del Senato nell'ambito dell'esame del disegno di legge AS 795, recante legge annuale per il mercato e la concorrenza 2022 - 5 settembre 2023 (doc. web n. 9921332);

c) audizione dinanzi alla 2^a Commissione del Senato nell'ambito del disegno di legge n. 808, recante modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare - 6 settembre 2023 (doc. web n. 9926529);

d) memoria presentata alla X Commissione della Camera dei deputati nell'ambito dell'esame, in seconda lettura, del disegno di legge AC 1555, recante la legge annuale per il mercato e la concorrenza 2022 - 29 novembre 2023 (doc. web n. 9997290).

Sono inoltre pervenute richieste di contributi nell'ambito dell'esercizio delle funzioni conoscitiva, di indirizzo e controllo delle Camere, a dimostrazione di una diffusa sensibilità rispetto alla protezione dei dati personali e alle sue istanze.

Tra le audizioni o i contributi resi nell'anno si segnalano, in particolare, i seguenti:

a) audizione dinanzi alla 2^a Commissione del Senato, nell'ambito dell'indagine conoscitiva sul tema delle intercettazioni - 24 gennaio 2023 (doc. web n. 9855910);

b) audizione dinanzi alla VII Commissione della Camera dei deputati, nell'ambito dell'esame della risoluzione n. 7-00055, recante iniziative per contrastare la

diffusione delle sfide di resistenza (*challenge*) nelle reti sociali telematiche - 26 aprile 2023 (doc. web n. 9880951);

c) audizione dinanzi alla 2^a Commissione del Senato nell'ambito dell'indagine conoscitiva sul tema della diffamazione anche in relazione ai nuovi strumenti tecnologici di comunicazione - 18 luglio 2023 (doc. web n. 9911932).

3.1.2. *La consultazione del Garante su atti normativi statali di rango primario: i pareri al Governo su progetti di legge e schemi di decreto legislativo*

Significativi contributi sono stati offerti dal Garante rispetto alle iniziative legislative ovvero agli atti con forza di legge, di matrice governativa, incidenti sulla materia.

Tra i pareri principali resi in questo contesto si segnalano, in particolare, i seguenti:

a) parere 11 gennaio 2023, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo di attuazione della dir. (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (doc. web n. 9844945);

b) parere 3 agosto 2023 sul disegno di legge, d'iniziativa governativa, AS 808 recante modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare (doc. web n. 9927390);

c) parere 31 agosto 2023, reso alla Presidenza del Consiglio dei ministri sullo schema di decreto legislativo recante semplificazione dei controlli sulle attività economiche in attuazione della delega al Governo di cui all'art. 27, comma 1, l. 5 agosto 2022, n. 118 (doc. web n. 9929069);

d) parere 21 dicembre 2023, reso alla Presidenza del Consiglio dei ministri su uno schema di decreto legislativo che reca disposizioni integrative e correttive del d.lgs. 10 ottobre 2022, n. 150, di attuazione della l. 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari (doc. web n. 9974918).

In tale parere, il Garante ha espresso una raccomandazione relativa al regime di pubblicità degli atti procedimentali soggetti a videoregistrazione. La "riforma Carabia", allo scopo di garantire una rappresentazione più accurata degli atti in questione, ha, infatti, ampliato notevolmente il ricorso alla riproduzione audiovisiva e fonografica: segnatamente, come modalità generale di documentazione, destinata ad affiancare il verbale per gli atti del procedimento (art. 134 c.p.p.) nonché come modalità preferenziale di documentazione dell'interrogatorio di garanzia dell'indagato *in vinculis* (art. 141-bis c.p.p.) e quale forma di documentazione dell'assunzione dibattimentale dei mezzi di prova (art. 510, comma 2-bis, c.p.p.). In relazione a tale innovazione – in ragione del suo impatto sul trattamento dei dati personali delle parti e dei terzi coinvolti, a vario titolo, nel procedimento – il Garante ha suggerito l'introduzione di un regime speciale di pubblicità degli atti procedimentali così documentati, tale da bilanciare le esigenze di pubblicità, espressione del principio di cui all'art. 101, comma 1, Cost., il diritto alla riservatezza e il principio di minimizzazione di cui all'art. 5, par. 1, lett. c), del RGPD.

3.1.3. *I pareri sugli atti regolamentari o amministrativi in generale*

Nell'esercizio della funzione consultiva rispetto a norme regolamentari (o atti amministrativi generali) suscettibili di incidere sulla protezione dei dati personali, il Garante ha reso numerosi pareri.

Nel periodo considerato, in particolare, è stato reso parere sui seguenti atti:

a) schema di decreto concernente il regolamento relativo alla disciplina del trattamento dei dati personali da parte dei centri per la giustizia riparativa, ai sensi

3

3

dell'art. 65, comma 3, d.lgs. 10 ottobre 2022, n. 150, di attuazione della l. 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari (parere 17 maggio 2023, n. 215, doc. web n. 9899898);

b) schema di decreto, concernente il regolamento relativo al funzionamento della banca dati relativa alle aste giudiziarie, ai sensi dell'art. 26, comma 6, d.lgs. 10 ottobre 2022, n. 149 (parere 17 maggio 2023, n. 216, doc. web n. 9897618);

c) schema di decreto recante il regolamento relativo all'individuazione di ulteriori categorie dell'albo dei consulenti tecnici di ufficio e dei settori di specializzazione di ciascuna categoria, ai requisiti per l'iscrizione all'albo e alla formazione, tenuta e aggiornamento dell'elenco nazionale di cui all'art. 24-*bis* delle disposizioni per l'attuazione del c.p.c. e disposizioni transitorie, ai sensi dell'art. 13, comma 4, delle medesime disposizioni per l'attuazione, come aggiunto dall'art. 4, comma 2, lett. a), d.lgs. 10 ottobre 2022, n. 149 (parere 17 maggio 2023, n. 217, doc. web n. 9897647);

d) schema di regolamento concernente le modalità di costituzione e funzionamento delle commissioni di conciliazione per la risoluzione bonaria delle controversie di cui all'art. 17, comma 4, l. n. 46/2022 (parere 8 giugno 2023, n. 239, doc. web n. 9913578);

e) schema di decreto del Ministro delle imprese e del *made in Italy* in attuazione dell'art. 4, comma 6, d.lgs. 25 novembre 2016, n. 219, recante definizione dei termini e delle modalità operative di alimentazione del fascicolo informatico d'impresa, di cui all'art. 43-*bis*, comma 1, lett. b), d.P.R. 28 dicembre 2000, n. 445, e all'art. 2, comma 2, lett. b), l. 29 dicembre 1993, n. 580, nonché delle modalità e dei limiti di accesso alle relative informazioni da parte dei soggetti pubblici e privati interessati (parere 22 giugno 2023, n. 282, doc. web n. 9919882);

f) schema di regolamento recante la determinazione dei criteri e delle modalità di iscrizione e tenuta del registro degli organismi di mediazione e dell'elenco degli enti di formazione, l'approvazione delle indennità spettanti agli organismi, ai sensi dell'art. 16 del d.lgs. 4 marzo 2010, n. 28 e recante l'istituzione dell'elenco degli organismi ADR deputati a gestire le controversie nazionali e transfrontaliere, nonché il procedimento per l'iscrizione degli organismi ADR ai sensi dell'art. 141-*decies*, d.lgs. 6 settembre 2005, n. 206 recante codice del consumo, a norma dell'art. 7, l. 29 luglio 2003, n. 229 (parere 6 luglio 2023, n. 305, doc. web n. 9920527);

g) schema di decreto interministeriale, presentato dal Ministro delle imprese e del *made in Italy*, recante la disciplina dell'attività professionale del mediatore familiare, previsto dall'art. 4, d.lgs. 10 ottobre 2022 n. 149 (parere 18 luglio 2023, n. 331, doc. web n. 9920162);

h) schema di regolamento del Ministro della cultura, di concerto con il Ministro dell'economia e delle finanze, recante criteri e modalità di attribuzione e di utilizzo della Carta della cultura giovani e della Carta del merito, di cui all'art. 1, commi 357 e seguenti della l. 30 dicembre 2021, n. 234 e successive modificazioni e corredato schema di decreto del Segretario generale, recante disciplina delle modalità e dei tempi della gestione e della conservazione dei dati personali (parere 31 agosto 2023, n. 386, doc. web n. 9929134);

i) schema di decreto di modifica del decreto del Ministro delle infrastrutture e dei trasporti 29 luglio 2008, n. 146, recante regolamento di attuazione dell'art. 65, decreto 18 luglio 2005, n. 171, recante il codice della nautica da diporto (parere 14 settembre 2023, n. 417, doc. web n. 9938721);

j) schema di regolamento del Ministero delle infrastrutture e dei trasporti recante la disciplina dei centri di istruzione per la nautica (parere 28 settembre 2023, n. 458, doc. web n. 9946342);

k) schema di decreto del Ministro della giustizia relativo alle infrastrutture digitali

per le intercettazioni (parere 28 settembre 2023, n. 460, doc. web n. 9942101);

l) schema di decreto del Ministero delle infrastrutture e dei trasporti recante determinazione degli strumenti e delle procedure per effettuare l'accertamento dello stato di ebbrezza in conseguenza dell'uso di bevande alcoliche dei conduttori delle unità da diporto, ai sensi dell'art. 53-*bis*, comma 7, d.lgs. 18 luglio 2005, n. 171, recante il codice della nautica da diporto (parere 30 novembre 2023, n. 596, doc. web n. 9970897);

m) schema di decreto del Ministro della giustizia recante il regolamento da adottarsi ai sensi dell'art. 87, commi 1 e 3, d.lgs. 10 ottobre 2022, n. 150 e in attuazione delle disposizioni in materia di giustizia digitale nel processo civile introdotte dal d.lgs. 10 ottobre 2022, n. 149 e dall'art. 36, d.l. 24 febbraio 2023, n. 13, convertito, con modificazioni, dalla l. 21 aprile 2023, n. 41 (parere 30 novembre 2023, n. 554, doc. web n. 9973320);

n) schema di regolamento recante definizione delle disposizioni transitorie al processo penale militare telematico ai sensi dell'art. 87, comma 7, d.lgs. 10 ottobre 2022, n. 150 (parere 7 dicembre 2023, n. 593, doc. web n. 9976701);

o) schema di decreto del Ministro della giustizia ai sensi dell'art. 2, comma 3, d.l. 10 agosto 2023, n. 105, convertito con modificazioni dalla l. 9 ottobre 2023 n. 137, recante i requisiti tecnici specifici per la gestione dei dati presso le infrastrutture digitali interdistrettuali (parere 28 dicembre 2023, n. 637, doc. web n. 9978591).

I pareri di cui alle lett. m) ed n) hanno riguardato recenti riforme processuali che hanno introdotto norme “di cornice” e rinviato, per l'attuazione, nel dettaglio, alle specifiche tecniche rispetto alle quali è previsto il parere del Garante. Non sono state rilevate particolari criticità sui testi esaminati, essendosi suggeriti solo rilievi sia sotto il profilo del *drafting* (sostituzione dell'espressione “dati sensibili” con “dati di cui all'art. 9 del RGPD”, come per il processo ordinario), sia in relazione ai parametri normativi di conformità del processo militare (ovvero il richiamo alla disciplina di protezione dati nell'ambito delle norme di riferimento e al regolamento eIDAS per l'identificazione informatica, nonché alle disposizioni sui *data breach* nell'ambito della disciplina sul malfunzionamento del sito).

3.1.4. La consultazione del Garante sugli atti normativi regionali o di province autonome

Al Garante è stato richiesto di esprimere il proprio parere su alcuni progetti di legge o schemi di regolamento di regioni o province autonome.

Si segnalano, in tal senso, i seguenti:

1) parere sul disegno di legge della Provincia autonoma di Trento concernente interventi a sostegno del sistema economico trentino (parere 9 febbraio 2023, n. 46, doc. web n. 9868127);

2) parere sullo schema di regolamento della Provincia autonoma di Trento concernente il funzionamento del registro anomalie congenite, in attuazione dell'art. 14, comma 5-*bis*, legge provinciale 23 luglio 2010 n. 16 (legge provinciale sulla tutela della salute) (parere 6 luglio 2023, n. 307, doc. web n. 9920921);

3) parere sulla proposta di legge della Regione autonoma Friuli Venezia Giulia e relativo regolamento attuativo, tesi a disciplinare le modalità del trattamento dei dati personali per lo svolgimento delle attività di spettanza nell'ambito dei compiti attribuiti al Punto unico regionale (PUR) (parere 31 agosto 2023, n. 361, doc. web n. 9928773);

4) parere sullo schema di regolamento della Provincia autonoma di Trento recante regole sulla protezione dei dati personali in attuazione dell'art. 29 della legge provinciale sugli interventi a favore dell'economia (parere 12 ottobre 2023, n. 470, doc. web n. 9997275);

3

3

5) parere sullo schema di regolamento di attuazione dell'art. 40, comma 11-*bis*, legge provinciale 27 dicembre 2010, n. 27, concernente il trattamento dei dati personali appartenenti a particolari categorie *ex art.* 9 del RGPD nello svolgimento delle funzioni catastali delegate dallo Stato alla Provincia autonoma di Trento in materia di catasto terreni e catasto urbano (parere 16 novembre 2023, n. 595, doc. web n. 9974277).

3.1.5. Segnalazioni

Nel 2023 sono state presentate due segnalazioni al Governo, volte a sollecitare l'adozione di tre provvedimenti (due d.m. per il Ministro della giustizia e uno per il Ministro dell'interno), tutti, per ragioni diverse, di notevole rilevanza ai fini della completa definizione del quadro normativo in materia di protezione dati.

Si tratta, in particolare del d.m. giustizia, avente natura regolamentare, volto a disciplinare il trattamento di dati giudiziari da parte di soggetti privati, nei casi non previsti già da norme legislative o regolamentari; del d.m. giustizia che dovrà effettuare la ricognizione, anche per categoria, dei trattamenti di dati personali svolti nel settore della giustizia penale, delle loro caratteristiche essenziali e delle modalità di esercizio dei diritti degli interessati, ai sensi dell'art. 5, d.lgs. n. 51/2018; del d.m. interno che, specularmente a quello di cui sopra, dovrà effettuare la ricognizione, anche per categoria, dei trattamenti di dati personali svolti nell'ambito dell'attività di polizia, delle loro caratteristiche essenziali e delle modalità di esercizio dei diritti degli interessati, ai sensi dell'art. 5, d.lgs. n. 51/2018.

3.1.6. Quesiti

Nell'anno di riferimento l'Autorità ha fornito riscontro a un quesito sottoposto da una società di noleggio con conducente, relativa all'applicazione della disciplina del contenuto del foglio di servizio di noleggio con conducente di cui all'art. 11, comma 4, l. 15 gennaio 1992, n. 21. In tale circostanza si è ricordata la segnalazione al Governo del 16 maggio del 2019, nella quale si ravvisava la dubbia compatibilità con il principio di proporzionalità della previsione dell'obbligo di indicare, all'interno del foglio di servizio, i dati del fruitore del servizio stesso e del percorso effettuato (lett. e) e c) del citato comma 4).

Il Garante ha ricordato alla società che, in tale occasione, aveva sollecitato al Governo un intervento normativo, di natura correttiva – non ancora realizzatosi – rispetto alla previsione considerata, tale da emendarla degli evidenziati profili di criticità.

3.2. Consultazione attraverso la piattaforma IMI

Nell'anno di riferimento si è registrato un significativo incremento delle procedure di cooperazione in ambito europeo, attraverso le quali sono state affrontate tematiche di primario interesse in materia di protezione dei dati.

Sono stati, in particolare, forniti i riscontri richiesti in rapporto a sette procedure IMI di assistenza reciproca *ex art.* 61 del RGPD, su importanti tematiche quali: la ricognizione della normativa interna di disciplina del trattamento dei dati particolari da parte degli enti e delle associazioni sportive per finalità connesse alla valutazione delle prestazioni fisiche degli atleti; la ricognizione della normativa interna sul trattamento dei dati personali nell'ambito del rapporto di lavoro; lo stato di recepimento in Italia della direttiva NIS2; la designazione dell'autorità di controllo ai fini del *Data Governance Act* (DGA) – reg. (UE) 2022/868 del 30 maggio 2022.

3.3. *Il contributo al Governo ai fini del riscontro ad atti di sindacato ispettivo*

3

Anche nel 2023 il Garante ha fornito, a richiesta del Governo, elementi informativi ai fini della redazione della risposta da rendere ad atti di sindacato ispettivo con profili in materia di protezione dei dati personali.

Con particolare riferimento all'interrogazione a risposta immediata n. 5-01008, presentata dall'On. Mari, concernente l'utilizzo di sistemi decisionali automatizzati nel contesto lavoristico (20 giugno 2023), l'Autorità ha fornito osservazioni con riferimento ai criteri di legittimità da rispettare nel monitoraggio dei lavoratori in *smart working* attraverso *software* che controllano i registri di attività per verificare la quantità di lavoro svolta dal dipendente.

Il Garante, in tale sede, ha ricordato le disposizioni che sin dalla l. n. 300/1970 hanno inteso tutelare la riservatezza dei lavoratori rispetto a controlli datoriali suscettibili di raggiungere, anche grazie alla tecnologia, particolari livelli di invasività. In tale quadro ha, dunque, indicato le norme sul divieto di indagine sulle opinioni dei lavoratori (art. 8), sui limiti al controllo della loro attività (art. 4) e sulle sanzioni previste in caso di violazione di detti limiti (art. 171, d.lgs. n. 196/2003).

Il Garante ha altresì affermato che la stessa disciplina unionale di protezione dati riconosce, rispetto al contesto lavoristico, un margine di flessibilità per norme "interstiziali" di fonte interna (art. 88 del RGPD), in ragione delle peculiarità di tale settore normativo e del conseguente bilanciamento che ciò richiede tra protezione dei dati personali ed esigenze datoriali, con possibilità di diverse modulazioni in sede interna.

Tra le disposizioni interne in materia ha dunque indicato l'art. 4 del d.lgs. n. 104/2022, recante l'attuazione della dir. (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea. Esso, nel novellare il d.lgs. n. 152/1997 ha introdotto, in capo al datore di lavoro, uno specifico onere informativo (limitato dal recente d.l. n. 48/2023 ai casi di automatizzazione integrale) relativo all'utilizzo di sistemi decisionali o di monitoraggio, di tipo automatizzato "deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori".

Il Garante ha inoltre ricordato che tale onere informativo (ulteriore e più specifico rispetto a quello di cui all'art. 13 del RGPD in ordine al trattamento di dati personali) fa salvo il disposto dall'art. 4 della l. n. 300/1970, secondo cui, appunto, gli strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali ovvero su autorizzazione amministrativa. In tale quadro normativo ha infine ricordato che per verificare la conformità degli strumenti utilizzati per lo svolgimento della prestazione lavorativa alle disposizioni del RGPD sarà necessario effettuare un'analisi dei rischi e una valutazione d'impatto degli stessi trattamenti, procedendo a consultazione preventiva del Garante.

3.4. *L'esame delle leggi regionali al vaglio di costituzionalità del Governo*

Nell'anno di riferimento si segnala, inoltre, la ripresa dell'attività di esame del Garante sulle leggi regionali, al fine di fornire alla Presidenza del Consiglio dei ministri eventuali elementi di valutazione circa la loro compatibilità con le disposizioni in materia di protezione dei dati personali, ai fini di cui all'art. 127 della Costituzione.

3

In particolare, l’Autorità ha esaminato, trasmettendo alla Presidenza del Consiglio le relative valutazioni e osservazioni, la legge della Regione Puglia n. 13/2023, recante disposizioni per prevenire e contrastare condotte di maltrattamento o di abuso, anche di natura psicologica, in danno di anziani e persone con disabilità e modifica alla legge regionale 9 agosto 2006, n. 26.

Con nota 11 luglio 2023, l’Autorità ha segnalato alla Presidenza del Consiglio, profili di dubbia compatibilità della legge con la disciplina di protezione dei dati personali (d.lgs. nn. 196/2003 e 51/2018), in relazione alla potestà legislativa esclusiva dello Stato nella materia dell’ordinamento civile (cui la Corte costituzionale, con sent. n. 271/2005, ha ricondotto la normativa di protezione dati), nonché ai “vincoli derivanti dall’ordinamento comunitario” in riferimento alle disposizioni del RGPD (cfr. art. 117, commi primo e secondo, lett. l), Cost., nonché Corte costituzionale, sent. n. 271/2005).

La nota, in particolare, evidenziava che nel normare un’attività, quale quella della videosorveglianza nelle strutture residenziali, di notevole incidenza sulle garanzie di riservatezza (tanto degli ospiti quanto dei lavoratori coinvolti) la legge sembrava intervenire al di là delle sue competenze, in un ambito riservato al legislatore statale, ex art. 117, commi primo e secondo, lett. l), della Costituzione.

L’Autorità, ha inoltre risposto con la nota 20 luglio 2023 alle eccezioni della Regione rispetto agli argomenti forniti, ribadendo quanto rilevato nella nota alla Presidenza del Consiglio anche riguardo al possibile disallineamento della legge regionale con i principi e la stessa disciplina di protezione dati.

La legge regionale è stata poi impugnata dalla Presidenza del Consiglio dei ministri (con decisione assunta nella riunione del 3 agosto del Consiglio dei ministri) per violazione del riparto di attribuzione sulla potestà legislativa rispetto ad alcune materie quali, appunto, la protezione dati (ex art. 117, commi 1 e 2, lett. i), Cost.) davanti alla Corte costituzionale, la quale con la recente sentenza 23 aprile 2024, n. 69 ha dichiarato l’illegittimità costituzionale dell’art. 3 della predetta legge reg. Puglia n. 13 del 2023 per contrasto con l’art. 117, primo comma, Cost., in relazione al RGPD e alla direttiva 2016/680/UE, e con l’art. 117, secondo comma, lett. l), Cost., con riguardo alla materia “ordinamento civile”.



GPDP

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

L'attività svolta dal Garante

**RELAZIONE ANNUALE
2023**

PAGINA BIANCA

II - L'attività svolta dal Garante

4 Il Garante e le amministrazioni pubbliche

4.1. *L'attività fiscale, tributaria e in materia di antiriciclaggio*

4.1.1. *La dichiarazione dei redditi precompilata*

Anche nel 2023 il Garante è stato chiamato a pronunciarsi in merito alla cd. dichiarazione dei redditi precompilata, sia sulle modalità di accesso alla dichiarazione da parte degli interessati e dei soggetti autorizzati che sulle tipologie di dati da trasmettere all'Agenzia delle entrate.

È stato sottoposto all'Autorità lo schema di provvedimento del Direttore dell'Agenzia delle entrate, concernente l'accesso alla dichiarazione 730 precompilata da parte del contribuente e degli altri soggetti autorizzati, a partire dall'anno d'imposta 2022, nel quale è stato, in particolare, integrato l'elenco degli oneri detraibili/deducibili e i relativi rimborsi, trasmessi dai soggetti terzi, che sono utilizzati dall'Agenzia delle entrate per l'elaborazione della dichiarazione, con i dati trasmessi dagli istituti statali di alta formazione e specializzazione artistica e musicale riferiti alle spese per corsi statali successivi al conseguimento del diploma. In tale contesto, l'Agenzia delle entrate ha rappresentato di ritenere conclusa la fase di sperimentazione già avviata, sulla base dell'esito positivo delle attività di controllo richieste dall'Autorità sulla corretta gestione delle deleghe da parte dei CAF, e di voler, pertanto, permettere a tutti i CAF che lo ritengano di sottoscrivere la convenzione per accedere alla dichiarazione precompilata in cooperazione applicativa con cornice di sicurezza. Su tali basi, l'Autorità ha espresso parere favorevole, ritenuto che il complesso delle misure e garanzie previste nello schema risulta conforme alla normativa in materia di protezione dei dati personali e tiene in adeguata considerazione gli elevati rischi per i diritti e le libertà degli interessati che comportano i trattamenti in questione (provv. 13 aprile 2023, n. 116, doc. web n. 9888129).

Per quanto riguarda la raccolta dei dati a fini di elaborazione della dichiarazione dei redditi precompilata, in primo luogo il Garante si è espresso favorevolmente sullo schema di decreto del Ministro dell'economia e delle finanze che prevede la trasmissione telematica all'Agenzia delle entrate dei dati riguardanti le spese per l'acquisto degli abbonamenti ai servizi di trasporto pubblico locale, regionale e interregionale (provv. 23 febbraio 2023, n. 45, doc. web n. 9869626).

Conseguentemente, il Garante ha dato il proprio parere favorevole sullo schema di provvedimento del Direttore dell'Agenzia delle entrate che disciplina la trasmissione dei predetti dati, essendo state ritenute adeguate le misure volte ad assicurare la tutela dei diritti e delle libertà fondamentali dell'interessato quali, ad esempio, la garanzia dell'opposizione all'utilizzo dei dati (provv. 31 agosto 2023, n. 360, doc. web n. 9928753).

Parere favorevole è stato reso anche sullo schema di provvedimento del Direttore dell'Agenzia concernente modalità e termini di comunicazione all'Anagrafe tributaria dei dati relativi ai rimborsi erogati per l'acquisto di occhiali da vista ovvero di

**Accesso alla
dichiarazione 730
precompilata**

**Spese per abbonamenti
ai servizi di trasporto
pubblico**

Rimborsi *bonus* vista

4

Trasmissione al
Sistema TS dei dati
relativi a spese
sanitarie

Destinazione 8, 5 e 2
per mille dell'IRPEF

lenti a contatto correttive – nell'ambito del cd. *bonus* vista disciplinato dal decreto del Ministro della salute, di concerto con il Ministro dell'economia e delle finanze, 21 ottobre 2022 (su cui il Garante si era pronunciato con provv. 6 ottobre 2022, n. 319, doc. web n. 9817038) – tenendo conto che i trattamenti hanno a oggetto i dati personali necessari per il perseguimento delle finalità connesse alla presentazione e gestione della dichiarazione dei redditi precompilata, comprese quelle di controllo formale delle stesse, e che i flussi avvengono mediante la fornitura di un *file* cifrato, direttamente nell'ambito dei sistemi informativi di SOGEI S.p.A., responsabile del trattamento sia del Ministero della salute che dell'Agenzia delle entrate (provv. 26 ottobre 2023, n. 494, doc. web n. 9953525).

Pronunciamento positivo del Garante è stato reso sullo schema di decreto del Ministro dell'economia e delle finanze con il quale vengono disposte, per effetto di modifiche intervenute nelle rispettive discipline di settore, la trasmissione al Sistema tessera sanitaria (Sistema TS) dei dati relativi alle spese sanitarie da parte dei soggetti iscritti all'Albo degli infermieri pediatrici e l'individuazione della Federazione nazionale degli ordini della professione sanitaria di fisioterapista e della Federazione nazionale degli ordini dei biologi quali soggetti tenuti a rendere disponibili al Sistema TS gli elenchi degli iscritti agli Albi di riferimento (provv. 27 aprile 2023, n. 161, doc. web n. 9894458).

Contestualmente, il Garante ha reso parere favorevole sullo schema di decreto del MEF – Ragioniere generale dello Stato che provvede, di conseguenza, ad adeguare le specifiche tecniche e le modalità operative dei flussi di dati relativi alle spese sanitarie a fini di elaborazione della dichiarazione dei redditi precompilata, nell'ambito della trasmissione al Sistema TS, al fine di dare attuazione alle predette novità relative, in particolare, agli infermieri pediatrici (provv. 27 aprile 2023, n. 162, doc. web n. 9894499).

In tale contesto, il Garante ha altresì avallato lo schema di provvedimento del Direttore dell'Agenzia delle entrate che disciplina le modalità tecniche di utilizzo dei dati delle spese sanitarie sostenute per prestazioni erogate da parte degli iscritti agli Albi professionali degli infermieri pediatrici, rinviando alla disciplina contenuta nei pertinenti provvedimenti, già valutati favorevolmente dal Garante, in relazione alle misure e garanzie ivi disciplinate e ritenute adeguate a proteggere i diritti e le libertà degli interessati (provv. 22 giugno 2023, n. 258, doc. web n. 9913892).

Il Garante è stato consultato dall'Agenzia delle entrate sullo schema di provvedimento del Direttore concernente le modalità di trasmissione all'Agenzia medesima dei dati contenuti nella scheda riguardante le scelte per la destinazione dell'otto, del cinque e del due per mille dell'IRPEF da parte dei sostituti d'imposta che prestano assistenza fiscale. Nel rendere il parere, è stato preliminarmente osservato che la raccolta e trasmissione all'Agenzia delle entrate nonché la conservazione delle schede, da parte dei datori di lavoro (in qualità di sostituti d'imposta) e della medesima Agenzia, di particolari categorie di dati personali dei dipendenti relativi alle predette scelte, nel delicato contesto lavorativo e professionale, sono presidiate, oltre che dalle specifiche garanzie previste dalla normativa in materia di protezione dei dati personali, anche dal pertinente quadro normativo, che prevede tutele volte a prevenire effetti discriminatori, anche indiretti, nei confronti dei lavoratori. Ciò posto, il Garante ha rilevato che le misure individuate nello schema per la dematerializzazione delle modalità di presentazione delle predette schede non offrivano un analogo livello di tutela in ordine alla riservatezza delle scelte dei lavoratori interessati, rispetto a quello previsto per la previgente disciplina, poiché non risultavano sufficienti a impedire che il datore di lavoro ne conoscesse il contenuto. È stato pertanto rilasciato parere favorevole, a condizione dell'introduzione di misure quali la cifratura del documento informatico contenente le scelte operate dal lavoratore, direttamente da

parte del lavoratore prima di consegnare il documento al sostituto di imposta, mediante strumenti e chiavi crittografiche messi a disposizione dall’Agenzia, nonché la raccolta delle predette scelte da parte dell’Agenzia direttamente presso il lavoratore, o comunque tramite un canale diverso dal sostituto di imposta (prov. 23 marzo 2023, n. 79, doc. web n. 9879234).

Il MEF ha sottoposto alla consultazione del Garante due schemi di decreto volti a disciplinare le finalità e le modalità di utilizzo, da parte dell’Agenzia delle entrate, dei dati fiscali, le modalità e i termini di acquisizione dei dati, le misure di sicurezza per la tutela dei diritti e delle libertà degli interessati e l’utilizzo dei dati ai fini del monitoraggio della spesa sanitaria pubblica e privata complessiva, con riferimento ai dati contenuti nelle fatture elettroniche e nei corrispettivi relativi a prestazioni sanitarie trasmessi al Sistema TS (ai sensi, rispettivamente, dell’art. 10-*bis*, d.l. 23 ottobre 2018, n. 119, e dell’art. 2, comma 6-*quater*, d.lgs. 5 agosto 2015, n. 127). È stato al riguardo espresso parere favorevole in ragione dell’individuazione di misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato quali la limitazione dell’utilizzo a fini fiscali dei soli dati trasmessi al Sistema TS effettivamente indispensabili per il perseguimento, da parte dell’Agenzia delle entrate e della Guardia di finanza, delle finalità previste dalla legge, con l’esclusione dei dati relativi alla salute degli interessati (prov. 7 dicembre 2023, n. 581, doc. web n. 9974159).

4.1.2. Antiriciclaggio

L’Organismo agenti e mediatori (OAM) ha sottoposto all’Autorità lo schema delle Specifiche tecniche delle procedure di registrazione, accreditamento e consultazione riferite al registro dei soggetti convenzionati ed agenti di prestatori di servizi di pagamento ed istituti emittenti moneta elettronica, ai sensi dell’art. 45, d.lgs. 21 novembre 2007, n. 231 (cd. decreto antiriciclaggio) e, in sua attuazione, del decreto del Ministro dell’economia e delle finanze del 31 maggio 2022 (su cui il Garante si era pronunciato con prov. 24 febbraio 2022, n. 77, doc. web n. 9751958). È stato rilasciato parere favorevole considerato che lo schema, oltre a tenere conto di quanto già definito in passato con riferimento al registro degli operatori compro oro (cfr. il parere reso con prov. 26 luglio 2018, n. 447, doc. web n. 9025512), ha recepito, in quanto compatibili e adattandole allo specifico contesto, le osservazioni fornite in tema di operatori di valuta virtuale (prov. 21 dicembre 2022, n. 449, doc. web n. 9856315). Si segnala che tali indicazioni hanno riguardato, in particolare, l’individuazione delle tipologie di dati personali e documenti oggetto di trattamento sia nella fase di registrazione degli utenti che in quelle di accreditamento e di trasmissione, la delimitazione delle tipologie di dati personali oggetto di consultazione sia nella sezione ad accesso pubblico del registro che nella sezione ad accesso riservato, l’adozione di misure volte a informare adeguatamente soggetti convenzionati e agenti dei trattamenti dei propri dati personali (anche con riferimento a quelli che comportano l’accessibilità al pubblico degli stessi), l’introduzione di un meccanismo di informazione reciproca e tempestiva tra i titolari del trattamento coinvolti in caso di violazioni di sicurezza o altre minacce che comportino un rischio per la sicurezza e per i diritti e le libertà degli interessati (prov. 13 aprile 2023, n. 141, doc. web n. 9894521).

Sempre in materia di antiriciclaggio, è stato sottoposto al vaglio dell’Autorità, da parte di InfoCamere S.c.p.A., lo schema di *Addendum* al disciplinare tecnico sulla sicurezza del trattamento dei dati sulla titolarità effettiva, previsto dall’art. 11, comma 3, del regolamento di cui al decreto del Ministro dell’economia e delle finanze, di concerto con il Ministro dello sviluppo economico, 11 marzo 2022, n. 55, già adottato da InfoCamere previo parere del Garante (prov. 6 ottobre 2022, n. 316, doc. web n. 9817361). L’Autorità, in particolare, si era riservata di valutare le misure tecniche e

4

Fatture elettroniche e corrispettivi in ambito sanitario

Registro dei soggetti convenzionati e agenti prestatori di servizi di pagamento

Titolarità effettiva

4

organizzative concernenti l'accesso alle informazioni sulla titolarità effettiva. A questo riguardo, il Garante, dopo aver evidenziato l'intervenuta sentenza della CGUE del 22 novembre 2022, cause riunite C-37/20 e C-601/20 – che ha dichiarato invalida la norma della direttiva europea antiriciclaggio che consente agli Stati di prevedere l'accessibilità al pubblico delle informazioni sulla titolarità effettiva delle società e delle altre entità giuridiche – ha rilasciato parere favorevole anche in considerazione del fatto che lo schema di *Addendum*, a seguito delle indicazioni fornite dall'Autorità nel corso delle interlocuzioni, ha provveduto a coordinare le previsioni concernenti l'accesso alle informazioni sulla titolarità effettiva da parte dei cd. soggetti legittimati, limitandone l'ambito in maniera più chiara ai titolari di un interesse giuridico rilevante e differenziato, e così assicurando il rispetto di quanto stabilito nella pronuncia della Corte di giustizia (provv. 14 settembre 2023, n. 397, doc. web n. 9938499).

4.2. Previdenza, assistenza sociale e altri benefici economici

Il 2023 ha visto modifiche normative sul piano del riconoscimento delle misure di sostegno economico nei confronti di persone in difficoltà, con il passaggio dal reddito di cittadinanza (RDC) e dalla pensione di cittadinanza (PDC) (disciplinati dal d.l. n. 4/2019) all'assegno di inclusione (ADI) e al supporto per la formazione e il lavoro (SFL) (introdotti dal d.l. n. 48/2023).

In tema di reddito e pensione di cittadinanza, il Garante ha fornito parere favorevole sullo schema di modulo per la domanda del beneficio, che modifica quelli adottati dall'INPS nel 2019 e nel 2022 (previo parere del Garante) ai sensi dell'art. 5, comma 1, d.l. n. 4/2019, al fine di dare seguito alle modifiche intercorse alla normativa di settore le quali hanno definito il progressivo esaurimento dell'erogazione della misura, la cui cessazione è divenuta operativa a partire dal 1° gennaio 2024 (provv. 8 giugno 2023, n. 241, doc. web n. 9913623).

Al fine di dare attuazione alle nuove misure di sostegno dell'ADI e del SFL, introdotte dal d.l. n. 48/2023, il Ministero del lavoro e delle politiche sociali ha sottoposto alla consultazione dell'Autorità due schemi di decreto concernenti, rispettivamente, l'istituzione e il funzionamento del Sistema informativo per l'inclusione sociale e lavorativa (SIISL) e l'istituzione e la realizzazione del SFL. Nel proprio parere, il Garante ha preliminarmente osservato che il SIISL – istituito presso il Ministero del lavoro e delle politiche sociali e realizzato dall'INPS, attraverso il quale viene assicurata l'interoperabilità di tutte le piattaforme digitali dei soggetti accreditati al sistema sociale e del lavoro a fini di erogazione di ADI e SFL – viene realizzato anche attraverso il riuso di componenti già sviluppate nell'ambito del Sistema informativo del RDC di cui al d.l. n. 4/2019, nel cui ambito sono state assicurate garanzie vagliate dall'Autorità (provv. 20 giugno 2019, n. 138, doc. web n. 9122428). Anche per tale ragione, oltre che per il recepimento delle indicazioni fornite dall'Ufficio nel corso delle interlocuzioni – quali quelle concernenti l'individuazione dei soggetti coinvolti e dei ruoli assunti da ciascuno in relazione ai trattamenti di dati personali effettuati, le tipologie di dati personali oggetto di alimentazione del SIISL e le relative fonti, i compiti dei soggetti accreditati competenti per l'erogazione delle misure di politica attiva nell'ambito del SFL, le garanzie contenute nella disciplina sui trattamenti di dati personali anche automatizzati effettuati a fini di profilazione nell'ambito delle attività di formazione, qualificazione e riqualificazione professionale, orientamento e accompagnamento al lavoro (cfr. Programma di garanzia di occupabilità dei lavoratori (GOL), su cui il Garante si è pronunciato favorevolmente con provv. 20 ottobre 2022, n. 353, doc. web n. 9827428) – è stato reso un parere favorevole (provv. 3 agosto 2023, n. 354, doc. web n. 9918937).

Reddito e pensione di
cittadinanza

SIISL e SFL

Nel percorso di attuazione del d.l. n. 48/2023, il Ministero del lavoro e delle politiche sociali ha redatto la disciplina della specifica misura dell'ADI, richiedendo, sul relativo schema di decreto, il previsto parere al Garante. Nel proprio parere, il Garante ha riscontrato i miglioramenti apportati al testo anche a seguito dell'accoglimento delle indicazioni fornite dall'Ufficio concernenti in particolare: l'individuazione del ruolo ricoperto dagli istituti di patronato e dai CAF in relazione al trattamento dei dati personali effettuato nell'ambito della presentazione della richiesta dell'ADI; la definizione dei dati personali oggetto di trattamento da parte dell'INPS a fini di verifica dei requisiti e le relative modalità; il richiamo alle garanzie del Programma GOL in caso di profilazione nonché sulle verifiche periodiche; l'adozione da parte dell'INPS di idonee misure di trasparenza e informazione riguardo agli adempimenti e agli obblighi cui sono tenuti i beneficiari. In ogni caso, il parere reca un'osservazione in merito alla necessità che i trattamenti effettuati nell'ambito delle verifiche sul possesso dei requisiti, ove non già disciplinati da altri fonti normative, vengano avviati dopo aver individuato misure adeguate a tutela dei diritti e delle libertà fondamentali degli interessati, a valle della valutazione d'impatto sulla protezione dei dati, in un provvedimento dell'INPS da adottarsi sentito il Garante (prov. 12 dicembre 2023, n. 597, doc. web n. 10000877).

ADI

4.3. La protezione dei dati personali in ambito scolastico e universitario

Anche nel 2023 il Garante ha interagito con il Ministero dell'istruzione e del merito, le Università e le istituzioni scolastiche nel corso di incontri e contatti volti a fornire chiarimenti e indicazioni sulla corretta applicazione della disciplina in materia di protezione dei dati personali.

In tale ambito, particolare rilievo ha assunto il provvedimento 10 ottobre 2023, n. 468 (doc. web n. 9953443) con il quale il Garante ha espresso, in via d'urgenza, parere favorevole, sottoposto a condizione, ai sensi degli artt. 36, par. 4, e 58, par. 3, lett. b), del RGPD, nonché dell'art. 21, comma 4-*quinquies*, d.l. n. 75/2023, sullo schema di decreto del Ministro dell'istruzione e del merito concernente la disciplina sul trattamento dei dati personali nell'ambito della Piattaforma famiglie e studenti.

Lo schema stabilisce che la Piattaforma rappresenta un canale unico di accesso al patrimonio informativo detenuto dal Ministero e dalle istituzioni scolastiche, interoperabile con i relativi sistemi informativi, interconnessa con l'ANS nonché, allorquando diventerà operativa, con l'ANIST, con l'obiettivo di mettere a disposizione appositi servizi digitali al fine di garantire il sostegno del diritto allo studio e un effettivo supporto a studenti e studentesse nel percorso di crescita e nello sviluppo delle competenze, nonché di semplificare l'erogazione delle prestazioni a favore di famiglie e studenti e di ottimizzare il lavoro del Ministero e delle istituzioni. La Piattaforma è costituita da un'area pubblica e una privata, quest'ultima accessibile, previa procedura di identificazione e autenticazione informatica, a varie categorie di utenti (studenti della scuola secondaria di primo e di secondo grado, genitori/ esercenti la responsabilità genitoriale, docenti, *tutor*, dirigenti scolastici, personale ATA, ecc.). Attraverso di essa, è possibile accedere a servizi digitali, su base facoltativa, quali il cosiddetto *e-portfolio* (un servizio che consente di visualizzare i dati e le informazioni relative al percorso di istruzione di studenti e studentesse, al fine di supportarli nelle scelte formative e professionali), il docente *tutor* (un servizio volto ad agevolare lo svolgimento dei compiti assegnati al docente che ricopre il ruolo di docente *tutor*), gite scolastiche (un servizio volto a consentire la più ampia partecipazione di studenti e studentesse a viaggi d'istruzione e visite didattiche, mediante il riconoscimento di contributi economici o altre tipologie di benefici in favore delle famiglie maggiormente bisognose).

Piattaforma famiglie e studenti

4

Lo schema di decreto e il relativo allegato tecnico tengono conto delle osservazioni fornite dall'Ufficio ai rappresentanti del Ministero nel corso di confronti informali al fine di rendere i trattamenti conformi alla disciplina in materia di protezione dei dati personali, in ossequio al principio di *privacy by design e by default*. Tali osservazioni hanno riguardato, in particolare, l'individuazione dei soggetti coinvolti e dei ruoli assunti da ciascuno in relazione ai trattamenti di dati personali effettuati e alle finalità istituzionali perseguite; le modalità attraverso le quali il Ministero effettua l'aggregazione dei dati personali, in modo da ridurre il rischio di re-identificazione degli interessati, per proprie finalità di monitoraggio e governo generale della Piattaforma; con specifico riferimento al servizio digitale docente *tutor*, la facoltatività del conferimento di informazioni da parte degli utenti e la limitazione delle finalità in base alle quali è consentito l'accesso a tale servizio; con specifico riferimento al servizio digitale gite scolastiche, la descrizione dei trattamenti previsti e, in relazione a ciascuno di questi, l'individuazione di ruoli, delle tipologie di dati personali trattati e delle operazioni eseguite e la specificazione dei relativi obblighi informativi, nonché l'aggregazione delle informazioni oggetto di scambio tra Ministero e INPS; i tempi di conservazione delle diverse tipologie di dati personali trattati nell'ambito della Piattaforma; l'individuazione di misure tecniche e organizzative da adottare al fine di assicurare il rispetto dei principi del RGPD e degli obblighi di sicurezza (procedure di autenticazione informatica, categorie di persone autorizzate ad accedere alla Piattaforma per lo svolgimento delle finalità istituzionali perseguite dall'ente di appartenenza, modalità di scambio dati con l'INPS e altro).

Poiché nell'ambito dei dati personali conferiti direttamente dagli utenti nella Piattaforma possono rientrare anche quelli appartenenti alle categorie di cui agli artt. 9 e 10 del RGPD, l'Autorità ha espresso parere favorevole sullo schema di decreto a condizione che esso fosse integrato con l'indicazione dei tipi di dati che possono essere trattati, delle operazioni eseguibili e delle misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, come stabilito dall'art. 2-*sexies* del Codice, da individuarsi sulla base di un'adeguata valutazione dei rischi.

Il Garante ha espresso, inoltre, in via d'urgenza parere favorevole sullo schema di decreto del Ministro dell'istruzione e del merito avente ad oggetto criteri e modalità relativi alla sezione dell'Anagrafe nazionale dell'istruzione (ANIST) riguardante gli studenti iscritti ai percorsi degli ITS *Academy* per il monitoraggio quantitativo e qualitativo del Sistema terziario di istruzione tecnologica attraverso l'apposita banca dati nazionale, ai sensi degli artt. 12, commi 1 e 2, e 14, comma 6, l. n. 99/2022.

Anche in questo caso, lo schema di decreto tiene conto delle osservazioni dell'Ufficio fornite nel corso delle interlocuzioni informali e delle riunioni con i rappresentanti del Ministero, al fine di rendere conformi i trattamenti ivi disciplinati alla normativa in materia di protezione dei dati personali, nel rispetto dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita. Tali osservazioni hanno riguardato, in particolare, la specificazione delle finalità perseguite dalla Sezione ITS *Academy* dell'ANIST e l'individuazione dei soggetti autorizzati ad accedere ai dati personali contenuti nella medesima in attuazione dei compiti definiti dalla legge; l'individuazione dei ruoli assunti dagli ITS *Academy* e dal Ministero in relazione ai trattamenti di dati personali effettuati nell'ambito della sezione ITS *Academy* dell'ANIST; la definizione, in termini generali, delle tipologie di dati personali contenuti nella sezione ITS *Academy* dell'ANIST; l'utilizzo da parte del Ministero, ai fini del monitoraggio del Sistema terziario di istruzione tecnologica, delle informazioni relative agli esiti occupazionali degli studenti iscritti e dei diplomati esclusivamente in forma aggregata.

L'Autorità ha reso il proprio parere sul presupposto che, in ogni caso, la piena operatività della sezione ITS *Academy* dell'ANIST e l'avvio dei conseguenti trattamenti

ITS Academy

di dati avverranno solo a seguito della completa definizione del quadro giuridico di riferimento mediante l’emanazione di un successivo decreto attuativo, da sottoporre al parere del Garante e volto ad individuare ulteriori elementi di dettaglio del trattamento quali, in particolare, le specifiche tipologie di dati personali oggetto di trattamento e le rispettive fonti; le operazioni eseguibili sui dati e le relative modalità di trattamento, nonché le specifiche misure tecniche e organizzative per assicurare la tutela dei diritti e delle libertà degli interessati; le garanzie per assicurare il rilascio delle certificazioni anche relative ai titoli di studio da parte degli ITS *Academy*, cui è attribuita la funzione certificatoria dalla normativa di settore; i tempi di conservazione dei dati personali nell’ambito della nuova sezione; il raccordo tra quest’ultima e la banca dati nazionale di cui all’art. 13 del d.P.C.M. 25 gennaio 2008, comprese le caratteristiche dei trattamenti effettuati in tale contesto e le modalità di interazione tra le stesse (provv. 16 novembre 2023, n. 525, doc. web n. 9966592).

Anche nel corso del corrente anno sono stati definiti reclami e segnalazioni aventi ad oggetto la pubblicazione, su siti web di istituti scolastici, di dati personali degli alunni nonché riguardanti la comunicazione a terzi dei predetti dati, in assenza di una base giuridica idonea e in violazione dei principi applicabili al trattamento dei dati.

In tale ambito il Garante ha censurato il comportamento di una scuola che ha pubblicato, nella sezione amministrazione trasparente del sito web istituzionale, una nota del dirigente scolastico recante gli elenchi nominativi degli alunni ammessi alla frequenza del tempo pieno della scuola primaria presso uno dei plessi dell’istituto e l’indicazione della classe di assegnazione degli stessi. Al riguardo è stato ricordato che uno specifico trattamento di dati personali può essere lecitamente effettuato da parte di un soggetto pubblico solo ove sia necessario per l’adempimento di un obbligo legale da parte del titolare del trattamento o per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri; inoltre, il trattamento deve trovare il proprio fondamento in una disposizione che abbia le caratteristiche di cui all’art. 2-ter del Codice. L’Autorità ha inoltre ricordato che il Garante, in collaborazione con il Ministero dell’istruzione, è intervenuto rinviando a una specifica FAQ in merito alla pubblicazione, sul sito internet degli istituti scolastici, di elenchi nominativi relativi alla composizione delle classi (cfr. FAQ relative ai trattamenti dei dati personali nel contesto scolastico nel quadro dell’emergenza sanitaria, doc. web n. 9337010, e, in particolare FAQ n. 10). Con la predetta FAQ era stato chiarito che la diffusione dei dati relativi alla composizione delle classi sul sito web degli istituti scolastici non è consentita in quanto tale operazione di trattamento è lecita solo nei casi previsti dall’art. 2-ter del Codice.

Il Garante ha quindi stabilito che la pubblicazione sul sito web dell’istituto scolastico aveva determinato una diffusione illecita di dati personali, in violazione degli artt. 5 e 6 del RGPD, nonché dell’art. 2-ter del Codice, e ha provveduto ad ammonire l’istituto scolastico (provv. 13 aprile 2023, n. 185, doc. web n. 9902516; v. anche provv. 6 luglio 2023, n. 288, doc. web n. 9920274).

Similmente il Garante ha ammonito un istituto scolastico, anche a seguito di un reclamo concernente la contestata *e-mail* inviata da un insegnante a tutti i genitori degli alunni della classe e contenente informazioni relative al comportamento non corretto tenuto dal figlio dei reclamanti e da un altro alunno. Il Garante, dopo aver ricordato che “nelle circolari, nelle delibere o in altre comunicazioni non rivolte a specifici destinatari non possono essere inseriti dati personali che rendano identificabili gli alunni” (cfr. FAQ n. 7 *Scuola e Privacy* – domande più frequenti e *La scuola a prova di privacy - Vademecum* ed. 2023.pdf, v. la voce “Comunicazioni Scolastiche” a p. 28) ha ritenuto che l’invio, da parte dell’istituto scolastico, della comunicazione in esame aveva di fatto reso conoscibili informazioni riguardanti i suddetti alunni

4

**Trattamenti di dati
personali di alunni e
studenti**

4

anche da parte di soggetti terzi non legittimati (tutti i genitori della classe destinatari delle *e-mail* diversi dai genitori dei due ragazzi interessati), dando in tal modo luogo a una comunicazione di dati personali in violazione degli artt. 5 e 6 del RGPD e 2-ter e del Codice (provv. 28 settembre 2023 n. 421 doc. web n. 9946323).

Il Garante ha inoltre censurato con un ammonimento il comportamento di un istituto scolastico che, facendo seguito ad una richiesta di accesso alla documentazione amministrativa presentata all'istituto ai sensi della l. n. 241/1990, ha inviato ai soggetti controinteressati, individuati ai sensi dell'art. 3 del d.P.R. n. 184/2006, copia dell'istanza di accesso recante, oltre al nominativo della reclamante, anche ulteriori dati personali quali il numero di telefono e copia del documento di identità dell'interessata. Al riguardo, l'Autorità ha chiarito che la contestazione mossa riguardava non tanto la comunicazione dell'identità del reclamante ai soggetti controinteressati nel procedimento di accesso agli atti – condotta non censurabile ai sensi della disciplina in materia di accesso ai documenti amministrativi –, né la trasmissione della mera istanza di accesso, quanto piuttosto l'invio della copia del documento d'identità integrale del reclamante nonché delle informazioni personali contenute nell'istanza di accesso, quali il numero di telefono e l'indirizzo *e-mail*. Tale comunicazione non era funzionale allo scopo della normativa (ossia quello di presentare un'eventuale opposizione all'accesso), ed era priva di idonei presupposti normativi risultando, pertanto, sproporzionata rispetto alla finalità del trattamento, in violazione del principio di minimizzazione dei dati (artt. 5, par. 1, lett. a) e c); 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del RGPD e dell'art. 2-ter, del Codice (provv. 28 settembre 2023, n. 422, doc. web n. 9947479).

4.4. Trasparenza e pubblicità dell'azione amministrativa

Nel corso dell'anno il Garante ha esaminato numerose questioni riguardanti il tema della protezione dei dati personali con riferimento alle esigenze di trasparenza e di pubblicità dell'azione amministrativa che, per chiarezza espositiva, saranno suddivise in relazione alla pubblicazione di dati personali *online* e all'accesso a informazioni e documenti detenuti dalla p.a. tramite l'istituto dell'accesso civico (art. 5 del d.lgs. n. 33/2013).

4.4.1. La pubblicazione di dati personali online da parte delle pubbliche amministrazioni

Diversi sono stati gli interventi, che hanno portato anche all'adozione di specifici ammonimenti o sanzioni, nei confronti di soggetti pubblici titolari del trattamento, per aver diffuso *online* dati personali in assenza di un'idonea base normativa in violazione dell'art. 2-ter, commi 1 e 3, del Codice e dell'art. 6, par. 1, lett. c) ed e); par. 2 e par. 3, lett. b), del RGPD nonché del principio di minimizzazione di cui all'art. 5, par. 1, lett. c), del RGPD. Ciò ha riguardato in particolare la pubblicazione di dati e informazioni personali su siti web istituzionali di un ministero, un'autorità portuale e di due comuni riferiti a:

- un soggetto citato in una delibera di giunta comunale pubblicata *online* che risultava identificabile dalle relative iniziali e dalle informazioni di contesto, anche considerando le indicazioni relative al periodo di lavoro svolto, alla qualifica professionale e alle vicende processuali riportate (provv. 2 marzo 2023, n. 65, doc. web n. 9874480, cfr. anche provv. 18 luglio 2023, n. 311, doc. web n. 9920562, dove il Garante ha dichiarato l'illegittimità della diffusione delle informazioni riguardanti un reclamante idonee a identificarlo indirettamente anche se era stato oscurato il nome e cognome);

Mancanza di idonea base normativa o violazione del principio di minimizzazione

Iniziali del nome e cognome di un dipendente

- una persona che aveva effettuato una segnalazione a un comune per un abuso edilizio, i cui dati personali erano contenuti nell'ordinanza dell'ente relativa a un ordine di demolizione che riportava in chiaro anche i dati personali del soggetto destinatario del provvedimento amministrativo (fra cui dati anagrafici, luogo e data di nascita, indirizzo di residenza) e dei professionisti incaricati con indicazione, fra l'altro, dell'effettuata segnalazione disciplinare al Collegio dei geometri (prov. 27 aprile 2023, n.166, doc. web n. 9896450);

- diversi soggetti tramite la pubblicazione *online* per errore dei relativi documenti di riconoscimento e tessere sanitarie (prov. 17 maggio 2023, n. 193, doc. web n. 9907862).

4.4.2. Accesso civico

In materia di diritto di accesso civico e protezione dei dati personali il Garante è intervenuto con l'adozione di numerosi pareri resi ai Responsabili della prevenzione della corruzione (RPCT) o a difensori civici ai sensi dell'art. 5, commi 7 e 8, d.lgs. n. 33/2013.

Al riguardo, sono stati ribaditi in via generale i principi e i criteri di reciproco bilanciamento dei due diritti delineati nella determinazione ANAC 28 dicembre 2016, n. 1309, adottata d'intesa con il Garante, "Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 comma 2 del d.lgs. 33/2013", alle quali si rinvia per una più puntuale disamina.

In tale contesto, merita di essere ricordato l'accesso civico a dati delicati come quelli detenuti dal Ministero della salute riguardanti i soggetti vaccinati. Nel caso di specie, la richiesta di ostensione riguardava i dati relativi ai decessi dei soggetti sottoposti alla somministrazione della prima dose di una qualunque tipologia di vaccino anti Covid-19. In particolare, sono state chieste informazioni per singolo assistito, prive del nome e cognome, ma comprendenti data di nascita, di eventuale decesso, della prima dose, della eventuale seconda dose, della eventuale terza dose, della eventuale quarta dose. Il Garante ha evidenziato che le informazioni individuali contenute nell'Anagrafe nazionale dei vaccini nel caso in esame hanno natura particolarmente delicata e, pertanto, una loro eventuale ostensione può alterare il regime e le misure di sicurezza adottate dal Ministero della salute ai sensi dell'art. 32 del RGPD, nonché le regole in materia di *accountability* e le valutazioni del rischio di re-identificazione effettuato dal predetto Ministero mediante la valutazione d'impatto prevista dall'art. 35 del RGPD per i trattamenti a rischio elevato. I dati sono infatti riferiti a soggetti vaccinati trattati su larga scala e alle dosi di vaccino effettuate, il cui numero può essere idoneo a rivelare – nel caso ad es. dell'effettuazione di una sola dose o del mancato completamento del ciclo vaccinale – l'esistenza di possibili casi di esonero successivo o differimento connesse a situazioni di morbilità, pregresse o attuali, temporanee o permanenti (con la conseguente riconducibilità alle «categorie particolari di dati personali» di cui all'art. 9 del RGPD) oppure altre convinzioni personali. Pertanto, dopo avere evidenziato che la normativa statale di settore contenuta nel decreto del Ministero della salute del 17 settembre 2018 riguardante l'istituzione dell'Anagrafe nazionale vaccini prevede l'accessibilità ai dati di tale Anagrafe solo a certe condizioni e in forma aggregata e anonima, è stato rappresentato che i dati richiesti con l'accesso civico nel caso in esame, anche se privi del nome e cognome, non erano dati aggregati né erano stati adeguatamente anonimizzati anche se privati del nome e cognome del soggetto assistito. A tale ultimo riguardo, si è ribadito che un processo di anonimizzazione non può definirsi effettivamente tale qualora non risulti idoneo a impedire che chiunque utilizzi tali dati, in combinazione con i mezzi "ragionevolmente disponibili", possa: 1. isolare una persona in un gruppo

Dati dei segnalanti

Documenti di riconoscimento

Le indicazioni generali fornite dal Garante

Dati relativi ai vaccini

4

**Art. 5-bis, comma 3,
d.lgs. n. 33/2013**

**Art. 5-bis, comma 2, lett.
a), d.lgs. n. 33/2013**

Obiezione di coscienza

**Elaborati concorsi
pubblici**

(*single-out*); 2. collegare un dato anonimizzato a dati riferibili a una persona presenti in un distinto insieme di dati (*linkability*); 3. dedurre nuove informazioni riferibili a una persona da un dato anonimizzato (*inference*). Nel caso in esame bisognava tenere conto del rischio di re-identificabilità dei soggetti interessati derivante dalla richiesta di ostensione dei dati individuali in forma disaggregata (vaccino somministrato, date di somministrazione delle diverse dosi, date di nascita ed eventualmente di decesso) e dalla possibilità per il soggetto istante (ma, alla luce del regime di pubblicità propria dell'accesso civico, anche per soggetti terzi) di incrociare e raffrontare i dati ottenuti con altre informazioni ausiliarie già conosciute o contenute in ulteriori banche dati oppure in dati statistici (provv.ti 27 novembre 2023, n. 552, doc. web n. 9967883; 12 ottobre 2023, n. 469, doc. web n. 9956589; 5 ottobre 2023, n. 466, doc. web n. 9953563).

Sempre in tema di dati delicati, anche nel 2023 il Garante si è espresso in ordine alla sussistenza di casi di esclusione dell'accesso civico ovvero di cd. eccezioni assolute con specifico riferimento a istanze concernenti dati sulla salute, rispetto alle quali l'amministrazione è tenuta a rifiutare l'accesso, senza necessità di svolgere ulteriori valutazioni di merito in ordine alla sussistenza di un eventuale pregiudizio concreto agli interessi dei soggetti interessati. Ci si riferisce in particolare a richieste di accesso civico aventi a oggetto documenti riguardanti una richiesta di chiarimenti formulata dall'ASL a una casa di cura, compreso il riscontro da essa fornito, che riportavano in chiaro il nominativo o le iniziali del soggetto controinteressato, con dettagliate informazioni riguardanti il relativo ricovero, le prestazioni sanitarie, il percorso di cura, i trattamenti e le visite specialistiche, le patologie e condizioni sanitarie, i rapporti con il personale sanitario, le dimissioni del paziente (provv. 15 dicembre 2023, n. 598, doc. web n. 9976123).

In altre fattispecie, invece, il Garante ha fornito parere su richieste di accesso civico generalizzato, esprimendosi sulla sussistenza del limite derivante dalla protezione dei dati personali di cui all'art. 5-bis, comma 2, lett. a), d.lgs. n. 33/2013 alla luce del quale l'accesso civico generalizzato va rifiutato. Ciò con particolare riferimento a:

- dichiarazioni di obiezione/non obiezione di coscienza rilasciate dai dipendenti in servizio nelle strutture consultoriali, nei reparti di ostetricia e ginecologia dei presidi ospedalieri e nelle aziende sanitarie rilasciate ai sensi dell'art. 9 della l. 19 aprile 1978, divisi per figura professionale e con precisa indicazione delle strutture alle quali le dichiarazioni afferiscono. Al riguardo, è stato fra l'altro evidenziato che i dati personali contenuti nelle citate dichiarazioni del personale sanitario e di quello esercente le attività ausiliarie rientrano nelle "categorie particolari di dati personali" di cui all'art. 9 del RGPD in quanto si tratta di dati idonei a rivelare convinzioni personali dei soggetti interessati, anche di tipo religioso o filosofico. L'ostensione di tali dati può arrecare, in relazione ai casi e al contesto in cui possono essere utilizzati da terzi, tenendo conto anche del particolare regime di pubblicità dei dati oggetto di accesso civico generalizzato, il pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), d.lgs. n. 33/2013. Pertanto, anche nel fornire dati aggregati deve essere effettuata un'attenta valutazione inerente al rischio di re-identificazione degli obiettori e non obiettori di coscienza (provv. 22 giugno 2023, n. 267, doc. web n. 9919260);

- elaborati scritti in un concorso pubblico. Il Garante ha evidenziato che la questione dell'accesso civico generalizzato alla copia degli elaborati scritti dei concorsi pubblici è stata esaminata più di una volta, sotto diversi profili (cfr. provv.ti 7 novembre 2019, n. 200, doc. web n. 9196072; 26 ottobre 2017, n. 433, doc. web n. 7156158; 24 maggio 2017, n. 246, doc. web n. 6495600; 7 novembre 2017 n. 366, doc. web n. 7155171). Al riguardo, ha ricordato che anche la CGUE ha affermato che il contenuto delle risposte fornite da un candidato in una prova concorsuale

riflette il relativo livello di conoscenza e di competenza in un dato settore, nonché i suoi processi di riflessione, il suo giudizio e il suo spirito critico, indicando anche molteplici aspetti di carattere personale circa le caratteristiche individuali relative, ad esempio, alla preparazione professionale, alla cultura, alle capacità di espressione o al carattere della persona (che costituiscono aspetti valutabili nella selezione dei partecipanti) (CGUE 20 dicembre 2017, C-434/16; cfr. anche punto n. 23 delle conclusioni dell'Avvocato generale, causa C-434/16, cit.). Pertanto, è stato osservato che l'uso di tali informazioni può avere un effetto sui diritti e interessi dei soggetti interessati, in quanto può determinare o influenzare, per esempio, le possibilità di accedere alla professione o all'impiego desiderati. Nel caso in esame, è stato comunque ribadito che, anche se va rifiutato l'accesso civico, resta ferma la possibilità che i medesimi elaborati scritti possano essere resi ostensibili nel caso in cui venga dimostrata l'esistenza di un interesse qualificato ai sensi della l. n. 241/1990 (provv. ti 29 gennaio 2023, n. 36, doc. web n. 9867345; 27 aprile 2023, n. 177, doc. web n. 9895517);

- note inviate ai dipendenti aventi a oggetto l'attribuzione delle specifiche responsabilità con indicazione dell'importo dell'indennità annuale spettante, alle quali erano allegate le singole schede di attribuzione dei punteggi e di determinazione del compenso. In tale fattispecie, è stato rilevato che le citate note contenevano dati personali dei dipendenti controinteressati di varia natura e specie, quali: il nome e cognome; la qualifica di dipendente della provincia con indicazione della categoria (es.: C o D), del livello (da 1 a 6), dell'area; l'importo dell'indennità annuale assegnata sulla base della scheda di pesatura; le specifiche mansioni e responsabilità attribuite in aggiunta ai normali compiti istituzionali; i punteggi assegnati per le mansioni esercitate nel periodo di riferimento. È stato rappresentato, fra l'altro, che l'indennità era attribuita in base a elementi valutativi dell'attività svolta e che l'ostensione generalizzata delle note avrebbe esposto i dipendenti a pregiudizi o turbative quanto al regolare svolgimento delle funzioni pubbliche o delle attività di pubblico interesse esercitate. Pertanto, è stato ritenuto che l'ente aveva correttamente respinto la richiesta di accesso civico alle predette note (provv. ti 13 luglio 2023, n. 308, doc. web n. 9990570; 3 agosto 2023, n. 343, doc. web n. 9925408; 29 settembre 2023, n. 461, doc. web n. 9953581);

- atti istruttori relativi a un interpello per la copertura di 84 posizioni dirigenziali non generali presso una pubblica amministrazione. Nel caso in esame, è stato osservato che la documentazione richiesta conteneva osservazioni di merito, anche comparative, circa la "spendibilità" / "idoneità" della candidatura di un determinato dirigente presso uno specifico ufficio piuttosto che un altro, in base alle complessità (anche gestionali) dell'ufficio da dirigere e alla luce delle preferenze indicate dal candidato (in diversi casi disattese dalla Commissione in sede di assegnazione dell'incarico). Ai verbali della commissione erano inoltre state allegate le singole schede di valutazione riferite ai dirigenti che avevano partecipato all'interpello, le quali risultavano contenere il punteggio singolo e totale rispetto a numerosi fattori relativi ad attitudini e capacità professionali oppure a specifiche competenze ed esperienze dei candidati nonché le rispettive dichiarazioni di disponibilità. In proposito, è stato sottolineato che i predetti dati e informazioni non costituivano dati pubblici e che la relativa ostensione doveva essere valutata alla luce delle regole e dei limiti previsti dalla disciplina statale di settore in materia di accesso civico, tenuto conto anche di una certa delicatezza dell'informazione richiesta, nonché del fatto che l'ostensione generalizzata delle predette informazioni personali tramite l'istituto dell'accesso civico poteva ben essere fonte di possibili ripercussioni negative sul piano professionale o relazionale, anche all'interno dell'ambiente lavorativo, cosicché si veniva a configurare per i soggetti controinteressati, a seconda delle ipotesi e del contesto in cui i dati

4

Indennità, gratifiche e punteggi di dipendenti

Valutazioni comparative di dirigenti

**Relazione su indagini
interne di una p.a.**

**Autorizzazioni
paesaggistiche**

CILA

Concessioni cimiteriali

**Insussistenza del limite
di cui all'art. 5-bis,
comma 2, lett. a),
d.lgs. n. 33/2013**

e le informazioni fornite potevano essere utilizzate da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), d.lgs. n. 33/2013 (prov. 3 agosto 2023, n. 353, doc. web n. 9921143);

- relazione finale di un'indagine amministrativa interna disposta a seguito di una segnalazione riguardante il contesto lavorativo ed effettuata tramite la distribuzione di alcuni questionari ai dipendenti. Al riguardo è stato evidenziato che la relazione conteneva dati personali di diversa natura e specie che identificavano più persone e fornivano indicazioni su una vicenda specifica e sui rapporti di lavoro fra colleghi, appartenenti al medesimo ufficio, con descrizione dei fatti e della segnalazione effettuata. Conseguentemente, è stato ritenuto che la relativa ostensione avrebbe determinato un'interferenza ingiustificata e sproporzionata nei diritti e nelle libertà dei soggetti controinteressati, con possibili ripercussioni negative sul piano sociale, relazionale e professionale (art. 5-bis, comma 2, lett. a), d.lgs. n. 33/2013; art. 5, par. 1, lett. b) e c), del RGPD) (prov. 26 ottobre 2023, n. 492, doc. web n. 9953599);

- autorizzazioni e valutazioni paesaggistiche di un comune con particolare riferimento a progetti, riproduzioni fotografiche, relazioni tecniche illustrative, tavole grafiche ed elaborati grafici, nonché informazioni e documenti riguardanti un procedimento sanzionatorio per assenza dell'autorizzazione paesaggistica poi sanata (prov. 29 gennaio 2023, n. 37, doc. web n. 9870805);

- dati e/o documenti riguardanti un intervento di manutenzione straordinaria secondo la procedura della CILA (comunicazione di inizio lavori asseverata), prevista dall'art. 6-bis, del d.P.R. n. 380/2001. Anche in tal caso, conformemente ai precedenti orientamenti in materia, è stato ricordato che le informazioni e i dati, anche di carattere personale, da presentare all'ente competente e contenuti nel predetto titolo abilitativo edilizio sono molteplici e di diverso genere e natura. È stato pertanto confermato che, anche in questo caso, la generale conoscenza dei dati e delle informazioni personali contenute nella CILA, considerando la quantità e qualità dei dati personali coinvolti, avrebbe determinato un'interferenza ingiustificata e sproporzionata nei diritti e libertà del soggetto controinteressato – in violazione del ricordato principio di minimizzazione dei dati (art. 5, par. 1, lett. c), del RGPD) – con possibili ripercussioni negative sul piano personale e sociale. Quest'ultimo aveva, in particolare, rappresentato, in sede di opposizione all'accesso civico, che con l'eventuale ostensione della documentazione richiesta si sarebbero fornite “indicazioni relative alla conformazione della [propria] abitazione principale” che potevano compromettere il relativo diritto alla *privacy* e creare un pregiudizio alla sicurezza personale (prov. 22 settembre 2023, n. 418, doc. web n. 9953858);

- concessioni cimiteriali rilasciate dal comune. Tali documenti contenevano dati e informazioni personali di natura delicata, in quanto inerenti ai titolari delle concessioni cimiteriali, alla decisione di rinnovare la concessione o di procedere invece all'estumulazione di un proprio caro o di spostare i relativi resti in altro sito, nonché alla precisazione di quanto pagato all'amministrazione per tali operazioni (prov. 16 novembre 2023, n. 550, doc. web n. 9965679).

Il Garante, infine, si è espresso anche in fattispecie per le quali non si poteva negare l'accesso civico per motivi di protezione dei dati personali.

Il riferimento è a un caso in cui oggetto di accesso civico sono state le “manifestazioni di interesse” inviate al sindaco dai componenti in carica della Commissione consultiva della mobilità istituita da un comune. In particolare, tali documenti contenevano dati personali (quali indicazioni anagrafiche, cittadinanza, godimento dei diritti civili e politici) con allegato il *curriculum* attestante la “conoscenza sul funzionamento della Commissione e la maturata esperienza e competenza”. A differenza dei precedenti casi esaminati dal Garante in materia di manifestazioni di interesse (cfr. prov. 30 marzo 2017, n. 162, doc. web n. 6393422), la fattispecie in esame si

caratterizzava per la circostanza che la richiesta di accesso civico generalizzato non riguardava tutti coloro che avevano inviato candidature e che non erano stati selezionati, ma esclusivamente le manifestazioni di interesse inviate dai componenti della Commissione consultiva per la mobilità nominati dal sindaco e che erano risultati in carica. Pertanto, è stato chiesto al comune destinatario dell'istanza di accesso civico di riesaminare il provvedimento di diniego, consentendo l'accesso ai dati e ai *curricula* dei componenti in carica della Commissione consultiva per la mobilità, per i quali sono previsti obblighi di pubblicazione obbligatoria ai sensi dell'art. 15, d.lgs. n. 33/2013, provvedendo, però, a selezionare e oscurare le informazioni personali che potevano risultare sproporzionate, eccedenti e non pertinenti rispetto alla finalità di trasparenza (es.: residenza, recapiti, codici fiscali, sottoscrizioni autografe o anche – previo coinvolgimento dei soggetti controinteressati – possibili informazioni su qualità ed esperienze eventualmente contenute nei *curricula* non rilevanti perché non attinenti alle competenze specifiche sulle materie richieste per partecipare alla selezione) (provv. 1° giugno 2023, n. 222, doc. web n. 9908447).

Analogamente, è stato precisato che non era possibile invocare il limite della proiezione dei dati personali previsto dall'art. 5-*bis*, comma 2, lett. a), d.lgs. n. 33/2013 in relazione a istanze concernenti informazioni e dati riferibili non a persone fisiche, ma a società o persone giuridiche, per i quali è stato ancora una volta ribadito che è necessario valutare la sussistenza di limiti diversi (es. art. 5-*bis*, comma 2, lett. c), d.lgs. n. 33/2013) (provv. 20 febbraio 2023, n. 40, doc. web n. 9872995, cfr. sul tema dell'accesso ai dati societari e persone giuridiche: provv.ti 13 aprile 2023, n. 149, doc. web n. 9888170; 10 agosto 2023, n. 355, doc. web n. 9990602; 14 agosto 2023, n. 356, doc. web n. 9929110).

4.5. Trattamenti di dati personali effettuati dalle amministrazioni centrali, regioni ed enti locali

4.5.1. Trattamenti di dati personali effettuati dalle amministrazioni centrali

Le amministrazioni centrali, come anche rappresentato nel paragrafo relativo alla digitalizzazione della p.a. (cfr. par. 4.10), hanno consultato il Garante sulle iniziative assunte nel solco del processo di digitalizzazione, stimolato dall'attuazione del PNRR. Il Garante ha esercitato i poteri attribuitigli dal RGPD e dal Codice al fine di assicurare il rispetto dei diritti e delle libertà degli interessati in tali contesti, spesso caratterizzati da rischi elevati in ragione delle caratteristiche presentate dai trattamenti prospettati dalle amministrazioni coinvolte.

Nel 2023, l'Autorità ha proseguito la propria attività di vigilanza sulle grandi banche dati pubbliche verificando le misure di sicurezza adottate e la legittimità degli accessi effettuati dai soggetti autorizzati.

Il Garante ha espresso parere favorevole sugli schemi di due decreti direttoriali del Ministero delle imprese e del *made in Italy*, attuativi del decreto del Ministero dello sviluppo economico del 7 maggio 2019, aventi a oggetto, rispettivamente, la definizione delle modalità e dei termini per la presentazione delle domande di iscrizione all'elenco dei *manager* qualificati e delle società di consulenza abilitati allo svolgimento degli incarichi manageriali, e il modello di domanda di ammissione al contributo e la definizione dei termini per la presentazione, nonché dei criteri di valutazione delle domande e per l'assegnazione prioritaria delle risorse disponibili. Nel quadro delle interlocuzioni intercorse, il Ministero aveva accolto le indicazioni fornite dall'Ufficio relative, in particolare, ai ruoli ricoperti dagli attori coinvolti, alle tipologie di dati personali oggetto di trattamento (anche distinguendo tra le informazioni fornite obbligatoriamente dai richiedenti, l'iscrizione all'elenco ministeriale e quelle fornite

4

Elenco *manager*
dell'innovazione

4

Trasferimento dati dalla CONSOB all'organismo di vigilanza USA sui revisori

Accesso alle informazioni per la ricerca dei beni da pignorare

Credito d'imposta nei procedimenti di mediazione

facoltativamente) e ai tempi di conservazione (sia in relazione alla consultazione da parte delle imprese che alla richiesta del *voucher* e alla fase di godimento dell'agevolazione). Nel parere è stato altresì ricordato che il titolare del trattamento deve tenere conto di quanto indicato nel report “2022 Coordinated Enforcement Action - Use of cloud-based services by the public sector” adottato dal CEPD il 17 gennaio 2023, al fine di assicurare il rispetto del RGPD nel momento in cui un soggetto pubblico, nell'esercizio delle sue funzioni istituzionali, si avvale di servizi *cloud* (prov. 23 marzo 2023, n. 80, doc. web n. 9875280).

Con un procedimento complesso sottoposto all'esame preliminare del CEPD, il Garante ha autorizzato la CONSOB, ai sensi degli artt. 46, par. 3, lett. b) e 58, par. 3, lett. i), del RGPD, a stipulare il progetto di accordo amministrativo per il trasferimento di dati personali verso il *Public Company Accounting Oversight Board* (PCAOB, ossia l'autorità non governativa statunitense di vigilanza sui revisori contabili), volto ad agevolare l'assolvimento delle rispettive funzioni di controllo, ispezione e indagine sui revisori che ricadono sotto la vigilanza di entrambe le autorità, alla luce di quanto previsto dall'art. 33, d.lgs. 27 gennaio 2010, n. 39 e dall'art. 4, commi 3 e 5-*bis*, d.lgs. 24 febbraio 1998, n. 58. Ai fini dell'autorizzazione, il Garante ha tenuto conto del fatto che i contenuti del progetto di accordo erano allineati a quelli del progetto di accordo amministrativo per il trasferimento di dati personali tra l'autorità di vigilanza francese sui revisori (H3C) e il medesimo organismo USA, avallato dal CEPD con parere 5/2021 del 2 febbraio 2021. In ogni caso, al fine di assicurare un livello adeguato di protezione in caso di trasferimento dei dati verso un Paese terzo, il Garante ha ritenuto indispensabile condizionare l'autorizzazione al rispetto di tutte le clausole previste nel progetto in accordo, ribadendo altresì che quest'ultimo lascia impregiudicati i propri compiti di vigilanza (prov. 17 maggio 2023, n. 196, doc. web n. 9904047).

Il Ministero della giustizia ha sottoposto all'Autorità uno schema di convenzione con l'Agenzia delle entrate, volto a regolamentare le modalità di accesso alle banche dati contenenti le informazioni utili ai fini della ricerca, da parte degli ufficiali giudiziari e con modalità telematiche, dei beni da pignorare, in attuazione di quanto disposto dall'art. 492-*bis* c.p.c., ai fini dell'acquisizione del parere previsto dall'art. 155-*quater* disp. att. c.p.c. Il Garante si è pronunciato favorevolmente, alla luce anche del recepimento delle indicazioni fornite durante le interlocuzioni (quali quelle concernenti l'individuazione delle categorie di soggetti che possono avere accesso ai dati personali detenuti nell'Anagrafe tributaria o la conservazione dei dati personali), ponendo però alcune condizioni in merito al tracciamento e alle attività di controllo svolte dal Ministero della giustizia e dall'Agenzia delle entrate sugli accessi effettuati, come la necessità di precisare che i dati oggetto di tracciamento saranno utilizzati dall'Agenzia delle entrate anche per verificare la liceità dei trattamenti, garantire la sicurezza dei trattamenti e, in caso di violazione dei dati personali, adempiere gli obblighi di cui agli artt. 33 e 34 del RGPD (prov. 17 maggio 2023, n. 219, doc. web n. 9907989).

Parere positivo è stato altresì rilasciato su due schemi di decreto del Ministro della giustizia, di concerto con il Ministro dell'economia e delle finanze, concernenti, rispettivamente, la determinazione, liquidazione e pagamento, anche mediante riconoscimento di credito di imposta, dell'onorario spettante all'avvocato della parte ammessa al patrocinio a spese dello Stato (ai sensi dell'art. 15-*octies*, d.lgs. n. 28/2010 e dell'art. 11-*octies*, d.l. n. 132/2014) e gli incentivi fiscali, nella forma del credito di imposta, nei procedimenti di mediazione civile e commerciale e negoziazione assistita (ai sensi dell'art. 20, comma 5, d.lgs. n. 28/2010 e dell'art. 21-*bis*, comma 2, d.l. n. 83/2015). Il Ministero ha tenuto conto delle indicazioni offerte dall'Ufficio nel corso delle interlocuzioni preliminari, che hanno riguardato, in particolare,

l'individuazione dei soggetti coinvolti nei trattamenti di dati personali, e dei relativi ruoli, in relazione alle attività di competenza di ciascuno, modalità adeguate per rendere correttamente le informazioni agli interessati, l'individuazione dei dati personali acquisiti in sede di presentazione dell'istanza di accesso ai predetti benefici, i trattamenti di dati personali effettuati nell'ambito dei controlli sul possesso dei requisiti necessari per accedere ai benefici fiscali secondo quanto previsto dal d.P.R. n. 445/2000, il rispetto del principio di integrità e riservatezza e degli obblighi di sicurezza nell'ambito delle trasmissioni di dati personali tra Ministero della giustizia e Agenzia delle entrate, la disciplina dei trattamenti di dati personali per fini statistici (provv. 22 giugno 2023, n. 257, doc. web n. 9917836).

4.5.2. Trattamenti di dati personali effettuati presso regioni ed enti locali

4.5.2.1. Ambiente

È pervenuta all'Autorità una comunicazione, ai sensi dell'art. 2-ter del Codice, di inizio trattamento dei dati personali, da parte di un Ambito territoriale ottimale (ATO), la società gestore del servizio idrico e i comuni di un bacino idrico integrato, al fine di definire una convenzione regolante la comunicazione al gestore dei dati personali posseduti dai comuni. Le finalità sottese a tale comunicazione sono il censimento corretto delle utenze del servizio idrico, la prevenzione dell'abusivismo e la corretta imputazione della tariffa in base alla destinazione d'uso (commerciale o residenziale).

Nel corso dell'istruttoria sono stati analizzati, in particolare, la natura pubblica dei soggetti coinvolti, il ruolo svolto da ciascuno di essi nel trattamento, le specifiche finalità perseguite connesse allo svolgimento di un compito di interesse pubblico e le relative basi giuridiche. A seguito di approfondimenti condotti dagli enti coinvolti nella convenzione, sono state dettagliate le tipologie dei trattamenti necessari per lo svolgimento delle attività che richiedono l'acquisizione dei dati dai comuni e le tipologie di dati anagrafici richiesti agli enti locali (generalità, intestatari dei contratti di fornitura attivi, soggetti residenti nel comune, etc.) ed è stato assicurato il rispetto dei principi applicabili al trattamento, con particolare riguardo alla trasparenza nei confronti degli interessati (liceità, correttezza e trasparenza), all'individuazione delle finalità e alla selezione dei dati da comunicare (limitazione delle finalità), alla adeguatezza e pertinenza dei dati rispetto alle finalità dichiarate (minimizzazione dei dati) e alle misure adeguate per la sicurezza del trattamento (integrità e riservatezza), ai sensi dell'art. 5, par. 1, lett. a), b), c) ed f), del RGPD. All'esito della valutazione degli elementi forniti dai soggetti stipulanti la convenzione, tenuto conto che la comunicazione dei dati personali ha ad oggetto una selezione di informazioni estratte dalla banca dati TARI, necessarie e pertinenti per effettuare il controllo delle utenze da parte del gestore del servizio idrico, e che tale comunicazione non ha natura sistematica e su larga scala, l'Autorità ha preso atto favorevolmente della notizia pervenuta ai sensi dell'art. 2-ter del Codice (nota 3 luglio 2023).

È pervenuto all'Autorità un quesito da parte di un comune circa la corretta individuazione del ruolo del gestore del servizio di raccolta dei rifiuti urbani quale titolare autonomo del trattamento, contitolare o responsabile del trattamento.

Al riguardo, l'Autorità, rammentata la figura del titolare del trattamento (art. 4, par. 1, punto 7), del RGPD, e linee guida 07/2020 del CEPD), con specifico riguardo alle condizioni di liceità, ha rappresentato che il trattamento dei dati personali da parte dei soggetti pubblici o gestori dei pubblici servizi è lecito se "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri" (art. 6, par. 1, lett. e) e par. 2 e 3, del RGPD; 2-ter del Codice) e deve avvenire nel rispetto dei principi stabiliti dall'art. 5 del RGPD. La gestione dei rifiuti

4

Gestione servizio idrico

Rifiuti urbani

4

PEC e notifica di
contravvenzioni al
codice della strada

urbani rientra tra le attività istituzionali affidate agli enti locali, che non possono, pertanto, “spogliarsi” di tale finalità e compito, ma possono scegliere di affidarne la gestione a soggetti terzi disciplinando il rapporto ai sensi dell’art. 28 del RGPD. Sul punto l’Autorità si era tra l’altro già espressa, affermando che “la gestione dei rifiuti urbani è, secondo la normativa di riferimento, un’attività di interesse pubblico svolta, in particolare, dai comuni che, con propri regolamenti, stabiliscono le modalità della raccolta differenziata, del conferimento e del trasporto delle diverse frazioni di rifiuti, per favorirne la gestione separata e promuoverne il recupero, nel rispetto dei principi di efficienza, efficacia ed economicità” (prov. 14 luglio 2005, doc. web n. 1149822).

Ciò premesso, l’Autorità ha invitato il comune a valutare, in ogni caso, esaminate le condizioni, il contesto e le circostanze relative all’affidamento del servizio dei rifiuti urbani, l’inquadramento corretto del rapporto con il gestore, anche ai fini della equa ripartizione delle responsabilità del trattamento dei dati personali (nota 5 dicembre 2023).

4.5.2.2. Mobilità e trasporti

Continuano a pervenire reclami e segnalazioni aventi ad oggetto la notifica di una sanzione, per violazione del codice della strada, attraverso la PEC inerente all’attività lavorativa e professionale degli interessati (es. studi professionali).

L’Autorità ha ribadito che, con la circolare 300/STRAD/1/10060.U/2021 del 17 novembre 2021, il Ministero dell’interno ha precisato che è esclusa “la possibilità di utilizzare gli indirizzi PEC riferiti a studi professionali per notificare violazioni commesse con un veicolo intestato al professionista, poiché esse sono visibili anche al personale che collabora con l’intestatario della PEC”.

Al fine di contemperare il profilo di protezione dei dati personali con le necessità di celerità e certezza dell’attività di notifica, occorre distinguere, tuttavia, le ipotesi in cui l’indirizzo utilizzato nell’ambito lavorativo non sia direttamente e agevolmente riferibile a uno studio professionale (ad es., perché riferibile a una persona fisica e non ad uno studio o ad un’associazione di professionisti). In questi casi, l’Autorità ha chiarito che non sussiste il rischio automatico di una comunicazione dei dati personali dell’interessato (il singolo professionista) a terzi (collaboratori, segretari, associati, ecc.), atteso che a tale indirizzo PEC potrebbero accedere soggetti diversi dal professionista intestatario solo su espressa autorizzazione di quest’ultimo (note 15 maggio, 10 giugno e 17 luglio 2023).

4.5.3. Esercizio dei diritti

Sono pervenuti numerosi reclami aventi ad oggetto l’esercizio dei diritti di cui agli artt. 15 e ss. del RGPD, che, tuttavia, viene spesso utilizzato impropriamente in luogo di altri istituti riconosciuti da specifiche normative di settore eventualmente applicabili (quali il cd. accesso bancario ed il cd. accesso documentale).

Al riguardo l’Autorità ha precisato che i diritti di cui agli artt. 15 e ss. del RGPD mirano a rendere consapevole l’interessato dei trattamenti dei dati che lo riguardano, ma non possono essere utilizzati in sostituzione di altri strumenti né per contestare nel merito provvedimenti amministrativi o aspetti di natura contrattuale sindacabili esclusivamente presso l’Autorità giudiziaria competente.

In particolare è stato ribadito che ai sensi dell’art. 15 del RGPD l’interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, l’accesso ai dati personali e alle informazioni di cui ai parr. 1 (lett. da a) ad h)) e 2 del medesimo articolo nonché “copia dei dati personali oggetto di trattamento” (par. 3), ma non, necessariamente, copia dei documenti nei quali tali dati sono riportati.

4

A seguito di un reclamo l'Autorità è venuta a conoscenza di un mancato riscontro all'esercizio di diritto di accesso ai sensi dell'art. 15 del RGPD presentato da un cittadino nei confronti di un comune e di un'azienda territoriale di edilizia residenziale. L'interessato, in particolare, aveva esercitato tale diritto al fine di comprendere quale soggetto fosse il titolare del trattamento, nonché il proprietario dell'appartamento di cui lo stesso era inquilino. Il mancato riscontro all'esercizio del diritto di accesso ai sensi dell'art. 15 del RGPD aveva impedito all'interessato di individuare correttamente l'ente proprietario dell'immobile e, quindi, aveva comportato l'impossibilità di beneficiare del diritto di prelazione all'acquisto dell'alloggio assegnato. Per tali ragioni l'Autorità ha sanzionato il comune, titolare del trattamento, per violazione degli artt. 5, 12, 15 del RGPD e 157 del Codice (provv. 1° giugno 2023, n. 224, doc. web n. 9916670).

L'Autorità ha, invece, ammonito l'azienda territoriale che, da quanto emerso nel corso dell'istruttoria, pur non essendo proprietaria dell'immobile aveva provveduto comunque ad adottare misure per attenuare il danno subito dall'interessato, collaborando con il comune, titolare del trattamento, nel fornire riscontro all'interessato (provv. 1° giugno 2023, n. 225, doc. web n. 9917702).

In un caso simile l'Autorità ha ammonito un comune per mancato riscontro alla richiesta di esercizio dei diritti avanzata dall'interessato ai sensi degli artt. 17, 18 e 21 del RGPD. In particolare, il comune non aveva fornito riscontro all'interessato nell'errata convinzione che l'infondatezza dell'istanza comportasse la non necessità di un formale riscontro. L'Autorità ha rammentato, al riguardo, che l'art. 12, par. 3, del RGPD stabilisce che il titolare del trattamento debba dare riscontro – anche negativo – alla richiesta dell'interessato senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della stessa. Se non ottempera alla richiesta dell'interessato deve, in ogni caso, informare l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale (cons. 59 e art. 12, par. 4, del RGPD). Considerato in ogni caso che il mancato riscontro nei termini stabiliti dal RGPD non aveva comportato alcuna conseguenza in capo all'interessato, in quanto le sue richieste di cancellazione, limitazione e opposizione non avrebbero comunque potuto essere accolte, si è ritenuto sufficiente ammonire il comune per la violazione degli artt. 5 e 12 (in combinato disposto con gli artt. 17, 18 e 21) del RGPD (provv. 7 dicembre 2023, n. 586, doc. 9970880).

4.6. Trattamenti per finalità amministrative

All'esito di una complessa istruttoria, che ha ricompreso anche un'attività ispettiva urgente, avviata a seguito di notizie di stampa, l'Autorità ha adottato un provvedimento sanzionatorio nei confronti di un comune e di un'azienda municipale (società *in house*) cui è affidata la gestione dei servizi cimiteriali, per aver diffuso i dati delle donne che si erano sottoposte a un'interruzione di gravidanza, indicandoli su targhette apposte sulle sepolture dei feti. I dati delle donne, oltre che sulle targhette, erano stati oggetto di ulteriori trattamenti da parte dei servizi cimiteriali e del comune connessi alla tenuta dei registri cimiteriali e all'archiviazione della documentazione ricevuta dalla ASL, costituita dall'autorizzazione al trasporto e sepoltura e dal certificato medico legale (cfr. par. 5.5).

Considerato che l'indicazione dei dati delle donne sulle targhette apposte sopra le sepolture risulta essere stata effettuata in assenza di una base giuridica (artt. 5, par. 1, lett. a) e 9 del RGPD; art. 2-*sexies* del Codice) e in violazione dello specifico divieto di

4

diffusione di dati sulla salute (art. 2-*septies*, comma 8, del Codice) e che il trattamento di tali dati è stato effettuato in modo inesatto e incongruo per contrassegnare una sepoltura che non riguardava la donna (art. 5, par. 1, lett. d), del RGPD) e, in ogni caso, privo di una finalità legittima, atteso che la necessità di identificare la sepoltura di un feto poteva essere soddisfatta riportando semplici codici (art. 5, par. 1, lett. b), del RGPD), è stato adottato nei confronti del comune, in qualità di titolare del trattamento, un provvedimento correttivo per la violazione delle disposizioni sopra richiamate. Inoltre, considerato che i predetti trattamenti sono stati effettuati dall'azienda municipale che gestisce i servizi cimiteriali, designata responsabile del trattamento, alla quale il titolare non aveva impartito alcuna istruzione specifica per i casi in esame, con il medesimo provvedimento il comune è stato ritenuto responsabile della violazione degli artt. 28 e 29 del RGPD (provv. 27 aprile 2023, n. 163, doc. web n. 9900808).

All'esito dell'istruttoria, sono stati adottati due ulteriori provvedimenti correttivi. Il primo nei confronti della predetta azienda municipale responsabile del trattamento, a seguito della violazione dell'art. 29 del RGPD, per non aver richiesto specifiche istruzioni al titolare del trattamento, nonostante l'asserita lacunosità del quadro normativo, e degli artt. 28, 29 e 32 del RGPD e 2-*quaterdecies*, in relazione all'attuazione, in parte incompleta e, in parte, non adeguata, delle istruzioni e delle misure organizzative tecniche impartite dal titolare, successivamente all'avvio dell'istruttoria, al fine di superare le criticità contestate (provv. 27 aprile 2023, n. 164, doc. web n. 9900826). Il secondo provvedimento correttivo è stato adottato nei confronti della ASL per aver trasmesso ai servizi cimiteriali del comune dati relativi alla salute, direttamente identificativi delle donne interessate da un'interruzione di gravidanza (sia essa spontanea o volontaria), in contrasto con i principi base del trattamento di cui all'art. 5, par. 1, lett. c) e f), del RGPD (provv. 27 aprile 2023, n. 165, doc. web n. 9900503; cfr. par. 5.5).

4.7. Servizi online e misure di sicurezza

A seguito di una segnalazione, è stata avviata un'istruttoria nei confronti di una società di servizi di elaborazione dati, interamente partecipata da un comune, che svolge in regime di *in house providing* i servizi relativi al supporto informatico, assistenza e consulenza, sviluppo e manutenzione del *software*, nonché attività di amministrazione dei sistemi informativi dell'ente. L'istruttoria ha accertato che l'accesso da rete pubblica alla intranet aziendale della predetta società risultava possibile con protocollo di comunicazione HTTP, rendendo, in tal modo, la comunicazione utente-*server* priva di protezione e di garanzie a tutela della riservatezza e dell'integrità dei dati scambiati tra il *browser* dell'utente e il *server* che ospitava la intranet della società, nonché inidonea a consentire agli utenti di verificare l'autenticità del sito web visualizzato. L'utilizzo di tecniche crittografiche, allo stato, è una delle misure comunemente adottate per proteggere, in particolar modo, le credenziali di autenticazione degli utenti di un sito/servizio *online* durante la loro trasmissione su rete internet, tenuto conto degli elevati rischi presentati dal trattamento di tali dati che possono derivare dall'accesso non autorizzato agli stessi o dalla loro divulgazione, anche in ragione della tendenza di molti utenti a riutilizzare la stessa *password*, o comunque una *password* molto simile, per l'accesso a diversi servizi *online*. Per tali motivi, ritenuto che il mancato utilizzo di tecniche crittografiche per la trasmissione dei dati configurasse una violazione dell'art. 5, par. 1, lett. f) e dell'art. 32 del RGPD, il Garante ha adottato nei confronti della società un provvedimento correttivo per avere trattato i dati in violazione del RGPD (provv. 31 agosto 2023, n. 362, doc. web n. 9935548; cfr. par. 4.8. per ulteriori profili di inosservanza da parte della stessa società).

4.8. Il RPD in ambito pubblico

Il 2023 è stato caratterizzato dall'avvio della seconda azione coordinata per l'attuazione del RGPD (*Coordinated Enforcement Framework - CEF 2023*) promossa dal CEPD, a cui hanno partecipato le autorità di protezione dati europee, tra cui il Garante, incentrata sulla designazione e la posizione dei RPD (cfr. par. 21.1).

L'Autorità ha altresì avviato un'indagine nei confronti di grandi enti locali per verificare il rispetto dell'obbligo di comunicazione dei dati di contatto del RPD di cui all'art. 37, par. 7, del RGPD, disponendo l'avvio, nei confronti di alcuni di questi enti risultati inadempienti, di appositi procedimenti volti all'adozione di provvedimenti correttivi e sanzionatori. Tale attività di vigilanza è stata poi estesa anche ad altri enti locali (cfr. *Newsletter* 26 maggio 2023, doc. web n. 9890504).

Il Garante ha sanzionato un comune per aver designato quale RPD un soggetto che si trovava in una posizione di conflitto di interessi, in violazione dell'art. 38, par. 6, del RGPD, in quanto direttore amministrativo della società partecipata dallo stesso comune per il quale quest'ultima svolge, in regime di *in house providing* e nella veste di responsabile del trattamento, servizi strumentali di carattere informatico. In tal modo, il ruolo assolto dall'RPD all'interno dell'organizzazione della società lo portava a concorrere ad assumere decisioni in ordine ai trattamenti che la stessa effettuava per conto del comune, titolare di tali trattamenti; ciò avveniva in un contesto, peraltro, in cui la società medesima, quale responsabile del trattamento, e le persone che agivano sotto la sua autorità (compreso il suo direttore amministrativo), ricevevano istruzioni dal titolare del trattamento. Inoltre, il provvedimento – che sanziona il comune anche per la mancata comunicazione all'Autorità dei dati di contatto del RPD designato in sostituzione di quello precedentemente in carica – pone in guardia i titolari del trattamento dall'inserimento, all'interno dei contratti di affidamento dell'incarico di RPD, di clausole che, in qualche modo, possano creare i presupposti per l'effettuazione di condotte in grado di minare l'autonomia decisionale del titolare del trattamento nella scelta dei successivi RPD (provv. 31 agosto 2023, n. 363, doc. web n. 9936094).

Nell'ambito della medesima vicenda, il Garante ha sanzionato la menzionata società per aver omesso di designare un nuovo RPD a seguito delle dimissioni di quello precedentemente designato, nonché di aggiornare i relativi dati di contatto, con riferimento sia all'obbligo di pubblicazione dei dati di contatto che all'obbligo di comunicazione all'Autorità (provv. 31 agosto 2023, n. 362, doc. web n. 9935548).

A seguito di una segnalazione l'Autorità ha, inoltre, appreso che un comune aveva utilizzato sistemi di videosorveglianza per verificare il corretto conferimento dei rifiuti urbani nel territorio comunale in maniera non conforme alla normativa in materia di protezione dei dati personali. Tra le altre violazioni è emerso che il comune aveva provveduto in ritardo alla designazione del RPD e aveva pubblicato in ritardo i dati di contatto del RPD designato, sul proprio sito web istituzionale, ovvero circa un mese dopo la data della designazione dello stesso. Per tali ragioni, l'Autorità ha sanzionato il comune per la violazione dell'art. 37, parr. 1 e 7, del RGPD (provv. 18 luglio 2023, n. 313, doc. web n. 9920578).

Infine, è stata sanzionata un'università, tra le altre cose, per non aver comunicato all'Autorità i dati di contatto del RPD (provv. 17 maggio 2023, n. 195, doc. web n. 9908484).

4.9. Ordini professionali

L'attività dell'Autorità ha riguardato anche taluni trattamenti di dati personali posti in essere da ordini professionali.

A seguito di un reclamo, il Garante ha censurato la condotta di un ordine

Designazione e
posizione dei RPD

Vigilanza su tematiche
RPD

4

territoriale degli avvocati, che – ai fini dell’attivazione di un profilo su un portale web predisposto per consentire la presentazione delle istanze di ammissione al gratuito patrocinio per conto dei propri clienti – aveva chiesto agli avvocati di indicare sia la propria PEC sia la *password* di accesso alla stessa. Il Garante ha osservato che l’ordine, ancorché non avesse conservato i dati in questione, li aveva comunque trattati, sia all’atto della registrazione di un utente al portale (momento in cui la *password*, in chiaro, veniva raccolta, cifrata e memorizzata all’interno di un asserito *cookie* tecnico) sia all’atto della presentazione di un’istanza (momento in cui la *password*, memorizzata in forma cifrata all’interno del predetto *cookie* tecnico, veniva raccolta, decifrata e utilizzata dal portale per l’invio, per conto dell’avvocato, del messaggio PEC contenente l’istanza).

A tal riguardo, il Garante ha chiarito che i *cookie* in questione non potevano considerarsi *cookie* cd. tecnici (in relazione ai quali l’art. 122, comma 1, del Codice prevede una deroga all’obbligo di acquisire il previo consenso informato), non essendo gli stessi strettamente necessari all’erogazione del servizio; in realtà, ciascun avvocato avrebbe potuto provvedere in autonomia all’invio dell’istanza firmata digitalmente dalla propria casella PEC, senza dover fornire all’ordine le credenziali di accesso alla stessa. Si è inoltre accertato che l’ordine non aveva fornito agli interessati, all’atto della registrazione al portale, le informazioni relative al trattamento dei dati personali ivi effettuato. Il complessivo trattamento è stato ritenuto non conforme al principio di protezione dei dati fin dalla progettazione e per impostazione predefinita, non avendo l’ordine adottato adeguate misure tecniche e organizzative, volte ad attenuare i rischi per i diritti e le libertà degli interessati e a garantire un trattamento conforme ai principi di protezione dei dati. Ravvisata la violazione degli artt. 5, 6, 13 e 25 del RGPD, nonché 122 del Codice, il Garante ha adottato un provvedimento sanzionatorio nei confronti dell’ordine (provv. 13 aprile 2023, n. 121, doc. web n. 9889644).

In un altro caso, un ordine territoriale degli avvocati aveva inoltrato al presidente e a un dirigente del locale tribunale una segnalazione che la reclamante aveva presentato all’ordine, in veste di avvocatessa, per informare lo stesso che sia lei sia un’imputata da ella difesa ritenevano di aver contratto il *virus* SARS-CoV-2 in occasione di un’udienza tenutasi presso tale tribunale. Il Garante, tenuto conto di tutte le specifiche circostanze emerse nel corso dell’istruttoria, ha ritenuto sufficiente ammonire il titolare del trattamento, per aver comunicato a terzi dati personali, di cui alcuni relativi allo stato di salute, in assenza di una base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del RGPD, nonché 2-ter e 2-sexies del Codice, nel testo antecedente alle modifiche apportate dal d.l. n. 139/2021 (provv. 2 marzo 2023, n. 57, doc. web n. 9873294; in relazione a un diverso caso che ha interessato un ordine provinciale dei medici chirurghi e degli odontoiatri nel contesto dei procedimenti di accertamento del requisito vaccinale da SARS-CoV-2, cfr. par. 13.9.1.2).

4.10. Digitalizzazione della pubblica amministrazione

Nel corso del 2023 è proseguito il processo di digitalizzazione della p.a., anche sulla spinta dell’attuazione al PNRR. In questo contesto, il Garante ha esercitato la funzione consultiva attribuitagli dal RGPD, dal Codice e dalla legge sugli schemi di atti promossi dalle istituzioni governative e dalle amministrazioni centrali, volti, in particolare, a introdurre nuove funzionalità nel panorama dell’erogazione dei servizi *online* ai cittadini. Sono, inoltre, proseguite le attività di vigilanza e controllo sull’operato dei fornitori di servizi, volte a verificare i processi di rilascio e gestione dei certificati e delle identità digitali (SPID) nonché le violazioni della normativa in materia di protezione dati e quella sui furti di identità perpetrati.

Il Ministero dell'interno aveva sottoposto al Garante la valutazione d'impatto sulla protezione dei dati al fine di ottenere l'autorizzazione a effettuare i trattamenti di dati personali concernenti la creazione, l'impiego e la gestione delle credenziali dell'identità digitale CIE (CIEId) – quale strumento di accesso ai servizi erogati in rete integrante un regime di identificazione elettronica ai sensi del reg. (UE) 910/2014 (reg. eIDAS) – in conformità del decreto del Ministro dell'interno, del Ministro per l'innovazione tecnologica e la transizione digitale e del MEF dell'8 settembre 2022 (su cui il Garante aveva espresso parere con provv. 7 luglio 2022, n. 247, doc. web n. 9803398). Il Garante ha autorizzato il predetto trattamento, considerato che la valutazione d'impatto aveva recepito le indicazioni fornite al fine di rendere i trattamenti conformi alla disciplina in materia di protezione dei dati personali. Tali indicazioni hanno riguardato, in particolare, l'individuazione di misure volte a tutelare gli interessati nella fase di gestione dell'identità digitale CIEId (come l'autonoma gestione dell'identità digitale dell'utente tramite il relativo portale, con la possibilità di modificare e certificare i propri contatti e di visualizzare i relativi *log*; l'invio all'utente di un avviso relativo ai contatti certificati in occasione delle operazioni di modifica degli stessi o di modifica delle credenziali); la registrazione, in appositi *file* di *log*, delle informazioni relative alle operazioni di attivazione e revoca nonché di gestione e utilizzo dell'identità digitale e la relativa conservazione; le informazioni nei confronti degli interessati circa gli attributi che vengono messi a disposizione, dal gestore della CIEId, ai fornitori di servizi a seguito del processo di autenticazione; l'introduzione di un meccanismo di tempestiva informazione tra Ministero dell'interno e fornitori di servizi/soggetti aggregatori in caso di violazioni di sicurezza o altre minacce che comportino un rischio per la sicurezza e per i diritti e le libertà degli interessati. Inoltre, con particolare riferimento all'utilizzo di CIEId da parte di minori, considerato che il citato decreto prevede che, con apposito provvedimento, sentito il Garante, il Ministero individui le funzionalità necessarie e le misure a tutela degli interessati – anche al fine di agevolare il controllo genitoriale finalizzato a verificare il corretto utilizzo dei servizi in rete da parte dei minorenni sotto la propria tutela – viene evidenziato che, nelle more dell'individuazione di adeguate garanzie, tale utilizzo sia consentito anche da parte di minori (ad esclusione di quelli nella fascia da 0 a 5 anni) per l'accesso ai servizi degli istituti scolastici di ogni ordine e grado, tenendo conto di quanto previsto nelle apposite linee guida adottate da AgID per SPID (provv. 23 marzo 2023, n. 81, doc. web n. 9880472).

Il Garante ha reso parere sullo schema di regolamento di funzionamento dell'infrastruttura nazionale del *Single digital gateway* (SDG), da adottarsi con determina del Capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, in attuazione degli impegni presi nell'ambito del PNRR. Il SDG è il "Sistema tecnico per lo scambio transfrontaliero automatizzato di prove" di cui al reg. (UE) 2018/1724 e al reg. (UE) 2022/1463, attraverso cui è consentito lo scambio tra richieste e relative "prove" (documenti o dati) tra le autorità competenti dell'UE nell'ambito di specifiche procedure amministrative, eventualmente su richiesta esplicita dell'interessato. Il Garante ha preliminarmente evidenziato che i trattamenti di dati personali e le relative specifiche tecniche e operative sono dettagliatamente disciplinati dai menzionati regolamenti europei e che nelle competenti sedi europee è ancora in corso il confronto per la definizione dei profili concernenti la realizzazione e gestione delle componenti del SDG da parte della Commissione, per cui risultano limitati i margini di autonomia decisionale lasciati alla regolazione nazionale. Ciò considerato, il Garante ha espresso parere favorevole, sottolineando che le amministrazioni titolari dei trattamenti concernenti i servizi dalle stesse erogate in tale ambito possono aderire al SDG, in conformità al regolamento di funzionamento in questione, senza acquisire il parere dell'Autorità, salvo il caso in cui, a valle di un'eventuale valutazione d'impatto sulla protezione dei dati effettuata da tali

CIEId

Single digital gateway

4

Piattaforma notifiche digitali

Valutazione d'impatto relativa al censimento linguistico

Linee guida AgID su apertura e riutilizzo dei dati dell'informazione del settore pubblico

amministrazioni aderenti, si renda necessaria una consultazione preventiva (prov. 7 dicembre 2023, n. 579, doc. web n. 9974086).

Sullo stesso tema il Garante ha contestualmente reso parere favorevole sullo schema di decreto del Ministro dell'interno di cui all'art. 62, comma 6-bis, d.lgs. n. 82/2005, concernente la messa a disposizione, tramite l'Anagrafe nazionale della popolazione residente (ANPR), delle procedure relative alla richiesta di una prova della registrazione di nascita e alla registrazione del cambio di indirizzo, che ai sensi del menzionato reg. (UE) 2018/1724 dovranno essere realizzate mediante il SDG (prov. 7 dicembre 2023, n. 580, doc. web n. 9974134, cfr. par. 4.11).

Il Garante ha altresì rilasciato un'autorizzazione condizionata a PagoPA S.p.A. per l'effettuazione dei trattamenti di dati personali nell'ambito della Piattaforma notifiche digitali, disciplinata dall'art. 26 del d.l. n. 76/2020 e dal decreto del Ministro per l'innovazione tecnologica e la transizione digitale n. 58/2022 (su cui si era pronunciato con prov. 14 ottobre 2021, n. 369, doc. web n. 9716841). L'Autorità ha valutato favorevolmente il recepimento delle proprie indicazioni concernenti la definizione dei ruoli assunti dai diversi soggetti coinvolti, l'individuazione di misure volte ad assicurare che il gestore invii la notifica (sulla base della natura dell'atto) al domicilio digitale specificamente preposto a ricevere le comunicazioni di natura personale o professionale, l'individuazione di misure idonee ad assicurare che l'acquisizione, da parte dei destinatari, della copia analogica dei documenti oggetto di notifica, presso gli sportelli a ciò preposti, avvenga previa comunicazione dei soli estremi del documento di identità del destinatario in luogo della copia del documento d'identità. Tuttavia, il Garante ha ritenuto necessario prescrivere l'adozione di ulteriori misure volte ad assicurare il rispetto dei principi del Regolamento, e in particolare a: limitare la visibilità della causale ai casi in cui sia certa la notifica nelle mani proprie del destinatario dell'atto oggetto di notifica; impedire all'operatore dello sportello, presso cui il destinatario si rivolge per l'acquisizione dei documenti notificati in forma analogica, di effettuare *download* o copie dei documenti medesimi; non consentire al medesimo operatore la visualizzazione dei documenti oggetto di notifica e delle causali ad essi riferiti; riportare, sulla pagina bianca resa dalla stampante prima dei documenti stampati, il numero delle pagine nonché informazioni che consentano al medesimo operatore di individuare correttamente il soggetto a cui consegnare l'atto (prov. 21 dicembre 2023, n. 604, doc. web n. 9976614).

A seguito del rilascio del parere favorevole del Garante in merito allo schema di regolamento d'esecuzione della Provincia di Bolzano in materia di censimento linguistico che, in attuazione dell'art. 18, comma 2, d.P.R. n. 752/1976 ha introdotto la possibilità di effettuare la rilevazione dei dati anche in via telematica (prov. 6 ottobre 2022, n. 318, doc. web n. 9825838), il Garante si è pronunciato sulla valutazione d'impatto elaborata dai comuni della Provincia autonoma di Bolzano e dall'Istituto provinciale di statistica della Provincia di Bolzano (ASTAT). Tale valutazione aveva tenuto conto delle indicazioni fornite dall'Ufficio nel corso delle interlocuzioni informali intercorse volte, in particolare, a individuare adeguate misure per rendere anonimo il dato relativo all'appartenenza/agggregazione di una persona al gruppo linguistico, in modo tale da impedire o non consentire la re-identificazione degli interessati. Su tale base è stato, pertanto, autorizzato il trattamento ai sensi degli artt. 36, par. 5, e 58, par. 3, lett. c), del RGPD (prov. 23 marzo 2023, n. 97, doc. web n. 9879199).

Il Garante si è espresso sulle linee guida elaborate dall'AgID recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico di cui all'art. 12, d.lgs. n. 36/2006 ai sensi dell'art. 71, d.lgs. n. 82/2005 (prov. 6 luglio 2023, n. 333, doc. web n. 9925342). Al riguardo, l'Autorità è intervenuta a ricordare che non rientrano nell'applicazione delle stesse i documenti, o parti di essi, il cui accesso, ai sensi delle previsioni del Regolamento, del Codice nonché del d.lgs. n.

51/2018, sia escluso o limitato, ovvero risulti pregiudizievole per la tutela della vita privata e dell'integrità degli individui. Ciò è in linea con i precedenti orientamenti del Garante sul riutilizzo dei dati personali, secondo cui, per quanto riguarda gli usi ulteriori di dati personali, e quindi anche il riutilizzo, come previsto dall'art. 6, par. 4, del RGPD, il trattamento di dati personali, per una finalità diversa da quella per la quale i dati personali sono stati inizialmente raccolti, deve essere – in ogni caso – “compatibile” con la finalità originaria del trattamento, con particolare riferimento ai casi in cui tale valutazione abbia a oggetto dati personali pubblicati *online* per adempiere a obblighi di trasparenza e pubblicità dell'azione amministrativa.

Le indicazioni dell'Autorità sono state seguite nelle linee guida, le quali non impongono ulteriori obblighi di pubblicazione *online* di dati personali rispetto a quelli previsti dalla disciplina vigente e, in particolare, non prevedono che ogni obbligo di pubblicazione *online* sancito dalla disciplina vigente si traduca, per ciò stesso, in obbligo di pubblicazione di dati personali come “dati aperti” e, come tali, per definizione, liberamente riutilizzabili per scopi ulteriori, conformemente a quanto previsto anche dal CAD (art. 52, comma 2). Per tale motivo, il soggetto chiamato a dare attuazione agli obblighi di pubblicazione sul proprio sito web istituzionale – qualora intenda rendere i dati riutilizzabili – deve determinare se, per quali finalità e secondo quali limiti e condizioni eventuali utilizzi ulteriori dei dati personali resi pubblici possano ritenersi leciti alla luce del “principio di finalità” e degli altri principi in materia di protezione dei dati personali.

4.11. La materia anagrafica ed elettorale

Con decreto del Ministero dell'interno sono state disciplinate le procedure per garantire l'accesso e l'espletamento delle procedure di cui all'all. II del reg. (UE) 2018/1724; si tratta delle modalità telematiche di richiesta e di rilascio dei certificati di nascita attraverso l'ANPR, in favore del cittadino dell'Unione europea, nato in Italia, non più iscritto nell'ANPR alla data della richiesta, ma comunque registrato nell'anagrafe comunale al momento del subentro del comune in ANPR o successivamente, e delle modalità telematiche con le quali il cittadino dell'Unione europea richiede, ai sensi degli artt. 3 e 9 del d.lgs. n. 30/2007, l'iscrizione anagrafica attraverso l'ANPR e, di conseguenza, può ottenere una certificazione anagrafica di residenza ai sensi del decreto del Ministro dell'interno del 3 novembre 2021. Al riguardo, è stato espresso parere favorevole in assenza di profili di criticità in materia di protezione dei dati personali, essendo state recepite le indicazioni fornite dall'Ufficio nell'ambito delle interlocuzioni informali intercorse durante l'istruttoria, con particolare riferimento alla necessità di esplicitare meglio le modalità di integrazione fra i servizi resi da ANPR e il nodo SDG nazionale, nonché il ruolo del Ministero dell'interno con riguardo allo scambio automatizzato di prove (prov. 7 dicembre 2023, n. 580, doc. web n. 9974134, cfr. par. 4.10).

L'Autorità si è inoltre espressa favorevolmente sullo schema di decreto del Ministero dell'interno riguardante l'erogazione del servizio dei certificati ANPR da parte degli sportelli degli uffici postali nell'ambito del Progetto *Polis-Case* dei servizi di cittadinanza digitale (di cui all'art. 1, comma 2, lett. f), n. 1, d.l. n. 59/2021, convertito, con modificazioni, dalla l. n. 101/2021 e all'art. 38 del d.l. n. 50/2022, convertito, con modificazioni, dalla l. n. 91/2022). L'operatore di Poste italiane, identificato il cittadino richiedente, effettua i necessari controlli anagrafici per verificare la possibilità di procedere al rilascio del certificato, che può essere rilasciato per il richiedente e per i componenti della rispettiva famiglia anagrafica. Al riguardo, è stato espresso parere favorevole non essendo stati rilevati profili di criticità in materia di protezione dei dati personali, ed essendo state recepite le indicazioni fornite

4

**ANPR certificazioni
e cambio residenza
tramite nodo SDG**

ANPR e Polis

4

ANPR e avvocati

Identificativo unico nazionale CIE

dall'Ufficio nell'ambito delle interlocuzioni informali intercorse durante l'istruttoria, con particolare riferimento ai requisiti e ai criteri di individuazione del personale preposto, nonché alle misure tecniche e organizzative volte, anche in un'ottica di responsabilizzazione, a minimizzare il rischio di trattamenti non autorizzati, nel rispetto di quanto previsto dall'art. 5, parr. 1, lett. f) e 2, nonché dagli artt. 24, 25 e 32 del RGPD (provv. 26 ottobre 2023, n. 493, doc. web n. 9954092).

Il Ministero dell'interno ha sottoposto all'Autorità lo schema di decreto ministeriale ai sensi dell'art. 62, comma 6-bis, d.lgs. n. 82/2005 recante l'aggiornamento dei servizi resi disponibili dall'ANPR, al fine di consentire agli avvocati di richiedere, per finalità connesse all'esecuzione del mandato professionale, i certificati anagrafici in modalità telematica resi disponibili tramite l'ANPR. Lo schema esaminato ha tenuto conto delle indicazioni fornite dal Garante nel corso delle interlocuzioni con il Ministero dell'interno, concernenti, in particolare, la necessità che il rilascio dei certificati richiesti dagli avvocati per conto dei propri clienti sia assistito da particolari garanzie, volte ad assicurare che tali certificati siano effettivamente utilizzati per le finalità connesse ad uno specifico mandato professionale, fermo restando il rispetto della disciplina di settore (artt. 33 e ss., d.P.R. n. 223/1989; l. n. 1064/1955). In considerazione delle criticità rilevate, sono state formulate alcune prescrizioni volte a conformare i trattamenti in questione alla disciplina in materia di protezione dei dati personali. In particolare, si è ritenuto di prescrivere l'individuazione di un criterio congruo per determinare il campione di avvocati da sottoporre alla verifica relativa all'iscrizione all'albo, la riformulazione di alcune locuzioni al fine di chiarire che i dati personali dei clienti non sono oggetto di trattamento, nonché l'introduzione di un meccanismo di controllo (da demandare ai consigli dell'ordine competenti) sulla sussistenza di uno specifico mandato professionale e sulla pertinenza dello stesso rispetto al certificato richiesto, in conformità ai principi di liceità, correttezza e trasparenza, di limitazione della finalità e di minimizzazione (art. 5, par. 1, lett. a), b), e c), del RGPD). Inoltre, è stato ingiunto al Ministero dell'interno di trasmettere al Garante, trascorsi sei mesi dall'avvio del trattamento, una relazione sull'efficacia dei criteri e delle misure adottate, che evidenzino le eventuali criticità riscontrate, tenendo conto anche degli esiti delle attività di verifica poste in essere dal Ministero stesso e dai consigli dell'ordine competenti (provv. 22 giugno 2023, n. 279, doc. web n. 9919862).

L'Autorità ha esaminato lo schema di decreto direttoriale del Ministero dell'interno, ai sensi dell'art. 3, comma 1, d.m. 23 dicembre 2015, recante l'aggiornamento delle caratteristiche della Carta d'identità elettronica previste dal modello di cui all'all. A del decreto ministeriale e volto ad adeguare l'attuale modello di CIE alla nuova numerazione degli atti dello stato civile, introducendo il nuovo formato del numero dell'atto di nascita riportato nella CIE (cd. identificativo unico nazionale). Al riguardo, è stato espresso parere favorevole non essendo stati rilevati profili di criticità in materia di protezione dei dati personali (provv. 6 luglio 2023, n. 306, doc. web n. 9920897).

4.12. Trattamenti di dati personali in ambito pubblico mediante dispositivi video

A seguito di una segnalazione, l'Autorità ha accertato che un comune aveva utilizzato sistemi di videosorveglianza per verificare il corretto conferimento dei rifiuti urbani nel territorio comunale in maniera non conforme alla normativa in materia di protezione dei dati personali. In particolare, il comune non aveva fornito un'adeguata informativa sul trattamento dei dati personali, in violazione del principio di liceità, correttezza e trasparenza, né aveva definito i periodi di conservazione delle immagini raccolte, in violazione dei principi di minimizzazione dei dati, limitazione della conservazione, responsabilizzazione e protezione dei dati fin dalla progettazione e per impostazione definitiva.

Al fine di installare e mantenere tali sistemi di videosorveglianza, inoltre, il comune si era avvalso inizialmente di una società senza aver mai provveduto a regolare i rapporti con la stessa ai sensi dell'art. 28 del RGPD (ovvero, per il periodo antecedente al 25 maggio 2018, ai sensi dell'art. 29 del Codice, nel testo anteriore alle modifiche di cui al d.lgs. n. 101/2018 e vigente nel periodo relativo alla vicenda emersa nella segnalazione) e successivamente di un'impresa individuale, regolando il rapporto con la stessa, ai sensi dell'art. 28 del RGPD, soltanto una volta avviato il trattamento dei dati personali. Da ultimo, è emerso che il comune aveva provveduto in ritardo alla designazione del RPD, del quale aveva pubblicato i dati di contatto, sul proprio sito web istituzionale, circa un mese dopo la data della designazione.

Per tali ragioni l'Autorità ha sanzionato il comune per violazione degli artt. 5, par. 1, lett. a), c) ed e), e par. 2 (in combinato disposto con l'art. 24), 12, par. 1, 13, 25, 28 e 37, par. 1 e 7, del RGPD (prov. 18 luglio 2023, n. 312, doc. web n. 9920578).

Inoltre, non avendo la società citata stipulato un accordo sulla protezione dei dati con il comune, prima dell'inizio del trattamento, e non essendo stati individuati dalla stessa altri presupposti che potessero legittimare il trattamento dei dati personali in questione, l'Autorità ha sanzionato la società per violazione degli artt. 5, par. 1, lett. a) e 6 del RGPD per aver posto in essere un trattamento di dati personali in maniera non conforme al principio di liceità, correttezza e trasparenza e in assenza di un idoneo presupposto normativo (prov. 18 luglio 2023, n. 314, doc. web n. 9920664).

Analogamente, anche l'impresa individuale è stata sanzionata per violazione degli artt. 5, par. 1, lett. a) e 6 del RGPD non avendo stipulato un accordo sulla protezione dei dati con il comune, prima dell'inizio del trattamento, e non essendo stati individuati dalla stessa altri presupposti che potessero legittimare il trattamento dei dati personali in questione (prov. 18 luglio 2023, n. 313, doc. web n. 9920645).

Il Garante si è poi occupato di un progetto attuato da un'agenzia nazionale e da un'istituzione museale comunale, che prevedeva l'impiego di dispositivi video, collocati in prossimità di opere d'arte, allo scopo di misurare il livello di gradimento delle stesse tramite un sistema di intelligenza artificiale basato su reti neurali convoluzionali, capace di individuare i volti dei visitatori (*face detection*) e interpretarne il comportamento durante la fruizione delle opere. All'esito dell'istruttoria, originata da una segnalazione, il Garante ha chiarito che, ancorché le immagini riprese risiedessero sul sistema per un intervallo temporale molto breve, lo stesso comportava comunque un trattamento di dati personali, consistente nell'acquisizione e temporanea memorizzazione dell'immagine del volto dei visitatori del museo (cfr. prov. 21 dicembre 2017, n. 551, doc. web n. 7496252). I due soggetti pubblici, qualificati quali contitolari del trattamento, non hanno comprovato che il trattamento potesse fondarsi su un'idonea base giuridica, né era stato stipulato un accordo di contitolarità del trattamento e ai visitatori del museo non era stata fornita un'esaustiva informativa sul trattamento dei dati personali. Il Garante, valutate tutte le specifiche circostanze del caso, ha, pertanto, adottato un provvedimento di ammonimento nei confronti di ciascun contitolare per la violazione degli artt. 5, par. 1, lett. a), 6, 12, 13 e 26 del RGPD, nonché 2-ter del Codice, nel testo antecedente alle modifiche apportate dal d.l. n. 139/2021 (prov. ti 13 aprile 2023, nn. 122 e 123, doc. web n. 9896412 e n. 9896808).

4

5 La sanità

5.1. *La sanità digitale*

Nel corso del 2023 numerosi sono stati gli interventi del Garante sui temi della sanità digitale, originati sia da richieste di parere su atti regolamentari sia da segnalazioni e reclami.

I principali ambiti di intervento hanno riguardato la riforma del Fascicolo sanitario elettronico (FSE) 2.0 e la realizzazione del sistema nazionale di telemedicina, che si collocano nelle azioni di attuazione della Missione 6 (salute) del PNRR. In tali interventi il Garante ha ribadito con forza il necessario coordinamento normativo delle disposizioni di attuazione dei diversi strumenti di sanità digitale, considerato che la prevista interconnessione tra i sistemi informativi sanitari e il FSE rende necessario che le misure tecniche e organizzative da introdurre nell'attuazione delle disposizioni a tutela dei diritti fondamentali dell'interessato e dei principi generali del trattamento siano tra di loro coerenti specie con riferimento alla titolarità dei trattamenti, all'individuazione delle responsabilità e dei compiti dei soggetti a vario titolo coinvolti (cfr. punto 3.2, parere 8 giugno 2023, n. 256, doc. web n. 9900433).

Nel settore della sanità digitale, l'Ufficio è inoltre intervenuto con riferimento ai trattamenti di dati sulla salute effettuati attraverso i sistemi informativi delle strutture sanitarie pubbliche e private utilizzati per la gestione dei dati e dei documenti clinici e, in particolare, in rapporto a quelli effettuati attraverso il *dossier* sanitario e alle componenti aziendali e regionali del FSE.

5.1.1. *Il Fascicolo sanitario elettronico*

A seguito dei pareri non favorevoli del 22 agosto 2022 (doc. web n. 9802729 e n. 9802752), il Ministero della salute ha sottoposto al Garante un nuovo schema di decreto relativo alla disciplina del FSE 2.0, la cui realizzazione è legata al raggiungimento degli obiettivi del sub-investimento FSE del PNRR (prov. 8 giugno 2023, n. 256, doc. web n. 9900433 e comunicato stampa 20 gennaio 2020, doc. web n. 9516732). Complessivamente lo schema trasmesso è risultato profondamente modificato in quanto, al fine di superare i numerosi rilievi all'epoca formulati, sono stati approfonditi, integrati e regolamentati tutti gli aspetti del trattamento dei dati personali connessi alla realizzazione del nuovo sistema di FSE 2.0.

Gli interventi correttivi hanno riguardato, tra l'altro:

- l'ambito di applicazione del decreto, che abroga solo in parte il d.P.C.M. n. 178/2015, il quale rimane pienamente in vigore per il perseguimento attraverso il FSE delle finalità di ricerca e di governo sanitario;

- dati e documenti che possono essere consultati attraverso il FSE, con riferimento ai quali è stata assicurata una elencazione tassativa e precisato, ad esempio, che le informazioni relative alle esenzioni per reddito e i relativi codici esenzione devono essere consultabili dal solo interessato;

- l'accesso al FSE in emergenza, prevedendo, come richiesto dal Garante, che, nel rispetto del principio di proporzionalità, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere e di rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato che non abbia espresso il consenso alla consultazione del proprio FSE per finalità di cura, gli esercenti le professioni sanitarie potranno accedere prioritariamente alla partizione del FSE denominata

5

profilo sanitario sintetico (PSS) e, ove necessario, agli ulteriori dati e documenti del FSE, a eccezione di quelli per i quali l'interessato abbia richiesto l'oscuramento, per il tempo strettamente necessario ad assicurare le indispensabili cure o fino a quando l'interessato non sia nuovamente in grado di esprimere la propria volontà al riguardo;

- i diritti degli interessati, con particolare riferimento all'individuazione di misure uniformi sul territorio nazionale per l'esercizio del diritto di oscuramento e di quello di conoscere gli accessi effettuati al proprio FSE;

- il profilo sanitario sintetico (PSS) e il taccuino personale (TP), indicandone la titolarità del trattamento e le responsabilità connesse anche ai profili di sicurezza;

- il consenso dell'interessato, garantendo, in particolare, il requisito della specificità in ordine alle diverse finalità perseguibili (cura, prevenzione e profilassi internazionale);

- l'accesso al FSE da parte dell'interessato, disciplinando l'istituto della delega sia per i profili soggettivi (soggetti delegabili, numero di deleghe consentite) che oggettivi (attività delegabili);

- i trattamenti per finalità di cura, attraverso una definizione puntuale dei diversi profili di autorizzazione all'accesso del FSE, specificando, per ciascuno di essi, le condizioni e i limiti di accesso in linea con i principi di minimizzazione, necessità e pertinenza;

- i trattamenti per finalità di prevenzione, definendo i ruoli del trattamento e introducendo misure volte a delimitare l'accesso ai dati da un punto di vista sia soggettivo, che oggettivo;

- i trattamenti per finalità di profilassi internazionale, indicando la tipologia di soggetti tenuti al "segreto professionale" che possono trattare i dati e di documenti del FSE sulla base di uno specifico e valido consenso dell'interessato, nonché le misure idonee a scongiurare il rischio di re-identificazione.

Lo schema di decreto, corredato della valutazione d'impatto come richiesto dal Garante nell'agosto 2022, ha portato alla previsione di misure di sicurezza specifiche, volte ad assicurare livelli minimi di sicurezza omogenei in ambito nazionale, individuando i criteri per la cifratura e per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali, il soggetto tenuto a effettuare le attività di autorizzazione, di gestione dei privilegi e di profilazione dei soggetti autorizzati in relazione ai diversi modelli architetturali previsti, le misure tecniche adottate con riferimento ai dati soggetti a cd. maggior tutela di anonimato e la possibilità per il personale sanitario di accedere di *default* solo ai FSE degli interessati che abbiano già manifestato il consenso. Particolare attenzione è stata prestata anche ai meccanismi di pseudonimizzazione, dei quali dovrà essere costantemente verificata l'efficacia alla luce dell'evoluzione dello stato dell'arte tecnologico e delle raccomandazioni e delle linee guida via via adottate a livello europeo (es. CEPD, ENISA) e a livello internazionale (es. NIST, ISO).

Lo schema di decreto, oltre a superare tutte le criticità rilevate dal Garante nel 2022, ha presentato anche significativi aspetti di novità con riferimento ai quali, per gli aspetti di protezione dei dati personali, merita evidenziare:

- la possibilità di scelta per le regioni e province autonome di due modelli architetturali di FSE, con conseguenze in ordine all'individuazione della titolarità del trattamento, alla connessa attribuzione dei ruoli del trattamento dei soggetti sanitari a vario titolo coinvolti e, pertanto, anche alle diverse misure tecniche e organizzative da adottare per minimizzare i rischi propri di ciascun modello;

- la previsione secondo cui una determinazione regionale, previa valutazione d'impatto e parere del Garante, può introdurre la conduzione di "gestioni specializzate di dati" del FSE in un'ottica di specificazione delle modalità e delle logiche di organizzazione ed elaborazione che sono individuate – per espressa previsione di

5

legge – con i decreti adottati ai sensi del comma 7 dell'art. 12 del d.l. n. 179/2012, in conformità ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali (cfr. art. 12, comma 6, d.l. n. 179/2012).

Con il richiamato parere dell'8 giugno 2023 il Garante è tornato poi ad affrontare il delicato tema relativo al diritto dell'interessato di opporsi all'alimentazione del FSE con i dati e i documenti sanitari relativi a prestazioni sanitarie erogate prima del 18 maggio 2020 (cfr. parere 7 aprile 2022, doc. web n. 9773977). Il Garante ha infatti preso atto che il decreto sul FSE 2.0 conferma l'onere in capo al Ministero della salute e alle regioni e province autonome di effettuare campagne di informazione in cui evidenziare la facoltà di opposizione da parte dell'interessato (art. 27, comma 1 dello schema di decreto). Tale previsione non è stata ritenuta comunque sufficiente, cosicché il Garante ha prescritto di integrare lo schema di decreto con l'indicazione di un termine entro il quale effettuare la predetta campagna informativa (punto 3.3). Al riguardo, il decreto del FSE 2.0 (adottato – successivamente al parere di giugno – il 7 settembre 2023) è stato integrato con l'indicazione di un termine – 6 mesi dall'entrata in vigore del decreto, poi pubblicato in G.U. il 24 ottobre, ovvero entro il 24 aprile 2024 – entro il quale il Ministero della salute, le regioni e le province autonome dovranno effettuare le campagne di informazione sopra ricordate (cfr. disposizioni transitorie - n. 1).

Nel predetto parere dell'8 giugno 2023 il Garante ha inoltre posto ulteriori condizioni concernenti l'informativa da rendere agli interessati in merito ai trattamenti di dati effettuati attraverso il FSE. In particolare, prendendo atto della previsione di un modello di informativa unico a livello nazionale, l'Autorità ha chiesto di integrare lo schema di decreto con la previsione del parere del Garante su tale modello e con l'indicazione di un termine congruo entro il quale il Ministero della salute, le regioni e le province autonome devono fornire agli interessati le informazioni relative ai trattamenti di dati personali effettuati attraverso il FSE in relazione al modello architeturale dalle stesse adottato.

Al riguardo, il decreto del FSE 2.0 in parola è stato ulteriormente integrato prevedendo il parere dell'Autorità sul modello di informativa (art. 7, comma 4) e l'obbligo di fornire tali informazioni all'interessato da parte del Ministero della salute e delle regioni e province autonome entro 3 mesi dall'entrata in vigore del decreto, ovvero entro il 24 gennaio 2024 (cfr. art. 7, comma 1).

In ottemperanza a quanto richiesto dal citato decreto, il 21 dicembre 2023 il Garante ha espresso il proprio parere favorevole sul modello di informativa per i trattamenti di dati personali effettuati attraverso il FSE 2.0, preventivamente condiviso con la Commissione salute della Conferenza delle regioni e delle province autonome (prov. 21 dicembre 2023, n. 600, doc. web n. 9976886). Tale modello, che sarà utilizzato in tutto il territorio nazionale, illustra, come richiesto dall'Autorità, i presupposti di liceità dei molteplici trattamenti che possono essere effettuati attraverso il FSE, nonché i diversi modelli architettureali che possono essere implementati da regioni/province autonome e che incidono significativamente in ordine all'attribuzione dei ruoli del trattamento. Particolare attenzione è stata prestata anche alle modalità attraverso le quali l'interessato può usufruire dell'istituto della delega ai fini dell'accesso al FSE, nonché esercitare i diritti riconosciuti dal RGPD e dalla specifica disciplina di settore, anche nei confronti dei dati cd. a maggior tutela di anonimato, comprese le conseguenze in caso di revoca del consenso.

Con specifico riferimento a segnalazioni, reclami e notifiche di violazione inerenti al trattamento dei dati personali effettuato attraverso il FSE, si segnalano, in particolare, i provvedimenti sanzionatori adottati nei confronti di una provincia autonoma e di due società designate dalla stessa quali responsabili del trattamento, relativi ad un accesso non autorizzato ai documenti sanitari di alcuni assistiti a causa della

vulnerabilità del servizio relativo al FSE della provincia (cfr. provv. 23 marzo 2023, n. 86, doc. web n. 9883731). In tali provvedimenti è stato evidenziato che, pur considerando che i molteplici trattamenti effettuati nell'ambito del FSE ricadono nella titolarità di più soggetti che perseguono finalità diverse, le attività di trattamento oggetto della violazione rientravano nella sfera di titolarità della provincia autonoma e non dell'azienda sanitaria. Nello specifico, infatti, la violazione risultava essere stata determinata da un non corretto funzionamento del sistema che consentiva l'accesso, senza specifiche limitazioni, ai documenti contenuti nel FSE della provincia autonoma, il quale ricade appunto sotto la titolarità di quest'ultima.

Ciò stante, l'Autorità ha sanzionato la provincia e le due società designate responsabili del trattamento per non aver messo in atto, fin dalla progettazione dei trattamenti effettuati nell'ambito del FSE, misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del RGPD e tutelare i diritti degli interessati, in violazione dell'art. 25 di quest'ultimo.

5.1.2. Il dossier sanitario

Nel 2023 il Garante ha continuato ad occuparsi dei trattamenti di dati sulla salute effettuati attraverso il *dossier* sanitario, con riferimento al quale permangono pienamente in vigore le indicazioni rese con le linee guida 4 giugno 2015 (doc. web n. 4084632). Queste ultime specificano che il *dossier* sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, costituisce un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario sulla base delle informazioni acquisite in occasione della cura del singolo evento clinico.

In merito ai suddetti trattamenti, merita evidenziare due provvedimenti riferiti all'utilizzo di tale strumento durante il periodo dell'emergenza sanitaria da Covid-19.

Nel provvedimento 12 ottobre 2023, n. 473 (doc. web n. 9954220) il Garante ha sanzionato un'azienda sanitaria per la violazione di numerose disposizioni in materia di protezione dei dati personali attraverso un uso del *dossier* sanitario che non rispettava, tra l'altro, la manifestazione di volontà dell'interessato e consentiva l'utilizzo dello stesso al di fuori delle finalità di cura del paziente. Il Garante ha ribadito che, nel caso in cui la condizione di liceità sia rappresentata, come nel caso di specie, dal consenso dell'interessato, questo deve essere prestato attraverso un atto positivo con il quale l'interessato manifesta una volontà libera, specifica, informata e inequivocabile relativa al trattamento dei dati personali che lo riguardano (cons. 32, 42 e 43, artt. 5, 6, par. 1, lett. a) e 7 del RGPD e linee guida 5/2020 sul consenso ai sensi del RGPD, adottate dal CEPD il 4 maggio 2020), non ritenendo pertanto ammissibile la tesi del titolare secondo cui il consenso dell'interessata era desumibile da comportamenti concludenti ("consenso implicito" e "azioni positive inequivocabili").

Nel provvedimento sanzionatorio è stato poi evidenziato che il *dossier*, attesa la sua natura facoltativa e la strutturale incompletezza informativa (cfr. diritto di oscuramento), non può essere utilizzato per finalità riconducibili alla gestione di esigenze organizzative e amministrative del titolare anche nell'ipotesi in cui, come nel caso di specie, il titolare assuma sia la veste di datore di lavoro che di autorità sanitaria che ha in cura l'interessata (cfr. anche provv. 26 maggio 2022, doc. web n. 9791909). Più nello specifico, il trattamento dei dati relativi alla salute dei dipendenti può essere legittimamente effettuato solo quando sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato (art. 9, parr. 2, lett. b) e 4, del RGPD;

5

5

v. pure art. 88 e cons. 51-53 del RGPD). In tale quadro, in assenza di esposte previsioni normative, non è pertanto consentito al datore di lavoro raccogliere e trattare, direttamente dagli interessati o, come nel caso di specie, da altre fonti, dati personali anche relativi allo stato di salute del lavoratore (cfr. FAQ in materia di “Trattamento dei dati nel contesto lavorativo pubblico e privato nell’ambito dell’emergenza sanitaria”, doc. web n. 9337010 e provv. 26 maggio 2022, doc. web n. 9788986).

L’Autorità, pur riconoscendo, le criticità connesse all’organizzazione dei turni ospedalieri del personale sanitario e la delicata situazione legata al contesto pandemico, ha rilevato che l’azienda avrebbe dovuto trattare i dati della reclamante nel rispetto della richiamata normativa di settore che ne costituisce la base giuridica e ne stabilisce limiti e presupposti. Con il medesimo provvedimento, inoltre, il Garante ha chiesto all’azienda di adottare misure correttive relative ai sistemi per il controllo di eventuali anomalie che possano configurare trattamenti illeciti, nonché delle operazioni effettuate sul *dossier*, mediante procedure che prevedano la registrazione automatica in appositi *file* di *log* di tutti gli accessi e delle operazioni compiute.

In materia si richiama anche un provvedimento adottato dal Garante nei confronti di un’azienda sanitaria a seguito dell’accesso, tramite il *dossier* sanitario, al referto Covid-19 di un interessato da parte di un’operatrice sanitaria che non lo aveva in cura (provv. 7 dicembre 2023, n. 587, doc. web n. 9978342).

L’istruttoria ha messo in luce che l’azienda aveva configurato il *dossier* sanitario con modalità tali da consentire a tutto il personale sanitario di accedere a tale strumento informativo con riguardo a qualunque paziente fosse presente nei reparti aziendali o in pronto soccorso. La predetta scelta aziendale, effettuata in relazione all’emergenza da Covid-19, non aveva riguardato solo i pazienti affetti da tale patologia, ma tutti quelli afferenti all’azienda dal marzo 2020 al 2023 e, quindi, ben oltre il termine di cessazione dello stato di emergenza sanitaria (31 marzo 2022). Il Garante ha pertanto rilevato che la scelta effettuata dall’azienda aveva reso di fatto accessibili i *dossier* sanitari di tutti gli assistiti, a prescindere dal coinvolgimento dell’operatore sanitario nel percorso di cura e dalla circostanza che la prestazione sanitaria fosse effettivamente resa ad un paziente Covid-19, e senza neanche prevedere distinte profondità di accesso al *dossier* da parte delle diverse figure abilitate (OSS, medici infermieri, personale di pronto soccorso).

Considerato che all’atto dell’adozione del predetto provvedimento era ancora prevista per gli infermieri e i medici ospedalieri la possibilità di accedere al *dossier* sanitario “senza specifiche limitazioni”, l’Autorità ha ingiunto all’azienda l’adozione di misure correttive volte a limitare l’accesso al solo personale sanitario che verosimilmente può essere coinvolto nel tempo nel processo di cura del paziente, anche sulla base delle prestazioni erogate e dei percorsi clinici attivati, ferma restando la possibilità di accesso ai *dossier* sanitari al ricorrere di specifici eventi (anche emergenziali). Un’ulteriore misura correttiva ha riguardato la necessità per l’azienda di adottare un sistema per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti, ovvero l’utilizzo di indicatori di anomalie (cd. *alert*) volti ad individuare comportamenti anomali o a rischio relativi alle operazioni eseguite dai soggetti autorizzati al trattamento, utili per orientare successivi interventi di *audit*.

5.1.3. La telemedicina

Nel richiamato parere dell’8 giugno 2023 sul FSE 2.0, il Garante è intervenuto sul tema della telemedicina rilevando la necessità di procedere a un aggiornamento delle linee guida per i servizi di telemedicina approvate con decreto del Ministero della salute del 21 settembre 2022 (sul quale non è stato acquisito il previsto parere del Garante) (punto 3.2).

Il decreto del 21 settembre 2022 ha previsto infatti interconnessioni di dati tra il FSE e le infrastrutture di telemedicina nazionale e regionali attraverso funzionalità e sistemi, tra cui l’EDS e il *Gateway*, che erano descritti negli schemi di decreto su cui

5

il Garante ha reso i citati pareri non positivi del 22 agosto 2022 e che invece sono assenti nella nuova disciplina del FSE 2.0. Per gli aspetti relativi alla protezione dei dati personali, l'Autorità ha ritenuto pertanto necessario che quanto previsto nel predetto d.m. sulla telemedicina sia uniformato alle caratteristiche e alle funzionalità del FSE, nonché alle misure a garanzia dei diritti e delle libertà fondamentali degli interessati presenti nel decreto sul FSE adottato il 7 settembre 2023. Contestualmente, il Garante ha rilevato che nelle linee guida sulla telemedicina, in cui non è presente alcun riferimento alla disciplina sul trattamento dei dati personali, non erano stati individuati, come richiesto dal RGPD e dal Codice, gli elementi essenziali del trattamento dei dati sulla salute effettuato attraverso sistemi di telemedicina (artt. 6 e 9 del RGPD e art. 2-*sexies* del Codice).

Alla luce di tali rilievi, il Garante ha chiesto al Ministero, nel citato parere dell'8 giugno 2023, di comunicare tempestivamente le iniziative assunte o che intendesse assumere al fine di conformare le predette linee guida a quanto previsto nello schema di decreto (poi adottato il 7 settembre 2023) nonché nella disciplina sul trattamento dei dati personali. A seguito di quanto osservato nel predetto parere, sono state avviate alcune interlocuzioni con il Ministero della salute e con AGENAS in merito alla definizione degli aspetti di protezione dei dati sopra rilevati e alla realizzazione della piattaforma nazionale sulla telemedicina oggetto degli investimenti del PNRR. La realizzazione della piattaforma presuppone infatti un trattamento di dati sulla salute su larga scala di soggetti interessati vulnerabili, il che può avvenire solo nel pieno rispetto della disciplina sulla protezione dei dati personali.

Il Garante è poi ritornato su tale tematica anche con il parere 22 giugno 2023, n. 284 (doc. web n. 9919981) sul sistema informativo per il monitoraggio dell'assistenza riabilitativa (SIAR), in cui ha preso atto che nella versione dello schema di decreto sottoposto al parere era stato espunto il riferimento alla telemedicina contenuto in una prima bozza. Tale espresso (e soppresso) riferimento era legato alle osservazioni informali formulate dall'Ufficio relative alla necessità di considerare che l'integrazione dell'attività di assistenza riabilitativa con i sistemi di telemedicina impone che i titolari del trattamento svolgano una preventiva valutazione d'impatto ai fini dell'introduzione di misure idonee a ridurre i rischi connessi a tale trattamento, svolto su larga scala nei riguardi di soggetti vulnerabili attraverso l'uso di nuove tecnologie.

Analoghe considerazioni sono state espresse dall'Ufficio e accolte da parte del Ministero nel parere 6 luglio 2023, n. 259 (doc. web n. 9918016) sul sistema informativo per il monitoraggio dell'assistenza domiciliare (SIAD).

Con riferimento ai servizi di telemedicina realizzati dalle singole strutture sanitarie (*app* di telediagnosi, teleconsulto, teleassistenza e telemonitoraggio utilizzate dal personale medico), il Garante anche nel 2023 ha avuto modo di ribadire che l'effettuazione di diagnosi o terapie a distanza non necessita di uno specifico consenso al trattamento dei dati personali dell'interessato, in quanto si tratta di una diversa modalità di svolgimento del rapporto medico-paziente (cfr. in particolare art. 9, parr. 2, lett. h) e 3, del RGPD). Il titolare del trattamento dovrà in ogni caso provvedere a effettuare la valutazione di impatto (art. 35 del RGPD), fornire all'interessato un'informativa completa con riferimento al trattamento dei dati effettuato attraverso le predette *app*, nonché assicurare il rispetto dei principi di integrità, riservatezza ed esattezza dei dati oggetto di trattamento.

5.2. L'uso dell'intelligenza artificiale in sanità

Nell'ambito dei compiti di promozione della consapevolezza riguardo agli obblighi previsti dal RGPD (art. 57, par. 1, lett. d)), il Garante ha adottato nel mese di settembre 2023 il decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di intelligenza artificiale (doc. web n. 9938038), al fine di fornire

5

alcune preliminari indicazioni in ordine ai profili giuridici legati alla protezione dei dati personali e ai connessi aspetti etici da tenere in considerazione in questo ambito (cfr. cap. 16).

Nel decalogo il Garante ha evidenziato che l'elaborazione di dati sulla salute attraverso tecniche di IA richiama i concetti di profilazione e di decisioni sulla base di processi automatizzati e che, ove i relativi trattamenti siano svolti per motivi di interesse pubblico, l'uso di tali strumenti è consentito solo se espressamente previsto dal diritto degli Stati membri, nel rispetto di misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi degli interessati (cons. 71 e art. 22, par. 4, del RGPD) (punto 1).

In base al principio della "protezione dei dati fin dalla progettazione" (art. 25, par. 1, del RGPD), l'Autorità ha esplicitato che nella realizzazione di sistemi di IA in ambito sanitario devono essere adottate misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del RGPD) e integrate nel trattamento le garanzie necessarie per soddisfare i requisiti del RGPD e tutelare i diritti e le libertà degli interessati (punto 2). Tali misure devono garantire – per impostazione predefinita – la proporzionalità del trattamento rispetto all'interesse pubblico perseguito, ponendosi l'obiettivo di ottenere un reale effetto di tutela.

Il terzo punto del decalogo ha riguardato la definizione dei ruoli del trattamento, considerando a tal fine necessaria, anche in un'ottica di *governance* dei dati, una visione complessiva della titolarità del trattamento che tenga conto che l'accesso a un sistema nazionale di IA in ambito sanitario potrebbe essere consentito a una molteplicità di soggetti sulla base di diversi presupposti di liceità e per differenti finalità.

Il Garante ha poi ricordato i tre principi cardine che devono governare l'utilizzo di algoritmi e di strumenti di IA nell'esecuzione di compiti di rilevante interesse pubblico, sulla base delle disposizioni del RGPD e alla luce della recente giurisprudenza del Consiglio di Stato: il principio di conoscibilità, quello di non discriminazione algoritmica e quello di non esclusività (punto 4).

Nel quinto punto del decalogo, il Garante ha richiamato l'attenzione sulla necessità di far precedere da una valutazione di impatto ai sensi dell'art. 35 del RGPD la previsione di un sistema centralizzato a livello nazionale attraverso il quale realizzare servizi sanitari con strumenti di IA, poiché ciò determinerebbe un trattamento sistematico, su larga scala, di particolari categorie di dati personali di cui all'art. 9 del RGPD relativi a soggetti vulnerabili, attraverso l'uso di nuove tecnologie e con un rischio elevato per i diritti e le libertà degli interessati.

Particolare rilievo è stato posto sull'esigenza di garantire elevati parametri di qualità dei dati, considerando che l'uso di informazioni non aggiornate o inesatte potrebbe anche influenzare l'efficacia e la correttezza dei servizi che i suddetti sistemi di IA, che si basano infatti sulla rielaborazione di tali dati, intendono realizzare (punto 6).

Nel richiamare il necessario rispetto dei principi di integrità e riservatezza, il Garante ha poi evidenziato la necessità di assicurare una puntuale descrizione delle logiche algoritmiche utilizzate al fine di "generare" i dati e i servizi attraverso i suddetti sistemi di IA, le metriche utilizzate per addestrare e valutare la qualità del modello di analisi adottato, le verifiche svolte per rilevare la presenza di eventuali *bias* e le misure correttive conseguentemente adottate, le misure idonee a verificare, anche a posteriori, le operazioni eseguite da ciascun soggetto autorizzato e i rischi insiti nelle analisi deterministiche e stocastiche (punto 7).

È stato poi rappresentato, in linea con i documenti internazionali e la giurisprudenza amministrativa, che la trasparenza e la correttezza nei processi decisionali fondati su trattamenti automatizzati costituiscono uno dei pilastri fondamentali da porre alla base dello sviluppo e utilizzo di sistemi di IA alla luce, nell'ambito dell'azione amministrativa, dei correlati rischi, anche discriminatori, che possono

derivare dall'uso di tali strumenti (punto 8).

Nel nono punto del decalogo è stato richiamato che il CEPD, il Garante europeo e lo stesso Garante hanno sottolineato la centralità del concetto di supervisione umana contenuto nella proposta di regolamento sull'IA, evidenziando che l'effettivo coinvolgimento degli esseri umani dovrebbe fondarsi su una supervisione altamente qualificata e sulla liceità del trattamento, al fine di assicurare il rispetto del diritto di non essere assoggettato a una decisione basata esclusivamente su un trattamento automatizzato.

Nell'ultimo punto sono stati richiamati i profili etici e deontologici del trattamento dei dati personali attraverso gli strumenti di IA, evidenziando che la validazione degli algoritmi dovrebbe garantire il miglioramento della qualità delle prestazioni del Servizio sanitario nazionale senza ripercussioni negative in termini sociali, deontologici, etici per l'interessato né per quanto concerne la responsabilità professionale.

Il decalogo è stato trasmesso agli enti di governo sanitario centrale e locale al fine di conformare le progettualità in essere ai principi nello stesso richiamati.

Sul tema dell'IA si menziona anche l'istruttoria avviata a seguito di alcune notizie stampa relative a un progetto regionale pilota volto a creare un supporto alla diagnosi di malattie rare attraverso l'IA.

5

5.3. Trattamenti di dati personali nell'ambito dei sistemi informativi sanitari centrali

Anche nel 2023, il Garante ha continuato a fornire i pareri di competenza con riguardo agli aspetti di protezione dei dati personali connessi all'attuazione dei sistemi informativi sanitari centrali.

In particolare, il Garante è tornato ad affrontare il tema del trattamento dei dati personali effettuato attraverso i dispositivi medici con il parere reso sullo schema di decreto recante disposizioni relative alle modalità di conferimento delle informazioni riguardanti i dati identificativi del fabbricante e l'elenco dei tipi di dispositivi medici su misura messi a disposizione sul territorio nazionale (prov. 27 aprile 2023, n. 186, doc. web n. 9896484). In tale parere, nel prendere atto del periodo di conservazione individuato dal Ministero della salute, il Garante ha ribadito la necessità che il medesimo Ministero preveda che sia inibito, nell'ambito delle attività funzionali alla fornitura o manutenzione dei dispositivi, l'accesso ai dati anagrafici e anamnestici del paziente, salva l'indispensabilità ai fini dell'erogazione del servizio di manutenzione e telediagnosi/teleintervento, rendendo comunque tracciabile ogni operazione di intervento/accesso, anche al fine di dare piena ottemperanza al precedente parere in materia del 26 maggio 2022, n. 189 (doc. web n. 9782450).

Il medesimo richiamo è stato ribadito anche nel parere reso sullo schema di decreto recante tempi di conservazione dei dati personali eventualmente forniti contestualmente alle comunicazioni di incidenti con i dispositivi medici in vitro, attuativo dell'art. 13, comma 9, d.lgs. 5 agosto 2022, n. 138 (prov. 17 maggio 2023, n.192, doc. web n. 9897587).

In relazione ai numerosi sistemi informativi nazionali su base individuale che alimentano il Nuovo sistema informativo sanitario (NSIS) di cui è titolare il Ministero della salute, in via preliminare, l'Ufficio ha chiesto al predetto Dicastero di comprovare, con motivazioni tecnico scientifiche, la necessità di conservare i dati per trenta anni dal decesso dell'assistito. Il Ministero ha rappresentato che, per la valutazione dei percorsi di cura, i dati devono comprendere l'intera vita degli assistiti, incluso l'evento morte, da cui far decorrere un periodo di tempo che, da un lato assicuri un termine uniforme di conservazione per tutti gli interessati, a prescindere dalla durata della loro vita, dall'altro consenta di disporre di una base dati sufficiente per le diverse finalità di analisi sottese a ciascun sistema informativo. L'adeguamento dei

Dispositivi medici

Nuovo sistema informativo sanitario

5

SIAR

flussi NSIS a tale periodo di conservazione si è reso inoltre necessario in base alla disciplina recante l'istituzione dell'Anagrafe nazionale degli assistiti (ANA), che prevede la conservazione dei dati degli assistiti per trent'anni dal decesso (art. 4, comma 4, d.P.C.M. 1° giugno 2022), in quanto nella procedura per l'interconnessione di cui all'art. 3 del decreto del Ministero della salute n. 262/2016 è previsto che ANA fornisca al Ministero della salute il servizio di verifica della validità del codice identificativo e di aggiornamento dei dati.

In relazione ai pareri favorevoli resi in tale ambito si segnala quello sullo schema di decreto volto a istituire il Sistema informativo per il monitoraggio dell'assistenza riabilitativa (SIAR) e sul relativo allegato tecnico (provv. 22 giugno 2023, n. 259, doc. web n. 9918016). Il SIAR trova attuazione nell'ambito dell'assistenza semiresidenziale e residenziale, a carattere intensivo, estensivo e di mantenimento, di cui all'art. 34 del d.P.C.M. 12 gennaio 2017, ed è finalizzato alla raccolta delle informazioni delle regioni e province autonome relative ai trattamenti riabilitativi, previa valutazione multidimensionale dell'assistito e presa in carico, e al progetto riabilitativo individuale (PRI). Il SIAR consente, da un lato, alle regioni e province autonome analisi comparative in materia di trattamenti riabilitativi, sulla base di indicatori calcolati previa aggregazione dei dati a livello aziendale su base annuale, e, dall'altro, al Ministero della salute di consultare le informazioni rese disponibili dal Sistema.

Nel SIAR confluiscono informazioni non direttamente identificative riferite all'erogatore del servizio di assistenza riabilitativa e all'assistito, cui si applica la procedura di interconnessione di cui al d.m. n. 262/2016, secondo le regole indicate nello schema di disciplinare tecnico che definisce altresì modalità, cadenza e tempi di raccolta e trasmissione delle stesse.

SICOF

Un altro importante parere relativo ai sistemi sanitari centrali ha riguardato lo schema di decreto volto a istituire il Sistema informativo per il monitoraggio delle attività erogate dai consultori familiari (SICOF) (provv. 22 giugno 2023, n. 260, doc. web n. 9918033). Tale sistema informativo, la cui gestione è affidata al Ministero della salute, in qualità di titolare del trattamento, trova attuazione in riferimento alle prestazioni erogate dai consultori familiari, istituiti dalla l. n. 405/1975. Il SICOF consente alle regioni e alle province autonome di monitorare le prestazioni erogate dai consultori familiari, nonché i livelli essenziali e uniformi di assistenza, attraverso analisi comparative in materia di assistenza sanitaria e socio-sanitaria, sulla base di indicatori calcolati previa aggregazione dei dati a livello aziendale su base annuale.

Il Sistema permette inoltre al Ministero della salute di consultare le informazioni rese disponibili nella medesima forma dal Sistema. Le informazioni non direttamente identificative, riferite all'erogatore del servizio di assistenza sanitaria e socio-sanitaria offerta dai consultori e all'assistito, sono trasmesse dalle regioni e dalle province autonome e sottoposte a verifica da parte del Ministero in ordine alla completezza e alla qualità. Anche con riferimento al SICOF si applica la procedura di interconnessione di cui al d.m. n. 262/2016.

SIAD

Rileva in tale ambito anche il parere reso sullo schema di decreto del Ministro della salute di modifica del decreto del Ministro del lavoro, della salute e delle politiche sociali del 17 dicembre 2008, recante istituzione del Sistema informativo per il monitoraggio dell'assistenza domiciliare (SIAD) (provv. 6 luglio 2023, n. 284, doc. web n. 9919981). La modifica trae origine dall'esigenza rappresentata dal Ministero della salute di integrare il flusso SIAD già esistente con i dati relativi alle cure palliative domiciliari e alle cure domiciliari di livello base, al fine di avere una base informativa omogenea tra le regioni utilizzabile per il calcolo degli indicatori del PNRR per l'assistenza domiciliare previsti nell'Investimento 1.2 "Casa come primo luogo di cura e telemedicina" della Missione 6, Componente 1 del PNRR.

Si segnala, sempre in tale ambito, il parere reso sullo schema di decreto del Ministro del lavoro, della salute e delle politiche sociali, di modifica del decreto 17 dicembre 2008 recante istituzione del Sistema informativo per il monitoraggio delle prestazioni erogate nell'ambito dell'assistenza sanitaria in emergenza-urgenza (provv. 6 luglio 2023, n. 283 doc. web n. 9919963).

Nel corso dell'istruttoria avviata dall'Ufficio, il Ministero ha comprovato con motivazioni tecnico-scientifiche la necessità di attribuire al sistema informativo anche la finalità di consentire l'allerta rapida relativa alle sindromi respiratorie, in base agli accessi in pronto soccorso. Lo schema di decreto e il relativo disciplinare tecnico hanno tenuto conto delle osservazioni formulate dall'Ufficio nel corso delle interlocuzioni informali che hanno riguardato, in particolare, la necessità di indicare nello schema di decreto i riferimenti normativi che attribuiscono al Ministero della salute specifiche competenze in materia di contrasto di ogni emergenza sanitaria, nonché ogni iniziativa volta alla cura delle patologie epidemico-pandemiche emergenti, di specificare i livelli di aggregazione dei dati contenuti nel sistema previsti per l'accesso da parte delle direzioni del Ministero, e di indicare nel disciplinare che il sistema non consente l'accesso a enti esterni al Ministero a eccezione dell'Istituto superiore di sanità in qualità di responsabile del trattamento.

L'Autorità ha pertanto espresso, nei termini previsti, il parere favorevole di competenza senza formulare osservazioni, evidenziando che esso veniva rilasciato su un testo in corso di revisione e che, qualora fossero state introdotte modifiche circa la tipologia dei dati raccolti o le operazioni effettuate, sarebbe stato necessario modificare lo schema di decreto in esame e acquisire un nuovo parere dell'Autorità.

Da ultimo, si segnala il parere sullo schema di decreto del Ministro della salute relativo al Sistema informativo nazionale per le dipendenze (SIND) che abroga e sostituisce il decreto del Ministro della salute 11 giugno 2010, incluso tra i sistemi informativi del Servizio sanitario nazionale interconnessi ai sensi del d.m. n. 262/2016 (provv. 12 ottobre 2023, n. 471, doc. web n. 9947458).

In particolare, in tale parere il Garante ha evidenziato che il trattamento dei dati personali dei detenuti attraverso il predetto Sistema, in quanto dati relativi a condanne penali e reati di cui all'art. 10 del RGPD, è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che preveda garanzie appropriate per i diritti e le libertà degli interessati. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti di tali dati e le relative garanzie sono individuati con decreto del Ministro della giustizia; tuttavia, in relazione al caso di specie il decreto suddetto non è stato adottato, sebbene il Garante, il 24 giugno 2021, abbia adottato il parere su uno schema di regolamento recante l'individuazione dei trattamenti di dati personali relativi a condanne penali e reati e delle relative garanzie appropriate ai sensi dell'art. 2-*octies*, comma 2, del Codice (doc. web n. 9682603, cfr. anche parere 30 giugno 2022, n. 237 doc. web n. 9794929).

Al riguardo, il Garante ha inoltre evidenziato che la rilevazione nel SIND della condizione di detenuto non poteva ritenersi legittimata dalla disciplina di riforma della sanità penitenziaria (l. n. 418/1998, d.lgs. n. 230/1999 e d.P.C.M. 1° aprile 2008), che prevede l'istituzione del Sistema informativo nazionale sulla salute dei detenuti e dei minori sottoposti a provvedimento penale, nell'ambito del NSIS del Ministero della salute, in quanto la citata disposizione normativa prevede la raccolta del dato giudiziario nell'ambito del sistema informativo sulla salute dei detenuti e non anche nel SIND, che riguarda le dipendenze.

Nel corso delle interlocuzioni, anche informali, il Ministero ha recepito le osservazioni formulate dall'Ufficio, espungendo la variabile relativa all'assistito detenuto dai dati raccolti dal SIND e fornendo assicurazioni in merito al tracciato denominato "Monitoraggio HIV" che rileva solo dati aggregati relativi all'esecuzione del

**Monitoraggio
prestazioni in
emergenza-urgenza**

SIND

5

Ricette transfrontaliere

test sierologico HIV da parte degli utenti del Servizio per le dipendenze (SerD), in cui non sono presenti variabili di natura anagrafica. È stato inoltre precisato che la produzione di analisi statistiche e indicatori statistici sul fenomeno dell'assistenza sanitaria a persone con dipendenze o con comportamenti a rischio è a cura dell'ufficio di statistica del Ministero della salute, in conformità alle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale adottate con provvedimento del Garante 19 dicembre 2018, n. 514 (doc. web n. 9069677) e riportate nell'all. A del d.lgs. n. 196/2003.

Accanto ai richiamati pareri favorevoli è stato espresso anche un parere negativo sullo schema di decreto del Ministero della salute, da adottare di concerto con il MEF, concernente la definizione delle caratteristiche e dei contenuti delle prescrizioni dei medicinali rilasciate nel territorio italiano su richiesta di un paziente che intenda utilizzarle in uno Stato membro ai sensi dell'art. 12, comma 9, d.lgs. n. 38/2014 (cd. ricetta transfrontaliera) (provv. 26 gennaio 2023, n. 24, doc. web n. 9856677). In tale parere il Garante ha rilevato significative criticità in ordine all'individuazione della titolarità dei trattamenti successivi alla generazione della ricetta transfrontaliera effettuata dal medico prescrittore, con riguardo alle attività necessarie all'utilizzo della ricetta all'estero e al controllo della regolarità della stessa.

Ulteriori criticità sono state ravvisate nelle informazioni da rendere all'interessato, nonché nell'assenza dell'individuazione delle misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati, delle operazioni eseguibili e del motivo di interesse pubblico rilevante perseguito. Le disposizioni esaminate inoltre sono risultate non coerenti con la disciplina sul FSE e alla luce dei rilievi già effettuati al riguardo nel citato parere del 22 agosto 2022. Ulteriori rilievi hanno riguardato l'assenza di garanzie sul rispetto dei parametri relativi alla qualità dei dati trattati e l'indeterminatezza del relativo periodo di conservazione, nonché gli aspetti di sicurezza del trattamento connessi anche all'assenza di una preventiva valutazione d'impatto.

5.4. Trattamenti per finalità di cura e amministrative correlate alla cura

5.4.1. Provvedimenti derivanti da data breach

Numerose istruttorie avviate dall'Autorità hanno riguardato, nel 2023, condotte di cui il Garante è venuto a conoscenza ricevendo notifiche di violazione di dati personali, comunicate dai titolari del trattamento ai sensi dell'art. 33 del RGPD. In un numero considerevole di casi le istruttorie hanno avuto come esito provvedimenti sanzionatori.

Una di esse ha riguardato la condotta di un'azienda sanitaria e, in particolare, l'unità di cardiocirurgia, che aveva inviato un'e-mail, in copia conoscenza, ai pazienti in attesa di trapianto cardiaco, nell'ambito dell'acquisizione dei consensi informati per l'adesione a uno studio clinico, attraverso modelli da compilare e sottoscrivere. Nell'esaminare la questione, l'Autorità ha ricordato che gli indirizzi e-mail sono riconducibili alla nozione di dato personale, anche se privi di riferimenti al nome e al cognome o comunque ad altre informazioni direttamente identificative degli interessati; ha, inoltre, evidenziato che dal contesto della comunicazione poteva desumersi che i destinatari dell'e-mail erano pazienti in attesa di trapianto cardiaco, cosicché il trattamento descritto aveva riguardato dati sanitari in quanto concernenti informazioni relative a prestazioni di assistenza sanitaria, che rivelano informazioni sullo stato di salute (art. 4, par. 1, n. 15 del RGPD). È stato, pertanto, evidenziato che tale invio aveva, di fatto, senza giustificato motivo e in assenza di presupposto giuridico, realizzato una comunicazione di dati personali e relativi alla salute degli

interessati (cui afferiscono gli indirizzi *e-mail*), in violazione dei principi base di cui agli artt. 5, par. 1, lett. f) e 9 del RGPD. L'Autorità ha conseguentemente adottato un provvedimento sanzionatorio nei confronti dell'azienda, considerando al riguardo una serie di elementi, tra i quali il fatto di avere preso conoscenza dell'evento a seguito della notifica di violazione dei dati effettuata dal titolare, il numero degli interessati (19), e l'insussistenza di atteggiamenti intenzionali da parte dell'azienda; la violazione era avvenuta infatti per l'errore compiuto da una dipendente nella fase di inserimento dei destinatari nello specifico campo della *e-mail*, nell'ambito di una procedura temporanea, adottata nel periodo pandemico per evitare, per la consegna della documentazione, la convocazione in presenza dei pazienti fragili destinatari della *e-mail* (provv. 11 gennaio 2023, n. 7, doc. web n. 9861356).

Altra vicenda di *data breach* ha riguardato l'illecita comunicazione di dati relativi alla salute posta in essere da un'azienda sanitaria per avere inserito, non intenzionalmente, documentazione sanitaria di un paziente in una cartella clinica relativa a diverso paziente – e a quest'ultimo consegnata – in assenza di un idoneo presupposto giuridico. L'azienda è stata sanzionata dal Garante per la violazione dei principi di base del trattamento di cui agli artt. 5 e 9 del RGPD e degli obblighi in materia di sicurezza di cui all'art. 32 del RGPD medesimo (provv. 26 gennaio 2023, n. 26, doc. web n. 9861289).

Il Garante, a seguito di due notificazioni di *data breach* effettuate da un'azienda sanitaria, titolare del trattamento, a distanza di pochi giorni e riguardanti, entrambe, l'errata consegna di referti radiologici, dopo aver disposto la riunione dei procedimenti in considerazione dell'analogia tra le due vicende, ha adottato un provvedimento sanzionatorio nei confronti di tale azienda. Nello specifico, l'azienda aveva – a causa dell'errore dell'operatore nella fase dell'imbustamento dei referti – consegnato alcuni referti (riferiti, complessivamente, nelle due vicende, a n. 4 pazienti) a soggetti terzi (due nel primo caso di *data breach* e due nel secondo caso) non autorizzati a riceverli. Tale condotta aveva integrato una comunicazione illecita di dati relativi alla salute, in quanto avvenuta in assenza di un presupposto giuridico che legittimasse la conoscenza delle predette informazioni da parte dei destinatari, in violazione dei principi di base di cui all'art. 5, lett. f) e all'art. 9 del RGPD, nonché degli obblighi di sicurezza dei dati personali di cui all'art. 32 del RGPD medesimo (provv. 26 ottobre 2023, n. 500, doc. web n. 9964729).

In un altro caso, un'azienda socio-sanitaria territoriale aveva notificato all'Autorità tre violazioni di dati personali, concernenti la comunicazione di dati sulla salute a soggetti non autorizzati a riceverla, avvenuta in distinte occasioni. In particolare, nel primo caso, la comunicazione conteneva una convocazione a visita da parte della commissione aziendale per la valutazione dell'invalidità civile, oltre che del soggetto autorizzato, anche di altre due persone; nel secondo, era stato inserito, nel campo denominato copia conoscenza, l'indirizzo di 198 destinatari, nell'invio di una *e-mail* proveniente dal Centro sclerosi multipla dell'azienda e avente a oggetto le “raccomandazioni aggiornate su Covid in pazienti affetti da sclerosi multipla”; nel terzo, era stata consegnata ad un paziente documentazione sanitaria contenente anche l'esito di un esame effettuato da un soggetto terzo. Tenuto conto che le violazioni oggetto di notifica ai sensi dell'art. 33 del RGPD avevano riguardato il medesimo titolare del trattamento in relazione a fattispecie analoghe, è stata disposta la riunione dei 3 procedimenti istruttori.

L'Autorità ha chiarito che i dati oggetto di comunicazione avevano riguardato, in tutti i casi, informazioni sulla salute degli interessati, evidenziando che, alla luce della descritta riconducibilità degli indirizzi *e-mail* alla nozione di dato personale, la circostanza per la quale dal contesto delle comunicazioni poteva desumersi che i destinatari erano pazienti in cura presso il Centro sclerosi multipla aveva comportato il

5

5

trattamento di informazioni relative alla salute, secondo la definizione dell'art. 4, par. 1, n. 15 del RGPD, anche se non era stata fornita alcuna indicazione sullo stato di gravità o di malattia del paziente (cfr., in tal senso, provv.ti 13 maggio 2021, n. 206, doc. web n. 9688020; 16 settembre 2021, n. 328, doc. web n. 9722297; 28 aprile 2022, n. 164, doc. web n. 9779057; 7 luglio 2022, n. 242, doc. web n. 9809998; 11 gennaio 2023, n. 7, doc. web n. 9861356). Tale conclusione è valsa anche in relazione alla convocazione a visita da parte della commissione aziendale per la valutazione dell'invalità civile, sulla base della documentazione sanitaria prodotta dagli interessati.

Nell'adottare il provvedimento correttivo, l'Autorità ha tenuto conto del numero di interessati coinvolti (circa 200); del fatto che non erano pervenuti reclami o segnalazioni sull'accaduto, essendo venuta a conoscenza degli eventi a seguito delle notifiche di violazione dei dati personali effettuate dal titolare; dell'introduzione di misure volte a ridurre la replicabilità degli eventi occorsi. Si è considerato, altresì, che i fatti si erano verificati, in un caso, nell'ambito dello svolgimento della campagna vaccinale e della necessità di fornire, immediatamente e in modo più agevole possibile, le informazioni relative alle raccomandazioni aggiornate sul Covid-19 in pazienti affetti da sclerosi multipla; in un altro, nell'ambito delle attività volte a incrementare, cessato lo stato di emergenza da Covid-19, i volumi delle attività e i ritmi di lavoro, al fine di far fronte alle lunghe liste di attesa determinatesi a seguito della sospensione e del rallentamento delle attività durante il periodo pandemico (provv. 18 luglio 2023, n. 316, doc. web n. 9935484).

In un'altra circostanza, l'istruttoria è stata avviata a seguito di una notifica di violazione di dati personali da parte di un ente che aveva dichiarato di aver erroneamente gestito una fattura relativa a prestazioni psichiatriche sia nella fase dell'intestazione che in quella dell'invio, entrambe effettuate nei confronti di soggetto diverso dall'interessato, omonimo. Nella vicenda illustrata, il Garante ha inteso valutare la violazione come minore, considerati taluni elementi, tra i quali: l'assenza di precedenti violazioni commesse dall'ente, l'elevato grado di cooperazione sin da subito prontamente dimostrato durante tutta la fase istruttoria e procedimentale, la circostanza che la comunicazione di dati sulla salute aveva riguardato un solo interessato e che la violazione era stata determinata da un errore di una dipendente, comunque sottoposta a procedimento disciplinare. Il Garante si è, pertanto, limitato ad ammonire il titolare del trattamento, ritenendo che tale tipologia di provvedimento potesse assolvere una funzione correttiva proporzionata, risultando anche una misura effettiva e dissuasiva (provv. 14 settembre 2023, n. 399, doc. web n. 9939623).

In molte circostanze le violazioni di dati comunicate dai titolari sono dipese da inadeguate misure di sicurezza. In particolare, un'azienda ha notificato una violazione avente a oggetto la comunicazione effettuata via posta ordinaria a un numero molto elevato di assistiti (39.852) di documentazione loro indirizzata, ma contenente il certificato, concernente una terza persona, di esenzione dalla partecipazione alla spesa sanitaria per motivi di reddito rilasciato dalla regione.

Sulla medesima questione l'Autorità ha ricevuto anche alcuni reclami da parte dei medesimi assistiti. In tale occasione il Garante, nell'adottare un provvedimento sanzionatorio per il descritto trattamento concernente solo dati comuni e avvenuto in violazione degli artt. 5, 6 e 32 del RGPD, non ha previsto misure correttive, considerato che l'azienda aveva inviato agli assistiti coinvolti il certificato di esenzione corretto a mezzo posta ordinaria e aveva chiesto di distruggere quello precedentemente ricevuto; l'Autorità ha, altresì, considerato l'elevato grado di cooperazione durante la fase istruttoria e procedimentale, la circostanza che il trattamento aveva riguardato un numero molto elevato di interessati, ma aveva comportato la comunicazione dei dati di un interessato a un unico soggetto diverso e, in ogni caso, che la scelta di procedere con l'invio massivo al domicilio degli assistiti dei certificati di esenzione era

stata assunta, nel contesto emergenziale da pandemia da Covid-19, al fine di evitare l'accesso in sede degli utenti e scongiurare in tal modo gli assembramenti presso gli sportelli dell'azienda (prov. 17 maggio 2023, n. 197, doc. web n. 9899929).

Un altro fronte sul quale l'Autorità è stata fortemente impegnata in rapporto alle notifiche di *data breach* è stato quello della sicurezza informatica.

In particolare, un'azienda sanitaria aveva comunicato una violazione di dati sulla salute a seguito di un attacco *ransomware* che, attraverso un virus, aveva limitato l'accesso al *database* della struttura sanitaria e per il quale era stato richiesto un riscatto al fine di ripristinare il funzionamento dei sistemi.

Diverse le criticità rilevate dal Garante durante l'istruttoria sull'accaduto, nell'ambito della quale si è resa necessaria anche un'attività ispettiva per verificare le misure tecniche e organizzative adottate dall'azienda sia prima che dopo l'attacco subito. In particolare, dall'esame delle informazioni e degli elementi acquisiti nonché della documentazione fornita dall'azienda, è emerso che il trattamento era stato effettuato in violazione della disciplina in materia di protezione dei dati personali, toccando molteplici profili. In primo luogo, è emersa una gestione inadeguata degli allarmi volti a rilevare l'incidente, che non aveva consentito all'azienda di venire tempestivamente a conoscenza della violazione dei dati personali occorsa. Ciò ha configurato una violazione delle disposizioni di cui all'art. 5, par. 1, lett. f) e all'art. 32, par. 1, del RGPD anche alla luce delle linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD, adottate dal CEPD il 28 marzo 2023 (punto n. 41). È emerso, altresì, che l'azienda non aveva adottato adeguate misure per segmentare e segregare le reti su cui erano attestate le postazioni di lavoro dei propri dipendenti nonché i sistemi (*server*) utilizzati per i trattamenti e che, al momento in cui si era verificata la violazione dei dati personali, l'accesso remoto alla rete dell'azienda, tramite VPN, era avvenuto mediante una procedura di autenticazione informatica basata solo sull'utilizzo di *username* e *password*.

La mancata adozione di misure adeguate a garantire la sicurezza delle reti, sia in relazione alla mancata segmentazione e segregazione delle stesse, che aveva causato la propagazione del *virus* all'intera infrastruttura informatica, sia con riferimento all'accesso remoto tramite VPN, non è risultata conforme alle disposizioni di cui agli artt. 5, par. 1, lett. f) e 32, par. 1, del RGPD, secondo le quali il titolare e il responsabile del trattamento devono mettere in atto misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento. Infine, alla luce di quanto emerso e, in particolare, della mancata adozione di misure e garanzie adeguate ad attuare efficacemente il principio di "integrità e riservatezza" e a proteggere da trattamenti non autorizzati o illeciti, sono stati ravvisati, altresì, gli estremi di una violazione del principio della "protezione dei dati fin dalla progettazione", di cui all'art. 25, par. 1, del RGPD, considerati i rischi per i diritti e le libertà degli interessati derivanti dai trattamenti in esame, in relazione alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Nel sanzionare l'illecito il Garante ha tenuto conto del fatto che il *data breach* ha riguardato dati idonei a rivelare informazioni sulla salute di un numero molto rilevante di interessati (842.000 tra assistiti e dipendenti), ma anche dell'atteggiamento non intenzionale e estremamente collaborativo dell'azienda, in ogni fase dell'istruttoria, ivi compresa quella ispettiva. Dopo l'accaduto, l'azienda ha adottato una serie diversificata di misure volte non solo ad attenuare il danno subito dagli interessati, ma anche a ridurre la replicabilità dell'evento stesso, tra le quali l'attivazione di una procedura di accesso alla rete tramite VPN con doppio fattore di autenticazione (prov. 28 settembre 2023, n. 426, doc. web n. 9941232).

Si segnala, infine che, nel corso dell'anno, in materia di sicurezza, sono stati effettuati alcuni accertamenti ispettivi anche presso altre aziende sanitarie che avevano notificato violazioni di dati personali, a seguito di attacchi *ransomware* (cfr. cap. 17).

5

5

Violazioni di dati personali

5.4.2. Provvedimenti derivanti da reclami e segnalazioni

Anche nell'anno di riferimento il Garante ha avviato numerose istruttorie a seguito di specifici reclami e segnalazioni, alcune delle quali hanno riguardato la violazione dei principi di base del trattamento e si sono concluse con l'adozione di provvedimenti correttivi.

Il Garante, in un caso oggetto di segnalazione, ha sanzionato un'azienda ospedaliera calabrese per la violazione degli artt. 5, par. 1, lett. a) ed f) e 9 del RGPD e degli obblighi in materia di sicurezza di cui all'art. 32 del RGPD medesimo, nonché dell'art. 75 del Codice, che fa salve le specifiche disposizioni di settore. È stata infatti accertata, al termine dell'istruttoria, la responsabilità dell'azienda per aver inviato, a mezzo di posta elettronica e nell'inosservanza delle misure indicate nell'all. A del d.P.C.M. 8 agosto 2013, un referto riguardante una paziente a un soggetto terzo non autorizzato e, pertanto, in assenza di presupposto giuridico che legittimasse tale comunicazione di dati relativi alla salute (provv. 26 gennaio 2023, n. 25, doc. web n. 9863050).

Si segnala, a seguito di un reclamo di una paziente, l'avvio di una istruttoria nei confronti di un'azienda socio-sanitaria locale che, nell'intenzione di trasmettere una *e-mail* alla reclamante, l'aveva inviata ad un indirizzo *e-mail* non riferibile alla stessa. La *e-mail* conteneva, in allegato, un provvedimento con il quale l'ufficio ricoveri *extra* regione dell'azienda sanitaria autorizzava il ricovero *extra* regione della reclamante. Tale documento conteneva, oltre ai dati identificativi della reclamante, anche l'indicazione dell'istituto ospedaliero presso il quale effettuare le cure mediche e una serie di altri elementi, come, ad esempio, la presenza dell'accompagnatore. A seguito dell'esame della vicenda, è emersa l'illiceità del trattamento di dati personali e sulla salute effettuato dall'azienda, per aver trattato dati personali in violazione dei principi di base del trattamento cui agli artt. 5 e 9 del RGPD nonché degli obblighi in materia di sicurezza di cui all'art. 32 del RGPD. Nel provvedimento sanzionatorio, adottato nei confronti dell'azienda, è stato tenuto conto del fatto che il trattamento aveva riguardato un solo interessato, che la violazione era avvenuta per errore nella individuazione della documentazione da allegare alla *e-mail* e che il titolare aveva dimostrato un elevato grado di cooperazione con l'Autorità (provv. 23 marzo 2023, n. 85, doc. web n. 9872621).

Molti provvedimenti hanno riguardato casi di diffusione di dati sanitari.

A seguito di una segnalazione, il Garante ha adottato un provvedimento sanzionatorio nei confronti di un'azienda sanitaria che aveva pubblicato, sul proprio sito internet, i documenti contenenti gli elogi ricevuti dai pazienti in relazione alle prestazioni ricevute per la cura di specifiche patologie dai quali – nella quasi totalità dei casi – era possibile identificare i pazienti stessi, in quanto i dati anagrafici erano stati cancellati in modo approssimativo con il tratto di un pennarello nero che tuttavia non impediva di leggere le parti oscurate (provv. 12 marzo 2023, n. 74, doc. web n. 9870171). In particolare, l'Autorità ha rappresentato che la procedura di cancellazione manuale con pennarello o con bianchetto, per sua natura imprecisa e non definitiva, non può essere ritenuta idonea a rendere anonime le informazioni personali degli interessati, né può definirsi una procedura di pseudonimizzazione, anche laddove eseguita in modo efficace, essendo piuttosto una semplice procedura manuale di oscuramento delle generalità degli interessati (cfr. al riguardo i provv. ti 17 settembre 2020, docc. web nn. 9479364 e 9479382). Il Garante ha inoltre rilevato che i dati pubblicati sul sito dell'ASL non rispettavano il principio di minimizzazione, in quanto la pubblicazione dell'elogio come presentato dall'interessato aveva comportato la diffusione di dati sulla salute (es. dettagli clinici) non pertinenti rispetto allo scopo perseguito nello specifico, riconducibile all'attività "di comunicazione e di informazione al miglioramento dei rapporti con gli utenti".

Un'altra azienda sanitaria è stata sanzionata dal Garante per aver diffuso dati sulla

Diffusione di dati sanitari

salute di un paziente mediante l'affissione al di fuori dei locali del pronto soccorso di un cartellone relativo alle attività sanitarie prestate dall'azienda in cui erano visibili i dati personali di tale paziente (provv. 1° giugno 2023, n. 227, doc. web n. 9917728). Nel suo provvedimento il Garante ha ricordato che è vietata la pubblicazione di qualsiasi informazione da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici. A tale scopo, fin dalla fase di redazione degli atti e dei documenti oggetto di pubblicazione, pur nel rispetto del principio di adeguata motivazione, non devono essere inseriti dati personali "eccedenti", "non pertinenti", "non indispensabili" (e, tantomeno, "vietati") (cfr. anche linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, parte II, par. 1, del 15 maggio 2014, doc. web n. 3488002).

Un ulteriore caso ha riguardato l'avvenuta pubblicazione su alcune testate giornalistiche, anche *online*, di immagini di documentazione sanitaria relative a un soggetto da tempo ricercato dalle Forze dell'ordine. Nel corso dell'istruttoria è stato appurato che sulla vicenda era stata presentata una denuncia alla Procura della Repubblica relativa al fatto che l'azienda sanitaria che aveva emesso i referti diffusi non aveva consegnato copie degli stessi a soggetti diversi dall'interessato e che il personale sanitario autorizzato al trattamento si era dichiarato estraneo alla diffusione dei dati (comunicato stampa 18 gennaio 2023, doc. web n. 9845388 e nota 28 giugno 2023).

Il Garante ha altresì sanzionato una azienda sanitaria in relazione alla presenza, nei locali di un *ex* sanatorio, di documentazione sanitaria (es. ricette, cartelle cliniche e radiografie) in stato di abbandono e accessibile a chiunque (provv. 28 settembre 2023, n. 424, doc. web n. 9946386). Nel provvedimento l'Autorità ha ricordato che la disciplina di settore individua termini di conservazione specifici che le strutture sanitarie devono rispettare in relazione alla tipologia documentazione sanitaria in loro possesso (cfr. *ex multis*, circolare del Ministero della sanità 19 dicembre 1986, n. 900; art. 5 del d.m. 18 febbraio 1982; art. 4 del d.m. 14 febbraio 1997; d.m. 3 agosto 2001; d.lgs. n. 200/2007; d.P.R. n. 445/2000; d.lgs. n. 42/2004; d.lgs. n. 82/2005; d.lgs. n. 502/1992). Laddove non vi sia una specifica disposizione normativa che individui i tempi di conservazione di un documento contenente dati personali, spetta al titolare del trattamento individuare un termine di conservazione congruo per il raggiungimento delle finalità legittimamente perseguite, che deve essere tra l'altro indicato nelle informazioni da rendere all'interessato ai sensi dell'art. 13 del RGPD.

Il Garante ha rilevato che, sebbene l'azienda avesse adottato il regolamento aziendale sulla conservazione di documentazione (cd. massimario di scarto), aveva poi lasciato in stato di abbandono copiosa documentazione sanitaria, che avrebbe dovuto essere conservata nei tempi e secondo le modalità indicate nel predetto regolamento, in contrasto con i principi di integrità e riservatezza dei dati, nonché di liceità, correttezza e trasparenza e di limitazione della conservazione di cui all'art. 5 del RGPD.

In un altro caso, un reclamante aveva lamentato la diffusione sul web da parte di un'azienda sanitaria di sue informazioni personali (data di nascita, residenza, codice fiscale) nonché dati relativi alla salute. In particolare era stata diffusa una nota del servizio di assistenza farmaceutica territoriale dell'azienda, avente a oggetto la richiesta di acquisto di un medicinale, unitamente a un certificato con il quale si accertava la patologia di cui il reclamante era affetto e i farmaci di cui lo stesso aveva bisogno. Nel provvedimento sanzionatorio adottato nei confronti dell'azienda per aver effettuato un trattamento di dati sulla salute in violazione dei principi di base del trattamento di cui agli artt. 5, 6 e 9 del RGPD nonché dell'art. 2-*septies*, comma 8,

5

5

del Codice, si è ritenuto di non dover adottare misure correttive, in quanto l'azienda aveva provveduto alla immediata deindicizzazione dei dati personali erroneamente diffusi, rimuovendoli dai contenuti dell'indice dei motori di ricerca (prov. 13 aprile 2023, n. 126, doc. web n. 9891029).

Analoga violazione relativa ad una diffusione dei dati sanitari è stata accertata nei confronti di un'azienda sanitaria che aveva divulgato le informazioni sulla salute della reclamante affiggendo, presso il cancello di ingresso dell'ambulatorio dove la stessa svolgeva attività di medico igienista, un cartello in cui si avvisava l'utenza che in una specifica data non sarebbe stata garantita la seduta vaccinale per esigenze di servizio derivanti dalla sua malattia. Secondo l'azienda, che aveva tempestivamente rimosso e sostituito il cartello recante l'avviso nel quale erano indicate le informazioni della reclamante, l'episodio, non intenzionale, era stato determinato da una incomprensione tra chi aveva dato la disposizione di segnalare all'utenza l'impossibilità di eseguire la prestazione che era in attesa di ricevere e chi effettivamente aveva eseguito detta segnalazione. Il provvedimento sanzionatorio adottato nei confronti dell'azienda per aver diffuso dati relativi alla salute della dottoressa, in violazione dei principi base di cui agli artt. 5 e 9 del RGPD, nonché dell'art. 2-*septies*, comma 8, del Codice ha considerato la mancanza di intenzionalità e il ridotto arco temporale in cui è perdurata la violazione (prov. 8 giugno 2023, n. 242, doc. web n. 9917883).

In un altro caso, a seguito di un reclamo, il Garante, ha adottato un provvedimento di ammonimento e correttivo nei confronti di un osteopata che aveva effettuato un trattamento illecito di dati sulla salute, in violazione delle disposizioni contenute negli artt. 5, par. 1, lett. a), 6, 9, 12 e 13, del RGPD. Dalla documentazione in atti, è emerso che il titolare del trattamento aveva effettuato una comunicazione dei dati sulla salute della reclamante a soggetti terzi senza un idoneo presupposto giuridico, violando altresì i principi di correttezza e trasparenza. L'osteopata, infatti, nonostante l'esplicita opposizione della reclamante, aveva utilizzato i dati sanitari di quest'ultima per realizzare una tesina che era stata poi consegnata alla scuola di formazione e al relatore. Il professionista sanitario inoltre aveva ripetutamente negato di aver utilizzato per la tesi il caso clinico che riguardava l'interessata e aveva fornito alla stessa un'informativa priva degli elementi essenziali di cui all'art. 13 del RGPD (prov. 26 ottobre 2023, n. 497, doc. web n. 9954241). Nel provvedimento il Garante si è soffermato sul fatto che la tesi recava numerose informazioni cliniche e anamnestiche mediante le quali era possibile identificare l'interessata, anche se indirettamente, e ha colto l'occasione per ribadire come la procedura di cancellazione manuale non possa essere definita idonea a rendere anonime le informazioni personali, né può definirsi una procedura di pseudonimizzazione ai sensi della definizione di cui all'art. 4, n. 4 del RGPD (cfr. al riguardo prov. 2 marzo 2023, n. 74, doc. web n. 9870171, cit.).

Il Garante ha inoltre richiamato quanto indicato nel codice di condotta per l'utilizzo dei dati sulla salute a fini didattici e di pubblicazione scientifica, approvato con il provvedimento del Garante 14 gennaio 2021, n. 7 (doc. web n. 9535354), il quale prevede l'anonimizzazione delle informazioni personali utilizzate per tali fini (alla luce delle linee guida 05/2014 del WP29) ovvero, qualora non sia possibile procedere all'anonimizzazione dei dati (per es. a causa delle peculiarità del caso clinico rappresentato), il ricorso a un valido consenso dell'interessato, che invece non era rinvenibile in quello acquisito in atti, rivelatosi non specifico e non informato in ordine alla finalità in questione.

A seguito di alcune segnalazioni l'Ufficio ha avviato un'istruttoria nei confronti di un IRCCS che era stato individuato come presidio sanitario di riferimento per la vaccinazione contro il vaiolo delle scimmie. Il procedimento istruttorio si è concluso con un provvedimento di ammonimento in quanto la raccolta di numerose e dettagliate informazioni sullo stato di salute e sulla vita sessuale delle persone interessate

Casi particolari

alla campagna di vaccinazione, già in fase di prenotazione della stessa e non anche nei colloqui fra medico e paziente e senza aver fornito le informazioni di cui all'art. 13 del RGPD, è stata valutata in violazione dei principi di liceità, correttezza, trasparenza e integrità e riservatezza di cui all'art. 5, par 1, lett. a) e f), del RGPD (provv. 6 luglio 2023, n. 289, doc. web n. 9920292).

In merito ai trattamenti di dati personali effettuati nell'ambito delle iniziative per contrastare il vaiolo delle scimmie, l'Ufficio ha interloquito con il Ministero della salute al fine di veder assicurato che non fosse prevista l'identificazione preventiva della platea dei soggetti da sottoporre a vaccinazione, in quanto la stessa era da considerarsi su base volontaria. Il Garante ha richiamato anche il rispetto del principio di minimizzazione dei dati personali chiedendo che non fosse prevista l'indicazione della categoria di rischio nella scheda vaccinale. Su tale aspetto il Ministero ha assicurato, infatti, che avrebbe informato le regioni e le province autonome, che in fase di registrazione della vaccinazione nell'anagrafe regionale, nel campo "categoria di rischio", fosse valorizzato il codice "01 nessuna indicazione" (nota 10 agosto 2022 e punto 1 provv. 6 luglio 2023, n. 289, doc. web n. 9920292, cit.).

Rassicurazioni da parte del Ministero della salute sono pervenute con riferimento all'attuazione della circolare adottata sul "Monitoraggio degli episodi di violenza commessi ai danni degli esercenti le professioni sanitarie e socio-sanitarie nell'esercizio delle loro funzioni" (nota 10 ottobre 2023). Secondo quanto specificato dal Ministero, a seguito dell'avvio di un'istruttoria da parte dell'Ufficio, i soggetti a cui compete l'acquisizione, dalle strutture sanitarie e sociosanitarie pubbliche e private, dei dati regionali sugli eventi avversi (aggressioni), privati degli elementi indentificativi diretti, sono i Centri regionali per la gestione del rischio sanitario e la sicurezza del paziente. Tali dati, a seguito di un processo di anonimizzazione, potranno poi essere trasmessi all'Osservatorio nazionale delle buone pratiche sulla sicurezza nella sanità istituito presso il Ministero per le finalità di monitoraggio attribuitegli dalla disciplina di settore.

Sono stati altresì esaminati casi di comunicazioni di dati effettuate da soggetti privati in assenza di idoneo presupposto giuridico. In particolare, a seguito di un reclamo di un cittadino e di una notifica di *data breach* effettuata dal titolare del trattamento, il Garante si è occupato della consegna, da parte di un gruppo societario sanitario privato, di una cartella clinica di pronto soccorso a un omonimo del reclamante, sulla quale erano stati trascritti gli eventi clinici riguardanti l'omonimo di quest'ultimo. L'Autorità, dopo aver disposto la riunione del procedimento relativo alla notifica di violazione trasmessa ai sensi dell'art. 33 del RGPD con quello attivato dal reclamo, considerato che riguardavano la medesima vicenda, ha accertato la violazione evidenziata, ritenendo il trattamento illecito per la violazione del principio di esattezza e di integrità e riservatezza (art. 5 par. 1, lett. d) e f) del RGPD); inoltre, ha valutato che, mediante l'erronea redazione della cartella clinica di pronto soccorso, successivamente consegnata al paziente omonimo del reclamante, la medesima società aveva effettuato una comunicazione di dati relativi alla salute concernenti due pazienti in assenza di un idoneo presupposto giuridico.

Nella determinazione della sanzione erogata dal Garante, sono stati considerati – oltre al fatturato della società, all'adozione nei confronti della società medesima di un precedente provvedimento per violazioni pertinenti e al peculiare contesto emergenziale da pandemia da Covid-19 – anche gli effetti potenzialmente gravi che la redazione di documentazione sanitaria errata poteva avere per la salute degli interessati (provv. 15 dicembre 2022, n. 43 del 2023, doc. web n. 9870788).

In un'altra occasione, una non corretta gestione dei dati personali è stata riscontrata nei confronti di una struttura sanitaria privata, a seguito di un reclamo di un cittadino che aveva lamentato di aver ricevuto periodicamente dalla società messaggi sul suo

5

5

numero privato per ricordargli appuntamenti per visite mediche mai richieste, e di aver rinvenuto, nella dichiarazione dei redditi 730 precompilata, talune fatture emesse sul proprio codice fiscale concernenti prestazioni erogate dalla società a vantaggio di un paziente omonimo. Anche in questo caso è stata rilevata una violazione del principio di esattezza, di integrità e riservatezza dei dati e, mediante la compilazione della fattura relativa alle prestazioni usufruite dall'omonimo contenente le informazioni (indirizzo e codice fiscale) del reclamante, una comunicazione di dati relativi alla salute (desumibili dalle prestazioni effettuate presso il Centro, con riferimento alle quali sono state emesse le relative fatture) in assenza di un idoneo presupposto giuridico. Il provvedimento sanzionatorio adottato nei confronti della società ha considerato, altresì, il fatto che l'episodio si è determinato anche a causa dell'omonimia dei nomi e cognomi degli interessati (provv. 1° giugno 2023, n. 228, doc. web n. 9909889).

L'Autorità, in relazione ad altra vicenda, oggetto di segnalazione, avendo accertata, al termine del procedimento istruttorio, l'illiceità del trattamento di dati personali effettuato da una struttura sanitaria lombarda, titolare del trattamento, nonché dalla società informatica nominata, da tale struttura sanitaria, quale responsabile del trattamento per i servizi di manutenzione e assistenza *software*, ha ammonito entrambi: il titolare del trattamento per aver posto in essere un trattamento di dati personali in violazione degli artt. 5, par. 1, lett. f), 25, par. 1 e 32, par. 1, del RGPD (provv. 30 novembre 2023, n. 557, doc. web n. 9984477) e il responsabile del trattamento per aver violato gli artt. 5, par. 1, lett. f) e 32 del RGPD (provv. 30 novembre 2023, n. 556, doc. web n. 9973790). Nel caso esaminato, il segnalante aveva potuto prendere visione, in assenza di legittimazione, di dati personali relativi alla salute contenuti nell'accettazione intestata ad altro interessato attraverso la piattaforma - messa a disposizione dei pazienti da parte della citata struttura sanitaria - per il *download* dei referti. Rilevato che a determinare tale lesione alla riservatezza era stato un *bug* dell'applicativo, il Garante ha accertato la responsabilità per non aver effettuato il test e il collaudo a seguito dell'aggiornamento della funzionalità del portale. La vulnerabilità del sistema - che avrebbe potuto consentire a terzi, come poi si è verificato, di accedere a informazioni relative ad accettazioni intestate ad altri interessati, manipolando l'URL di accesso ad una specifica pagina del sito - era stata prevista in fase di test iniziale e opportunamente bloccata, ma non è stata considerata in seguito a una operazione di aggiornamento del medesimo portale, volta a introdurre la funzionalità che prevedeva la possibilità di visualizzare il registro delle operazioni eseguite.

In tali provvedimenti l'Autorità ha tenuto a evidenziare che sebbene sul titolare del trattamento ricada una "responsabilità generale" per i trattamenti posti in essere (v. artt. 5, par. 2, cd. *accountability*, e 24 del RGPD), anche quando questi siano effettuati da altri soggetti "per suo conto" (cons. n. 81, artt. 4, punto 8) e 28 del RGPD), il Regolamento ha disciplinato gli obblighi e le altre forme di cooperazione a cui è tenuto il responsabile del trattamento e l'ambito delle relative responsabilità (v. artt. 30, 32, 33, par. 2, 82 e 83 del RGPD). Il Garante ha ritenuto trattarsi di una "violazione minore", ai sensi del cons. 148 del RGPD e delle linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del RGPD (adottate dal Gruppo Art. 29 il 3 ottobre 2017, WP 253 e fatte proprie dal CEPD con l'*Endorsement* 1/2018 del 25 maggio 2018), in quanto l'episodio era risultato essere un fatto isolato privo di dolo, determinato da un comportamento intenzionale del segnalante e riconducibile a un grado di colpa da valutarsi come lieve, considerato che la violazione aveva riguardato i dati sulla salute di un solo interessato, e che sia il titolare che il responsabile erano intervenuti prontamente per attenuare gli effetti della violazione e prevenire il ripetersi di eventi analoghi, dimostrandosi ampiamente collaborativi con l'Autorità.

Sempre nell'ambito dei reclami ricevuti dai cittadini, si segnala l'intervento del

5

Garante nei confronti di un'azienda di rilievo nazionale e alta specializzazione, che aveva smarrito vetrini e tasselli istologici di una donna contenuti all'interno della cartella clinica, con la conseguente impossibilità per il CTU, chiamato a esprimersi in Corte d'appello, nell'ambito di un giudizio esperito dall'interessata, di esaminare il predetto materiale biologico e sostenere, o meno, la validità della richiesta risarcitoria avanzata dalla donna. Nell'esaminare la vicenda descritta, l'Autorità ha ritenuto che, indipendentemente dalla qualificazione dei predetti vetrini e tasselli quali "dati genetici", certamente essi sono riconducibili alla categoria di dati sulla salute previsti nell'art. 9 del RGPD in quanto trattasi di materiali biologici della donna, associati ad elementi numerici riferiti alla sua identità, idonei a rivelare informazioni in ordine all'avvenuta erogazione, nei confronti della stessa, di servizi di assistenza sanitaria. Ciò chiarito, è emerso che l'azienda non era dotata di protocolli scritti per la gestione e la custodia dei reperti istologici. Sul punto è stato rilevato che le linee guida del Ministero della salute, Consiglio superiore di sanità in materia di "Tracciabilità, raccolta, trasporto, conservazione e archiviazione di cellule e tessuti per indagini diagnostiche di anatomia patologica" (maggio 2015), in relazione al materiale campionato (blocchetti in paraffina e vetrini), hanno chiarito che il previsto termine di dieci anni è un termine minimo, alla scadenza del quale si estingue l'obbligo di conservazione per la struttura che lo detiene. In ogni caso, qualora siano in corso giudizi civili o penali, la struttura sanitaria, sentito il medico autore della condotta, è tenuta a valutare l'opportunità di conservazione del materiale anche oltre il termine decennale, in considerazione del contenzioso in corso (cfr. punto 5.3.2. del predetto documento).

Alla luce di quanto evidenziato, l'Autorità ha valutato che le predette circostanze non avrebbero dovuto esonerare l'azienda dall'obbligo di documentare quale operazione di trattamento (ivi compresa, l'eventuale cancellazione e distruzione) fosse stata effettuata sui dati personali contenuti nei vetrini associati a persone identificate in modo univoco a fini sanitari. Pertanto, anche alla luce del principio di responsabilizzazione (art. 5, par. 2, del RGPD), l'azienda, anche nel caso in non fosse stata più obbligata a conservare i campioni biologici, avrebbe dovuto, comunque, adottare modalità volte a garantire la tracciabilità degli stessi e individuare procedure documentate di gestione delle operazioni poste in essere, in tutte le fasi del trattamento, tenendo conto, in particolare, dei rischi derivanti dalla perdita dei dati personali conservati, secondo quanto previsto dagli artt. 5, par. 1, lett. f) e 32 del RGPD. In relazione allo smarrimento dei dati contenuti nei vetrini appartenenti alla reclamante, è stata rilevata conseguentemente l'illiceità del trattamento di dati personali, per la violazione degli artt. 5, par. 1, lett. f) e par. 2 e 32 del RGPD, nonché del provvedimento 5 giugno 2019, n. 146, doc. web n. 9124510 recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, d.lgs. n. 101/2018.

Nella definizione delle sanzioni pecuniarie, è stato ritenuto che la violazione delle disposizioni citate è stata conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trovando applicazione l'art. 83, par. 3, del RGPD, mentre il livello di gravità è stato considerato medio, tenuto conto del numero di interessati coinvolti, della categoria di dati personali interessata, della finalità del trattamento nonché del livello del danno subito dall'interessata. Sono stati altresì considerati l'elevato grado di cooperazione con l'Autorità in tutte le fasi del procedimento e, a seguito dei rilievi sollevati dall'Ufficio, l'adozione di una specifica procedura relativa alla consegna di vetrini, tasselli, esami istologici e citologici (prov. 21 dicembre 2023, n. 601, doc. web n. 9980617).

5.4.3. *Provvedimenti derivanti da istruttorie attivate d'ufficio*

Il 30 gennaio 2023 il Presidente del Garante ha inviato una nota a tutte le regioni e province autonome sulle garanzie che devono essere adottate nei reparti di pronto

5

soccorso nel trattare i dati sulla salute. In tale nota il Presidente ha evidenziato che l'ordinamento appresta specifiche tutele alle persone che si sottopongono a particolari tipologie di interventi sanitari o affette da patologie caratterizzate da una forte stigmatizzazione sociale. Ha inoltre rappresentato la necessità che l'erogazione delle prestazioni sanitarie, anche in emergenza, sia effettuata nel pieno rispetto soprattutto delle fasce più deboli quali i disabili, fisici e psichici, i minori, gli anziani e i soggetti che versano in condizioni di disagio o bisogno, garantendo altresì le specifiche tutele previste a favore delle vittime di violenza, di chi chiede l'accesso a percorsi clinici in anonimato e dei pazienti affetti da HIV.

Il Presidente ha pertanto richiamato gli enti locali a conformarsi a tali prescrizioni a proseguire l'opera di formazione degli operatori sanitari prevista dal RGPD e a vigilare affinché, nell'erogazione dei servizi sanitari, anche attraverso le nuove modalità offerte dalla sanità digitale, la protezione dei dati personali sia considerata un valore fondante sin dalla fase di progettazione (nota 30 gennaio 2023, doc. web n. 10011979).

5.4.4. Provvedimenti relativi al trattamento di dati personali effettuato nell'ambito dell'emergenza sanitaria

Nel 2023 sono state chiuse centinaia di istruttorie avviate a seguito di segnalazioni e reclami in ordine al trattamento dei dati connessi alla sanzione per mancato assolvimento dell'obbligo vaccinale degli ultracinquantenni. Al riguardo, si è ricordato che, a seguito del parere reso il 18 febbraio 2021 (doc. web n. 9746905), il Ministero della salute ha accolto le osservazioni formulate dall'Ufficio nell'ambito dell'istruttoria e ha introdotto specifiche misure di garanzia idonee a tutelare i diritti fondamentali e gli interessi delle persone fisiche. Nello specifico, è stato accolto l'invito a prevedere che i soggetti destinatari dell'avvio del procedimento sanzionatorio diano notizia all'Agenzia delle entrate della sola avvenuta presentazione della predetta comunicazione all'ASL competente, con modalità idonee ad assicurare il rispetto del principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c), del RGPD. Analogamente sono state individuate idonee modalità con le quali l'Agenzia delle entrate possa comunicare al Ministero della salute l'elenco dei soggetti per i quali non era stato prodotto l'avviso di addebito, indicando esclusivamente l'insussistenza dell'obbligo vaccinale o l'impossibilità di adempiervi, senza fornire informazioni idonee a rivelare lo stato di salute dell'interessato, nel rispetto del richiamato principio di minimizzazione dei dati.

Con riferimento al trattamento dei dati personali effettuato nell'ambito dell'emergenza sanitaria, a seguito di una segnalazione il Garante ha adottato un provvedimento sanzionatorio nei confronti di una casa di cura che consentiva – anche dopo la cessazione dello stato di emergenza – l'accesso agli ambulatori solo a coloro che fossero in possesso di una certificazione verde (provv. 28 settembre 2023, n. 423, doc. web n. 9946369). Nel ricostruire i vari interventi normativi sul tema e i relativi pareri rilasciati dall'Autorità, è stato rappresentato che la limitazione delle libertà personali effettuata attraverso il trattamento di dati sulla salute degli interessati e realizzata mediante la previsione di subordinare l'accesso a luoghi e a servizi al possesso di una certificazione attestante l'avvenuta vaccinazione o guarigione da Covid-19, o l'esito negativo di un test antigenico o molecolare, è ammissibile solo se prevista da una norma di legge statale (artt. 6, par. 2, e 9 del RGPD e artt. 2-ter e 2-sexies del Codice, cons. n. 48, reg. del Consiglio sul certificato Covid digitale dell'UE adottato il 14 giugno 2021; cfr. anche Corte cost., sent. n. 271/2005 sulla riserva di legge statale sulla protezione dati; Corte cost., sent. n. 37/2021). La disciplina di settore non ha mai previsto la certificazione verde per esigenze di salute, per le quali è sempre stato consentito l'accesso ai luoghi preposti per l'approvvigionamento di

farmaci e dispositivi medici e, comunque, per ogni finalità di prevenzione, diagnosi e cura. Pertanto, le modalità di accesso alle prestazioni sanitarie indicate dalla casa di cura hanno determinato di fatto un trattamento differenziato e potenzialmente discriminatorio.

In tema di *green pass* si evidenzia inoltre che il Garante, su delega di una Procura della Repubblica, ha svolto, nel mese di dicembre 2023, assieme al Nucleo speciale *privacy* e frodi tecnologiche della Guardia di finanza, indagini ai sensi dell'art. 370 c.p.p., in merito ai trattamenti di dati personali sulla salute effettuati da una clinica privata a seguito della refertazione di un tampone positivo al Covid-19 durante il periodo pandemico. Le indagini sono state avviate da una segnalazione di un interessato che aveva ricevuto un referto di un tampone positivo al Covid-19 che non aveva mai eseguito.

Piena collaborazione in materia è stata prestata anche nei confronti di una Procura regionale della Corte dei conti ai sensi dell'art. 58, comma 2, d.lgs. n. 174/2016 (codice della giustizia contabile), in merito alle attività istruttorie svolte ai fini dell'adozione del provvedimento di avvertimento adottato il 25 maggio 2021 nei confronti della Regione Campania in merito all'uso delle certificazioni verdi Covid-19 (doc. web n. 9590466) (nota 4 maggio 2023).

5.5. Trattamenti per finalità ulteriori rispetto a quelle di cura e/o amministrative correlate alla cura

L'Autorità è intervenuta su alcune vicende (apprese da agenzie di stampa) relative alla gestione delle sepolture dei feti e dei prodotti abortivi, rispetto alle quali erano emersi profili di criticità. Si faceva riferimento, in particolare, alla comunicazione da parte di un'azienda sanitaria ai servizi cimiteriali di un comune dell'elenco delle donne che avevano effettuato un intervento di interruzione di gravidanza, unitamente alla documentazione relativa, per ciascuna di esse, all'autorizzazione al trasporto e al seppellimento dei prodotti abortivi.

Nel provvedimento adottato nei confronti dell'azienda, l'Autorità ha chiarito che secondo la normativa di settore l'interruzione volontaria di gravidanza può essere praticata quando “la prosecuzione della gravidanza, il parto o la maternità comporterebbero un serio pericolo per la sua salute fisica o psichica, in relazione o al suo stato di salute”, oppure quando “la gravidanza o il parto comportino un grave pericolo per la vita della donna” o “siano accertati processi patologici, tra cui quelli relativi a rilevanti anomalie o malformazioni del nascituro, che determinino un grave pericolo per la salute fisica o psichica della donna” (artt. 4 e 6, l. n. 194/1978). Inoltre, “l'interruzione della gravidanza, spontanea o volontaria, nei casi previsti dagli artt. 4, 5 e 6 della l. 22 maggio 1978, n. 194, è considerata a tutti gli effetti come malattia” (art. 19 del d.lgs. n. 151/2001). Da ciò consegue che i dati personali relativi all'interruzione di gravidanza rientrano a pieno titolo tra i dati relativi alla salute, non solo in quanto il riferimento alla salute fisica e psichica della donna è esplicitato dalle predette disposizioni normative, ma anche perché si tratta di un evento connesso a una “prestazione di servizi di assistenza sanitaria” (anche, ad es., in caso di aborto spontaneo) (art. 4, par. 1, n. 15 del RGPD) (cfr. anche provv. 4 giugno 2015, n. 334, doc. web n. 4130998).

La citata legge n. 194/1978 ha previsto un rigoroso regime di riservatezza a tutela della donna che rientra nelle specifiche disposizioni di settore fatte salve dall'art. 75 del Codice. Il predetto regime di riservatezza è stato, peraltro, più volte ribadito dal Garante nell'ambito di diversi interventi, qualificando tali dati tra quelli soggetti “a maggiore tutela dell'anonimato” (parere su schema di decreto in materia di certificato

5

5

di assistenza al parto, 1° marzo 2000, doc. web n. 1085431; parere su schema di decreto in materia di FSE, 22 maggio 2014, doc. web n. 3230826; linee guida in materia di *dossier* sanitario, 4 giugno 2015, doc. web n. 4084632). Con riferimento alla sepoltura dei prodotti abortivi, la disciplina in materia di polizia mortuaria prevede specifiche regole in relazione alla presunta età di gestazione degli stessi, contenute nel d.P.C.M. n. 285/1990 (artt. 7 e 70), che deve essere interpretato e applicato alla luce della disciplina dell'UE in materia di protezione dei dati personali (art. 22, comma 1, d.lgs. n. 101/2018).

L'Autorità ha pertanto rilevato che l'acquisizione da parte dei servizi cimiteriali delle predette informazioni, direttamente identificative della donna, non risultava necessaria ai fini dell'espletamento dei compiti assegnati dalla legge ai servizi cimiteriali, né era richiesta ai fini dell'apposizione della targhetta sul cippo. Infatti, secondo la disciplina normativa pertinente al riguardo, le informazioni da indicare riguardano quelle del defunto, le quali non possono in alcun modo essere assimilate a quelle delle donne che hanno avuto una interruzione di gravidanza. È stata quindi ritenuta non conforme al principio di minimizzazione dei dati l'indicazione delle informazioni che identificano in maniera diretta le donne nel provvedimento di autorizzazione e sepoltura dei prodotti abortivi da trasmettere ai servizi cimiteriali. Inoltre, tale comunicazione comporta l'inserimento delle informazioni identificative delle donne nei registri cimiteriali tenuti ai fini dell'identificazione dei feti inumati nelle apposite aree, consentendo, di fatto, di estrarre da tali registri, tenuti in forma automatizzata, l'elenco delle donne che hanno effettuato un'interruzione di gravidanza in tutte le strutture ospedaliere ubicate nel territorio di riferimento, con ciò determinando un trattamento sproporzionato rispetto alla finalità, perseguita dai servizi cimiteriali, di provvedere alla sepoltura dei prodotti abortivi.

La comunicazione dei dati direttamente identificativi delle donne ai servizi cimiteriali non è risultata neanche giustificata, come asserito, quale unica modalità di individuazione del luogo del seppellimento del prodotto del concepimento al fine di consentire alla donna, che lo desidera successivamente, di conoscerne il luogo di sepoltura. Infatti, tale legittima esigenza può essere utilmente soddisfatta adottando specifici accorgimenti che, da un lato, garantiscano tale identificabilità, e dall'altro risultino idonei a ridurre il rischio che si verifichi un pregiudizio rilevante per le donne interessate, in considerazione della natura particolarmente delicata dei dati trattati. L'eventuale utilizzo di specifiche misure tecniche e/o organizzative (quali l'oscuramento dei dati identificativi delle donne, la pseudonimizzazione o la cifratura dei dati) garantirebbe la possibilità di individuare con certezza il prodotto del concepimento e il luogo della sua sepoltura, senza consentire – in modo diretto – di risalire all'identità della donna.

Il Garante ha pertanto sanzionato la condotta dell'azienda, ma ha ritenuto sufficiente ammonire il titolare del trattamento rilevandosi la difficile interpretazione del lacunoso quadro normativo di riferimento; inoltre sono stati riscontrati, da un canto, l'assenza di reclami e segnalazioni al Garante nei confronti dell'azienda, dall'altro, l'elevato grado di cooperazione che quest'ultima ha dimostrato fin da subito attraverso la disponibilità a trovare soluzioni condivise. L'Autorità, infine, ha contestualmente ingiunto all'azienda di adottare adeguate misure tecniche e/o organizzative per non rendere immediatamente identificabili le donne che hanno effettuato un'interruzione di gravidanza nella documentazione da trasmettere ai servizi cimiteriali (provv. 27 aprile 2023, n. 165, doc. web n. 9900503; cfr. par. 4.6).

La questione relativa alla gestione della sepoltura dei feti e dei prodotti abortivi ha interessato anche un comune e i servizi cimiteriali dello stesso, nei confronti dei quali il Garante ha adottato specifici provvedimenti (cfr. par. 4.6).

Altri interventi del Garante in relazione a trattamenti effettuati per finalità diverse rispetto a quelle di cura e/o amministrative correlate alla cura sono avvenuti su

istanza degli interessati. In particolare, in un caso, un reclamante aveva lamentato la trasmissione di informazioni sulla sua salute da parte di un medico, cui si era rivolto per effettuare una visita specializzata (visita pneumologica, con un esame polisonnografico), alla società che aveva indirizzato il paziente dal predetto professionista sanitario, al fine di fargli acquistare un macchinario con il quale effettuare una terapia ventilatoria, in assenza del proprio consenso.

Nel provvedimento sanzionatorio nei confronti del medico, il Garante ha chiarito innanzitutto che le informazioni volte a rivelare lo stato di salute possono essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o su indicazione dell'interessato previa delega scritta di quest'ultimo (artt. 9 del RGPD e 84 del Codice - nella versione precedente alla riformulazione a opera del d.lgs. n. 101/2018 - in combinato disposto con l'art. 22, comma 11, d.lgs. n. 101/2018). Inoltre, l'Autorità ha evidenziato che il consenso dell'interessato non è richiesto (art. 9, par. 2, lett. h) e par. 3 del RGPD) soltanto per i trattamenti "necessari" al perseguimento di specifiche finalità di cura, effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale. Tali trattamenti sono quelli "essenziali" per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute (cfr. cons. 53 del RGPD, provv. 7 marzo 2019, n. 55, doc. web n. 9091942).

Tuttavia, nel caso di specie, la trasmissione alla predetta società delle informazioni sullo stato di salute dell'interessato, seppur asseritamente volta ad agevolare l'acquisizione del macchinario, non poteva considerarsi imprescindibile per la cura, posto che il paziente era già nelle condizioni di agire autonomamente per procurarselo. Infine, a nulla sono valse le memorie difensive con le quali il medico aveva fatto valere il ricoperto ruolo di responsabile del trattamento, in quanto non è risultato che la comunicazione dei dati sulla salute al soggetto fornitore del macchinario era stata effettuata a seguito di specifica istruzione della medesima società; al contrario, è emerso che la decisione in tal senso era stata assunta autonomamente dal medico, titolare autonomo del trattamento.

Nel medesimo provvedimento, è stato altresì considerato che, nel rispetto del principio di minimizzazione dei dati, ai fini dell'attività di "titolazione", la società avrebbe avuto bisogno di acquisire elementi relativi alla sola patologia dell'eventuale destinatario del macchinario, ma non anche il suo intero referto, comprensivo dei dati identificativi. Pertanto, la condotta del medico è stata sanzionata perché ritenuta in violazione dei principi di base del trattamento di cui all'art. 5, par. 1, lett. a), c) e f) del RGPD e in assenza dei presupposti giuridici previsti dall'art. 9 del RGPD, considerato che non è stata dimostrata l'acquisizione del consenso dell'interessato al trattamento dei propri dati personali per la predetta operazione (provv. 28 settembre 2023, n. 425, doc. web n. 9946712).

L'Autorità si è inoltre occupata della pubblicazione *online* della documentazione relativa a un corso formativo per psichiatri contenente dati personali della reclamante e informazioni sulla salute e sulle indagini giudiziarie riguardanti il figlio deceduto (biografia, perizie psichiatriche, anamnesi, medicinali assunti, reati per i quali era stato indagato). I predetti documenti facevano parte del materiale didattico messo a disposizione dei partecipanti tramite un *link* inviato per *e-mail* alla fine del corso e risultava inoltre accessibile *online* da chiunque conoscesse l'URL. Nel provvedimento sanzionatorio, il Garante, oltre a ribadire che ai dati delle persone decedute continuano ad applicarsi le tutele della normativa in materia di protezione dei dati personali, ha ritenuto che la società aveva effettuato un trattamento di dati personali, sulla salute e giudiziari, in violazione dei principi di base del trattamento di cui agli artt. 5, 6, 9 e 10, nonché degli obblighi in materia di sicurezza di cui all'art. 32 del RGPD, e degli artt. 2-*septies* e 2-*octies* del Codice. Infatti, oltre a verificare l'adeguatezza delle misure di anonimizzazione adottate sui dati personali della reclamante

5

5

e del figlio deceduto, la società avrebbe dovuto mettere in atto misure tecniche, organizzative e di verifica adeguate a garantire in via permanente la riservatezza dei dati trattati, utilizzando una procedura di autenticazione informatica per consentire l'accesso alla documentazione soltanto ai medici che avevano frequentato il corso. Nel determinare l'importo della sanzione irrogata, è stato ritenuto alto il livello di gravità della violazione, in considerazione della durata e delle categorie di dati personali interessate (unitamente al fatturato della società e ad altri elementi) (prov. 16 novembre 2023, n. 527, doc. web n. 9960948).

5.6. *Esercizio dei diritti*

Il Garante, nel corso dell'anno, ha anche trattato reclami proposti nei confronti di strutture sanitarie pubbliche e private per non avere fornito riscontro a istanze avanzate dagli interessati nell'esercizio dei diritti garantiti dal Regolamento.

In tali ipotesi il Garante ha sempre avuto cura di evidenziare che, qualora il titolare ritenga di non volere/potere ottemperare alla richiesta dell'interessato, deve comunque informare quest'ultimo, senza ritardo, circa i motivi di tale inottemperanza e della possibilità di presentare reclamo al Garante o, in alternativa, ricorso giurisdizionale (art. 12, par. 4, del RGPD).

In prevalenza, i reclami hanno riguardato il mancato riscontro a richieste di esercizio del diritto di accesso ai dati personali di cui all'art. 15 del RGPD. In numerosi casi, il Garante, trattandosi, in realtà, di mancato riscontro a richieste volte ad accedere alla documentazione sanitaria ai sensi della l. n. 241/1990 o di altra normativa di settore (l. n. 24/2017, ecc.) ha archiviato il reclamo ponendo in evidenza, come già in precedenza, che il diritto di accesso garantito dalla normativa UE e nazionale, in materia di protezione dei dati, deve essere tenuto distinto dal diritto di accesso ai documenti pubblici stabilito dalla legislazione nazionale e che le valutazioni in ordine alle determinazioni adottate sulla specifica richiesta di accesso alla documentazione esulano dall'ambito dei compiti attribuiti dalla legge al Garante (artt. 57 del RGPD, nonché 154 del Codice), restando sindacabili di fronte alle autorità competenti (cfr. art. 25 della l. n. 241/1990). In taluni casi ha anche tenuto ad aggiungere che la *ratio* del diritto di accesso sancito dall'art. 15 del RGPD è quella di rendere consapevole l'interessato dei trattamenti dei dati che lo riguardano effettuati dal titolare del trattamento, nonché di rendere agevole la verifica della liceità degli stessi, precisando che l'istituto dell'accesso ai dati personali non può essere utilizzato in sostituzione di differenti strumenti e istituti riconosciuti da altre normative di settore eventualmente applicabili in concreto. In tal senso, l'Autorità ha richiamato quanto indicato dal CEPD – in esplicitazione di quanto previsto dall'art. 15, par. 3, del RGPD, per il quale “Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento” – nel documento “*Guidelines 01/2022 on data subject rights - Right of access*”, con particolare riguardo al par. 5.2.5, punto 152, di quest'ultimo; in sostanza, il CEPD ha ricordato che l'obbligo sancito dal RGPD si configura quale obbligo di fornire copia immodificata dei dati personali contenuti nei singoli documenti, non già di fornire copia dei documenti contenenti i dati, e che a tal fine occorre fornire tutti i dati personali oggetto di trattamento, anche in forma compilativa, purché ciò consenta all'interessato di prendere piena conoscenza del trattamento in questione. L'Autorità ha anche ricordato l'ipotesi stabilita dalla giurisprudenza della CGUE, per la quale il titolare fornisce “copia integrale dei documenti contenuti nella sua cartella medica che contengano, tra l'altro, detti dati, solo qualora la fornitura di una siffatta copia sia necessaria per consentire all'interessato di verificarne l'esattezza e la completezza nonché per garantirne l'intelligibilità” (cfr. sentenza della CGUE 26 ottobre 2023 – C-307/22).

In alcuni casi il Garante ha adottato specifiche misure, anche sanzionatorie, a seguito dei reclami pervenuti. In un caso, ha sanzionato un'azienda sanitaria per il mancato riscontro a un'istanza di accesso ai dati avanzata dall'interessata, ai sensi dell'art. 15 del RGPD, anche al fine di verificare la correttezza del trattamento dati connesso alla campagna vaccinale. Nello specifico, non avendo la struttura sanitaria fornito risposta all'interessata nei termini previsti dall'art. 12 del RGPD, né rappresentato idonei motivi per giustificare tale inottemperanza, se non a seguito dell'invito formulato dall'Autorità ai sensi dell'art. 15 del reg. del Garante n. 1/2019, è stata inflitta una sanzione pecuniaria per la violazione dell'art. 12, par. 3, in relazione all'art. 15 del RGPD (provv. 11 gennaio 2023, n. 6, doc. web n. 9853446).

In un altro caso, il Garante ha adottato un provvedimento sanzionatorio nei confronti di un imprenditore individuale, già titolare di un centro medico organizzato in forma di ambulatorio, la cui impresa era stata cancellata dal registro delle imprese successivamente alla data di presentazione dell'istanza di esercizio dei diritti formulata dall'interessato. Quest'ultimo, assunta la veste di reclamante, ha rappresentato al Garante, fra altro, di aver esercitato i diritti di cui agli artt. da 15 a 22 del RGPD nei confronti di tale titolare, richiedendo l'accesso ai propri dati personali, la rettifica e la cancellazione (artt. 15, 16 e 17 del RGPD) di alcuni dati inesatti – nella specie, il referto di un prelievo effettuato presso la citata struttura sanitaria riportava dati identificativi errati (data di nascita e codice fiscale) – nonché la limitazione degli stessi (art. 18 del RGPD), senza, tuttavia, ricevere riscontro. Il riscontro era stato fornito solo a seguito dell'invito, formulato dal Garante al titolare, ad aderire alle richieste dell'interessato ai sensi dell'art. 15 del reg. del Garante n. 1/2019 e ritenuto, comunque, inidoneo dall'interessato. Il Garante, pertanto, ha inflitto una sanzione pecuniaria al titolare per la violazione dell'art. 12, in relazione ai diritti esercitati di cui agli artt. 15, 16, 17 e 18 del RGPD. In tale circostanza il Garante ha ritenuto non ricorrere i presupposti per l'adozione di altre misure correttive di cui all'art. 58, par. 2, del RGPD, in quanto l'impresa individuale, al cui esercizio risultavano riconducibili le violazioni sopra descritte, risultava cancellata dal registro delle imprese al momento dell'adozione del provvedimento, nonché per il fatto che lo stato di emergenza disposto dal Consiglio dei ministri dal 31 gennaio 2020 – in relazione al quale assumeva rilevanza la richiesta del reclamante di rettifica del referto del tampone per la rilevazione del Covid-19 – era cessato in data 31 marzo 2022 sulla base del d.m. n. 24/2022 (provv. 31 agosto 2023, n. 389, doc. web n. 9938463).

Con riferimento, poi, a un reclamo per il mancato riscontro a un'istanza di accesso ai dati, il Garante, dopo avere accertato la violazione dell'art. 12 del RGPD in relazione all'art. 15 del RGPD medesimo, ritenendo, sulla base della valutazione delle circostanze del caso, trattarsi di una "violazione minore" ai sensi del cons. 148 del RGPD, ha adottato un provvedimento di ammonimento nei confronti di un istituto ospedaliero, titolare del trattamento (provv. 13 aprile 2023, n. 179, doc. web n. 9909566).

5

6 La ricerca scientifica

6.1. *Provvedimenti adottati ai sensi dell'art. 110 del Codice*

Nel campo della ricerca scientifica si menzionano numerosi provvedimenti con i quali il Garante, adito in consultazione preventiva ai sensi dell'art. 110 del Codice, si è espresso in ordine al trattamento dei dati personali per finalità di ricerca medica, biomedica e epidemiologica nei casi di impossibilità all'acquisizione del consenso da parte dei pazienti arruolati, in quanto deceduti o non contattabili anche ai sensi del punto 5.3. delle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (all. n. 5 al provvedimento che individua le prescrizioni contenute nelle autorizzazioni generali che risultano compatibili con il RGPD e il Codice, 5 giugno 2019, doc. web n. 9124510).

Come di seguito illustrato nel dettaglio, l'Autorità si è soffermata, in particolare, sul corretto inquadramento delle condizioni di liceità del trattamento, sugli adempimenti correlati alla trasparenza, sui tempi di conservazione dei dati, sulle misure implementate per la pseudonimizzazione e l'anonimizzazione dei dati.

Nella maggior parte dei provvedimenti adottati, il Garante ha ribadito che il promotore dello studio e i centri partecipanti possono dare inizio ai trattamenti dei dati personali necessari per la realizzazione dello studio stesso solo dopo l'ottenimento dei pareri favorevoli dei rispettivi comitati etici, in quanto condizione di liceità del trattamento dei dati personali per le finalità in esame laddove non sia possibile acquisire il consenso degli interessati (cfr. provv.ti 29 ottobre 2020, n. 202, doc. web n. 9517401 e 1° novembre 2021, n. 406, doc. web n. 9731827).

Con specifico riferimento agli obblighi di trasparenza, il Garante ha ribadito la necessità di rendere pubbliche, per tutta la durata dello studio, le informazioni da fornire agli interessati, in quanto deceduti e non contattabili, attraverso una specifica inserzione sui siti internet del promotore e dei centri di sperimentazione coinvolti, secondo quanto previsto dagli artt. 14, par. 5, lett. b), del RGPD e 6, comma 3, delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, all. A5 al Codice.

Un primo provvedimento ha riguardato un'azienda ospedaliera universitaria che aveva presentato un'istanza di consultazione preventiva per la realizzazione di uno studio multicentrico, retrospettivo, osservazionale, epidemiologico e non farmacologico, volto a "valutare l'impatto della pandemia da Covid e relative misure istituzionali di distanziamento sociale sugli accessi in emergenza urgenza per patologia neuropsichiatrica infantile (NPI) e collocare tale impatto nel contesto del trend antecedente la pandemia stessa", in ragione del fatto che, a causa dell'elevato numero di pazienti da arruolare nello studio (tra i 6.000 e i 10.000) e della natura *no profit* dello stesso, l'acquisizione del consenso avrebbe comportato uno sforzo sproporzionato, tale da compromettere gravemente il conseguimento delle finalità della ricerca.

Il Garante, al riguardo, ha espresso un parere favorevole condizionato, ritenendo che l'azienda avesse correttamente individuato le basi giuridiche del trattamento e documentato lo sforzo sproporzionato che il tentativo di contattare ogni singolo paziente avrebbe comportato, tenuto conto dell'ampio numero di aderenti e della natura *no profit* dello studio (punto 5.3 delle prescrizioni). Non ha invece ritenuto di poter considerare, quale valida giustificazione dell'impossibilità di acquisire il consenso, il richiamo al "*bias* di selezione dovuto al fatto che a esprimere il consenso

sarebbero più facilmente i soggetti sensibili alla ricerca e/o alle questioni cliniche oggetto della stessa, appartenenti a uno status socioeconomico mediamente più elevato e che abbiano la possibilità di investire circa un'ora del loro tempo e venire in ospedale per firmare dei consensi informati”, in quanto tale motivazione prescinde dalle specificità del caso esaminato e non è prevista tra quelle indicate al punto 5.3 delle prescrizioni sopra ricordate.

Il Garante ha inoltre preso favorevolmente atto della corretta applicazione dell'art. 89 del RGPD da parte dell'azienda, prevedendo robuste tecniche di minimizzazione dei dati durante tutta la fase del trattamento e la possibilità di perseguire lo scopo di ricerca attraverso la raccolta e l'analisi di dati aggregati, atteso che tale tipologia di informazioni è risultata sufficiente per il perseguimento degli scopi di ricerca, nel rispetto dei principi di responsabilizzazione e di *privacy by design* (artt. 5, par. 2, 24 e 25 del RGPD).

Il Garante ha posto ulteriori specifiche condizioni con riferimento all'anonimizzazione dei dati al termine del periodo di conservazione e nelle ipotesi di condivisione dei dati con soggetti terzi. In particolare, con riguardo alle tecniche di generalizzazione, ha richiesto all'azienda di ridefinire le classi di equivalenza al fine di garantire una numerosità minima per ciascuna di esse, ritenendo congrua una soglia di almeno 20 unità. Inoltre, in considerazione del numero di variabili oggetto di aggregazione, ha chiesto di assicurare che il numero di statistiche aggregate da rendere conoscibili al fine di scongiurare il rischio di ricostruzione di dati riferibili ai singoli sia significativamente inferiore rispetto al numero delle variabili considerate. Infine il Garante ha chiesto la rimozione di ogni singolarità, qualora il titolare ne venga a conoscenza, con qualsiasi mezzo, in una fase successiva all'applicazione delle predette tecniche di anonimizzazione, e il tracciamento di tali eventi in modo da ripetere la valutazione del rischio di re-identificazione al raggiungimento del 1% di singolarità individuate sul totale delle informazioni incluse nella banca dati (provv. 2 marzo 2023, n. 73, doc. web n. 9875254).

Il secondo parere, anch'esso favorevole, ma condizionato, ha riguardato l'istanza di consultazione preventiva presentata da una un'altra azienda ospedaliero universitaria promotrice di uno studio osservazionale, multicentrico, retrospettivo, *no profit*, volto a fornire una più accurata caratterizzazione dei pazienti affetti da istotipi rari di neoplasie delle vie biliari al fine di garantire il miglior approccio terapeutico (provv. 22 giugno 2023, n. 261, doc. web n. 9919244). Il Garante ha ritenuto che l'azienda avesse correttamente individuato la base giuridica per il trattamento avendo rappresentato in maniera esaustiva i motivi sottesi all'impossibilità di riuscire a informare gli interessati e acquisirne un valido consenso, correlati, in particolare, all'alta incidenza di mortalità della patologia osservata e alla circostanza che l'analisi retrospettiva dei dati avrebbe comportato una raccolta di informazioni a partire dall'anno 2002 (punto 5.3 delle prescrizioni). Inoltre, l'azienda ha dimostrato gli sforzi – ragionevoli e proporzionati – profusi per tentare di contattare i pazienti, anche attraverso la stipula di una convenzione con il comune di riferimento, per la consultazione per via telematica della banca dati dell'Anagrafe della popolazione su base nazionale che è stata ritenuta conforme al quadro normativo applicabile (artt. 34, comma 1, d.P.R. n. 223/1989 e 58 del CAD).

Il Garante ha tuttavia rilevato che il modulo informativo trasmesso non era specificamente riferito ai trattamenti di dati personali effettuati nell'ambito dello studio, ritenendo necessario condizionare il parere alla modifica delle informative affinché l'azienda fornisse in maniera chiara, intellegibile, puntuale ed esplicita (art. 12 del RGPD) tutti gli elementi di cui agli artt. 13 e 14 del RGPD, in particolare le pertinenti basi giuridiche, le finalità del trattamento e i tempi di conservazione ovvero i criteri utilizzati per determinarli.

6

6

Il Garante ha poi preso favorevolmente atto della riduzione del periodo di conservazione dei dati, dagli originari venticinque a cinque anni, che è risultato adeguato allo scopo della raccolta. Con riguardo alla diffusione dei dati in forma anonima e aggregata, tenuto conto del generico riferimento dell'azienda alla "generalizzazione" come tecnica per l'anonimizzazione dei dati, il Garante ha condizionato il parere favorevole all'assicurazione fornita dal titolare che il risultato della "generalizzazione" fosse composto da gruppi (*cluster*) costituiti da un numero di interessati distinti, sufficiente a evitare singolarità o inferenze immediate.

Il Garante ha inoltre evidenziato come l'implementazione delle misure di cui all'art. 89 del RGPD, volte, in particolare, all'effettiva applicazione del principio di minimizzazione, non esima il titolare del trattamento dall'introdurre altresì idonee misure tecniche e organizzative ai sensi dell'art. 32 del RGPD, per un'effettiva applicazione del principio di integrità e riservatezza dei dati, nel caso di specie ritenute idonee (art. 5, par. 1, lett. f), del RGPD).

In un altro caso, una società farmaceutica francese ha presentato un'istanza di consultazione preventiva in qualità di promotore e titolare del trattamento di uno studio osservazionale retrospettivo volto a valutare i tassi di incidenza degli eventi trombotici nei pazienti affetti da malattia di agglutinine fredde.

Il Garante ha espresso un parere favorevole condizionato, rilevando in particolare che il trasferimento dei dati pseudonimizzati dei pazienti italiani presso società affiliate aventi sede fuori dal territorio dell'Unione europea, ossia in Paesi terzi, si fonda in astratto su idonei presupposti giuridici (artt. 24, 28, 44 e ss. del Codice). A tale riguardo, tenuto conto che il predetto trasferimento sarebbe avvenuto sulla base delle *binding corporate rules* (BCR) della società, il Garante ha evidenziato che in ogni caso la loro efficacia e correttezza dovrà comunque essere verificata in concreto da parte del titolare del trattamento, in applicazione del principio di *accountability* (art. 5, par. 2, del RGPD).

Nel provvedimento in esame, il Garante ha fornito specifiche indicazioni alla società in ordine alla prospettata ipotesi di realizzare ricerche future con i dati raccolti per la realizzazione dello studio, sulla base del consenso degli interessati raccolto durante il periodo di conservazione dei dati. A tale riguardo, è stato chiarito che il provvedimento riguardava esclusivamente lo studio per il quale la società aveva avanzato l'istanza di consultazione preventiva, e si è ribadito che, laddove il titolare si fosse trovato in una delle condizioni di impossibilità ad acquisire il consenso di cui all'art. 110 del Codice e al punto 5.3 delle prescrizioni, avrebbe dovuto avanzare specifica istanza di consultazione preventiva ai sensi del predetto art. 110 del Codice. Il Garante ha altresì posto precise condizioni, volte ad assicurare effettiva applicazione al principio di trasparenza e quindi, in ultima istanza, a tutela dell'autodeterminazione informativa dei pazienti. In particolare, ha ritenuto necessario che il modulo informativo fosse modificato con la corretta indicazione delle basi giuridiche del trattamento relative ai pazienti contattabili, richiamando l'art. 9, par. 2, lett. a), del RGPD, e a quelli non contattabili, integrando il riferimento all'art. 9, par. 2, lett. j), del RGPD con quello all'art. 110 del Codice, e che fosse inoltre chiarito come, oltre al consenso al trattamento dei dati per lo studio, sarebbe stata richiesta un'ulteriore manifestazione di volontà al solo scopo di poter contattare i pazienti per futuri scopi di ricerca.

In relazione ai pazienti non contattabili, anche a vantaggio dei loro aventi causa (art. 2-*quaterdecies* del Codice), il Garante ha ritenuto non idonea a garantire effettiva applicazione del principio di trasparenza, né coerente con le indicazioni fornite dall'art. 6, comma 3, delle regole deontologiche, la sola affissione dell'informativa presso ogni centro partecipante, in quanto tale modalità richiede che gli interessati si rechino presso il centro partecipante, diventando di fatto così contattabili (cfr. anche provv. 7 dicembre 2023, n. 582 doc. web n. 9971457).

Il Garante ha rilevato, inoltre, nella valutazione di impatto la carenza di specifiche misure per le attività di monitoraggio eventualmente svolte da remoto, condizionando il parere a che la società integrasse la valutazione d'impatto con una specifica sezione in cui fossero indicati tali trattamenti e i correlati rischi per i diritti e le libertà degli interessati e le necessarie misure per mitigarli (provv. 6 luglio 2023 n. 285, doc. web n. 9919999).

Un altro caso, per molti profili simile al precedente, ha riguardato l'istanza presentata da un'azienda ospedaliero universitaria per lo svolgimento di uno studio osservazionale multicentrico, retrospettivo e prospettico per valutare la sicurezza e l'efficacia di un farmaco in pazienti oncologici, che coinvolge tutte le unità oncologiche italiane (26 centri), con una dimensione campionaria stimata di 50 pazienti. Il Garante ha espresso un parere favorevole condizionato, ribadendo in particolare quanto già indicato nel precedente parere 2 marzo 2023, n. 73 (doc. web n. 9875254) in ordine all'anonimizzazione dei dati e ponendo specifiche condizioni al fine di assicurare effettiva applicazione al principio di trasparenza (provv. 18 luglio 2023, n. 315, doc. web n. 9920977).

Una società farmaceutica statunitense, con un proprio rappresentante nel territorio dell'Unione europea in conformità all'art. 27 del RGPD, aveva avanzato un'istanza di consultazione preventiva, in relazione a un progetto (da realizzarsi in alcuni paesi dell'Unione europea, tra cui, l'Italia) di *Real World Data Collection* (RWDC) su pazienti decedute o non contattabili alle quali era stato somministrato un farmaco antitumorale. Al riguardo, il Garante ha ribadito quanto già evidenziato nei pareri sopra richiamati in ordine ai trasferimenti dei dati delle pazienti in forma pseudonimizzata al titolare stabilito negli Stati Uniti d'America, alla trasparenza dei trattamenti, all'eventualità che l'attività di monitoraggio dello sponsor venisse svolta da remoto nonché alle misure per prevenire il rischio di reidentificazione degli interessati (provv. 31 agosto 2023, n. 364, doc. web n. 9936136).

Un altro parere favorevole condizionato, che merita di essere segnalato, è quello adottato dal Garante nei confronti di una università a seguito della presentazione di una istanza di consultazione preventiva per la raccolta retrospettiva di dati necessari a uno studio clinico inserito nel programma europeo Horizon 2020 e implicante l'arruolamento di circa 50 pazienti pediatriche dell'azienda ospedaliera facente capo all'istante affetti da due specifiche patologie tumorali. Tale studio avrebbe comportato la realizzazione di una piattaforma *open e cloud-based* (funzionale alla gestione clinica delle predette patologie) nella quale sarebbero stati salvati i dati dei pazienti in forma pseudonimizzata e resi accessibili ai soli membri del consorzio sulla base del progetto di ricerca europeo (provv. 28 settembre 2023, n. 465, doc. web n. 9948285).

Con specifico riferimento alle basi giuridiche del trattamento, il Garante ha ritenuto pertinente l'impossibilità di acquisire il consenso dei pazienti, correlata a impedimenti di tipo organizzativo, in ragione dell'ampiezza del periodo di osservazione, dell'importante numero di decessi a causa della gravosità della malattia e del grave pregiudizio alla completezza del campione potenzialmente derivante dalla mancata inclusione dei dati dei pazienti deceduti o non contattabili. Tuttavia, il Garante ha rilevato che l'università non aveva adeguatamente comprovato i ragionevoli sforzi compiuti o che avrebbe inteso compiere, all'esito dei quali attestare l'effettiva irreperibilità degli interessati, e ha quindi chiesto di integrare in tal senso la valutazione d'impatto.

Il Garante ha ritenuto invece che il presupposto giuridico per il trattamento di dati personali raccolti nel *database* dello studio da parte dei membri del consorzio fosse da individuare nel reg. (UE) 1291/2013 del Parlamento e del Consiglio dell'11 dicembre 2013 che ha istituito il programma-quadro per la ricerca e l'innovazione

6

6

denominato Horizon 2020 (2014-2020) quale disposizione del diritto dell'Unione europea, conforme all'art. 9, par. 2, lett. j), del RGPD. In relazione al principio di trasparenza, nel ribadire le misure già indicate nei precedenti pareri, il Garante ha ritenuto altresì necessario far menzionare nelle informative agli interessati il periodo di conservazione dei dati raccolti dall'università per la realizzazione dello studio o il criterio utilizzato per determinare tale periodo (art. 13, par. 2, lett. a), del RGPD).

Un altro parere favorevole condizionato ha riguardato un caso simile a quelli sopra riportati, concernente un'istanza di consultazione preventiva presentata da una società farmaceutica francese per lo svolgimento di uno studio clinico multicentrico, osservazionale, retrospettivo e prospettico volto a consentire l'analisi dell'aggregazione di dati clinici, biologici, genomici e di *imaging* multimodali associati alla risposta al trattamento e alla prognosi di pazienti con tumore polmonare. Dall'istanza era emerso che lo studio sarebbe stato altresì volto a perseguire molteplici finalità secondarie quali lo sviluppo di un algoritmo prognostico proprietario, da utilizzare anche per le cure di altri tipi di tumore, nonché lo sviluppo di un'offerta di prodotti e/o servizi a scopo commerciale e la creazione di un *database* pseudonimizzato, a fini statistici e di ricerca clinica.

Il parere reso dal Garante ha riguardato esclusivamente i trattamenti dei dati necessari al perseguimento degli scopi primari dello studio relativi ai pazienti deceduti, poiché relativamente ai pazienti in vita il trattamento si sarebbe fondato sul relativo consenso; viceversa, in riferimento agli scopi secondari dello studio, il Garante ha rilevato la persistenza di profili di criticità in particolare in ordine all'individuazione delle finalità del trattamento (risultate non chiare, sovrapponibili a quelle primarie o estranee agli scopi di ricerca scientifica), alle basi giuridiche e ai tempi di conservazione dei dati, riservandosi pertanto di proseguire l'attività istruttoria. Rispetto, dunque, al trattamento dei dati necessari al perseguimento degli scopi primari dello studio, il Garante ha ritenuto che la società avesse correttamente indicato le pertinenti basi giuridiche, anche se è stata rilevata l'inconferente e imprecisa l'indicazione nella valutazione d'impatto e nelle informative di altre basi giuridiche per il trattamento dei dati personali, quali l'interesse pubblico rilevante, non avendo la società specificato la disposizione del diritto dell'Unione o dell'ordinamento interno su cui si fonderebbe tale trattamento (artt. 6, par. 1, lett. e), par. 2 e 3; 9, par. 2, lett. g); 89 del RGPD e 2-*sexies*, comma 2, lett. cc), del Codice).

In relazione alle tecniche di intelligenza artificiale e di apprendimento automatico, il Garante ha evidenziato come la raccolta e l'analisi statistica delle informazioni risultassero indispensabili per la successiva creazione di qualsiasi modello predittivo. Le previsioni formulate dall'algoritmo, nel caso di specie per sviluppare uno strumento diagnostico per i pazienti affetti dalla predetta patologia oncologica, si basano infatti sul preventivo esame, attraverso modelli matematici e statistici, di un'ingente mole di informazioni già detenute dalla società ed effettuato con una tempistica assai più rapida rispetto a quella che potrebbe garantire un analista umano, seppure esperto. Tuttavia, sulla scorta di precedenti giurisprudenziali e dottrinali, l'Autorità ha evidenziato la necessità di integrare tali elaborazioni automatizzate con l'intervento umano al fine di rivedere ed eventualmente correggere i calcoli probabilistici formulati attraverso gli algoritmi (cfr. Cons. di Stato, sent. n. 8472/2019; parere congiunto del CEPD e del GEPD, 5/2021 cit.; documento "Intelligenza Artificiale e Medicina: Aspetti Etici" del 29 maggio 2020 del Comitato nazionale per la bioetica e Comitato nazionale per la biosicurezza, le biotecnologie e le scienze della vita).

Il Garante ha inoltre rilevato specifiche criticità in ordine alla prospettata ipotesi di creare un *database* separato per scopi di ricerca e statistica al fine di promuovere lo sviluppo di nuove soluzioni diagnostiche e terapeutiche. In particolare, rimarcando l'indeterminatezza di tale finalità, è stato evidenziato come il trattamento

dei dati personali per il perseguimento delle predette finalità secondarie non possa fondarsi esclusivamente sull'interesse legittimo del titolare, atteso che i richiamati trattamenti riguardano dati inerenti alle particolari categorie ai sensi dell'art. 9, par. 1, del RGPD e impongono pertanto al titolare di verificare la sussistenza di una delle specifiche esenzioni dal divieto di trattamento di tali dati, di cui all'art. 9, par. 2, del RGPD, tra cui il consenso correttamente e validamente prestato. Il Garante ha poi rilevato alcune carenze nelle informative predisposte ai sensi degli artt. 13 e 14 del RGPD e richiesto al titolare di colmarle prima dell'inizio del trattamento (provv. 12 ottobre 2023, n. 472, doc. web n. 9953841).

In un altro caso, una società farmaceutica con sede in Svizzera ha presentato un'istanza di consultazione preventiva per la realizzazione di uno studio retrospettivo multinazionale, osservazionale, basato sulla raccolta dei dati sull'infezione da Citomegalovirus (CMV) nel contesto dei trapianti d'organi solidi. Il Garante ha espresso un parere favorevole condizionato, ritenendo necessario che il titolare effettuasse almeno tre tentativi di contatto non andati a buon fine e registrati nella cartella clinica dei pazienti, prima di considerare un paziente disperso al *follow up*, e richiedendo di espungere dalla valutazione d'impatto e dall'informativa il riferimento a basi giuridiche non pertinenti, quale l'interesse legittimo del titolare, (art. 6, par. 1, lett. f), del RGPD).

Il Garante non ha ritenuto conformi al principio di limitazione della conservazione le motivazioni addotte dalla società per conservare i dati codificati per un periodo di 30 anni dalla conclusione dello studio, riconducibili all'esigenza di uniformare il predetto periodo di conservazione alle normative nazionali dei Paesi in cui la società opera, in quanto l'ulteriore conservazione dei dati per scopi di ricerca scientifica può essere ammessa, conformemente all'art. 89, par. 1, del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato. Il Garante ha pertanto condizionato il parere alla conservazione dei dati per un periodo analogo a quello previsto per i centri partecipanti e, dunque, per 7 anni dalla conclusione dello studio. Il Garante ha altresì ribadito le indicazioni relative alle misure necessarie per l'anonimizzazione dei dati già indicate nei precedenti pareri, ponendo al riguardo una specifica condizione in caso di diffusione ovvero di condivisione dei dati con la comunità scientifica (provv. 26 ottobre 2023, n. 498, doc. web n. 9960973).

Un ulteriore parere favorevole condizionato è stato reso dal Garante nei confronti di un'azienda ospedaliero universitaria per la realizzazione di due studi retrospettivi (parere 26 ottobre 2023, n. 499, doc. web n. 9963509).

In particolare, l'azienda ospedaliero universitaria ha presentato due distinte istanze di consultazione preventiva in qualità di promotore e titolare del trattamento, a causa dell'impossibilità in entrambi gli studi di acquisire il consenso dell'elevato numero di interessati coinvolti, per motivate e comprovate ragioni organizzative, temporali ed economiche. Il Garante ha disposto la riunione dei procedimenti, con conseguente adozione di un unico parere, posto che l'azienda rivestiva in entrambi gli studi il ruolo di promotore e che le principali operazioni di trattamento sarebbero state realizzate in un contesto analogo, attraverso il medesimo sistema informativo e applicando le medesime misure tecniche e organizzative, (art. 10, comma 4 del reg. Garante n. 1/2019).

Le condizioni poste al parere favorevole hanno riguardato nuovamente la trasparenza dei trattamenti, più specificamente l'esigenza di pubblicare le informative per tutta la durata dello studio ai sensi degli artt. 14, par. 5, lett. b), del RGPD e 6, comma 3, delle regole deontologiche, nonché in un caso la necessità di precisare, all'interno delle informative e della valutazione d'impatto, i ruoli (di titolare, contitolare o responsabile del trattamento) rispettivamente attribuiti ai centri partecipanti, ai

6

6

sensi degli artt. 24, 26 e 28 del RGPD, e di integrare la valutazione d'impatto individuando, in relazione allo scenario di rischio considerato, misure adeguate in base alla probabilità e gravità dello stesso (v. anche provv. 21 dicembre 2023, n. 607, doc. web n. 9979453).

In un ulteriore caso il Garante si è espresso con un parere favorevole condizionato nei confronti di un consorzio *no profit* (composto dai principali ospedali pediatrici italiani e dipartimenti di pediatria nonché da reti terapeutiche pediatriche nazionali ed internazionali) per la realizzazione della fase retrospettiva di uno studio concernente una sorveglianza ospedaliera sulle infezioni del tratto respiratorio inferiore nei reparti di emergenza e in quelli di terapia di dodici principali ospedali pediatrici e/o dipartimenti pediatrici italiani (provv. 16 novembre 2023, n. 551, doc. web n. 9983501).

In particolare, il Garante, ritenendo che il titolare avesse correttamente individuato le basi giuridiche del trattamento, gli adempimenti necessari per assicurare effettiva applicazione al principio di trasparenza, adeguate misure tecniche organizzative per circoscrivere i rischi connessi ai trattamenti, ivi inclusa la pseudonimizzazione dei dati *ex art.* 89 del RGPD, ha rilevato solamente la mancata descrizione delle misure per l'anonimizzazione e l'aggregazione dei dati degli interessati e pertanto condizionato il parere, ribadendo le indicazioni già fornite nei precedenti pareri.

Si segnala un'altra istanza di consultazione preventiva presentata da una azienda ospedaliera universitaria, avente ad oggetto la realizzazione di un emendamento a uno studio retrospettivo, osservazionale, sul quale il Garante aveva espresso il parere di competenza con il provvedimento 7 aprile 2022, n. 118 (doc. web n. 9772545). Tale emendamento, funzionale alla descrizione di eventuali cambiamenti nel quadro epidemiologico e clinico in seguito alla pandemia da SARS-COV-2, ha riguardato l'ulteriore estensione del periodo di osservazione degli accessi in pronto soccorso della popolazione di età inferiore ai 18 anni, fino al mese di aprile 2023, indipendentemente dalle motivazioni del ricovero.

Il Garante, con provvedimento 7 dicembre 2023, n. 582 (doc. web n. 9971457) ha espresso parere favorevole condizionato ribadendo la necessità di pubblicare l'informativa nella versione emendata, sui siti web del promotore e delle aziende sanitarie della regione, in conformità con gli artt. 14, par. 5, lett. b), del RGPD e 6, comma 3, delle regole deontologiche.

6.2. Chiarimenti in merito all'art. 110-bis, comma 4, del Codice

Il Garante, in riscontro a un'istanza di consultazione preventiva avanzata da un istituto di ricovero e cura a carattere scientifico (IRCCS) per la realizzazione di uno studio relativo al trattamento anche di dati personali di pazienti deceduti o persi al *follow up* rientrante nelle linee di ricerca dell'istituto stesso, ha fornito specifici chiarimenti in ordine all'art. 110-bis, comma 4, del Codice secondo il quale “non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento” (nota 18 luglio 2023).

In via preliminare, è stato chiarito che la disposizione non riguarda la ricerca medica biomedica ed epidemiologica, giacché quest'ultima trova la sua speciale disciplina nell'art. 110 del Codice, che per altro, nelle ipotesi di impossibilità di acquisizione del consenso, tiene anche conto delle implicazioni etiche correlate a tali tipologie di trattamenti non contemplate nell'articolo in esame.

6

Posta tale premessa, è stato chiarito che in forza dell'art. 110-*bis*, comma 4, del Codice, gli IRCCS possono legittimamente trattare i dati sulla salute raccolti per scopi di cura, per ulteriori finalità di ricerca scientifica, senza dovere acquisire uno specifico consenso da parte degli interessati ovvero, quando ciò non sia possibile, senza dover ricorrere alla consultazione preventiva del Garante di cui all'ultima parte dell'art. 110, comma 1, del Codice. Più in particolare, la disciplina di settore degli IRCCS ne vincola l'attività a uno stretto controllo da parte del Ministero della salute e al rispetto di specifici standard etici e metodologici (art. 8, d.lgs. n. 288/2003), e ciò, congiuntamente con l'art. 110-*bis* comma 4, del Codice, offre agli IRCCS una specifica base normativa che, ai sensi dell'art. 9, par. 2, lett. j), del RGPD, consente loro di trattare i dati raccolti per finalità di cura anche per ulteriori finalità di ricerca scientifica in campo medico, biomedico epidemiologico.

L'art. 110-*bis*, comma 4, costituisce quindi una di quelle "disposizioni di legge" alle quali fa riferimento l'art. 110 del Codice (primo comma, seconda parte), individuando quale ulteriore adempimento per il trattamento dei dati per scopi di ricerca in campo medico, biomedico e epidemiologico, ai sensi dell'art. 9, par. 2, lett. j), del RGPD, lo svolgimento e la pubblicazione della valutazione d'impatto di cui all'art. 35 del RGPD. Al riguardo è stato altresì precisato che l'art. 110-*bis*, comma 4, del Codice può riguardare sia gli studi monocentrici che quelli multicentrici, in tale ultimo caso limitatamente a quanto previsto dalla specifica normativa di settore in particolare con riferimento alle reti di ricerca degli IRCCS (art. 8, d.lgs. n. 288/2003, cit.).

Sotto altro profilo, atteso che il consenso al trattamento dei dati costituisce una manifestazione di volontà diversa dal consenso informato alla ricerca, il Garante ha ribadito l'obbligo di garantire il rispetto degli standard e della disciplina etica di settore nel contesto di tali ricerche. È stato infine sottolineato che, qualsiasi sia la base giuridica del trattamento, il titolare è tenuto a rispettare i principi applicabili al trattamento e a porre in essere i relativi adempimenti, in particolare, a fornire le informazioni agli interessati, ai sensi degli artt. 13 e 14 del RGPD (artt. 5, 24, 25 e 32 del RGPD).

6.3. Altri provvedimenti in materia di trattamenti per scopi di ricerca scientifica

Nell'anno di riferimento il Garante ha adottato un provvedimento correttivo e sanzionatorio nei confronti di una società proprietaria di una biobanca, a seguito di un reclamo con il quale era stata lamentata l'illegittimità dell'inerzia della società rispetto alla raccolta del consenso degli interessati e all'obbligo di rendere l'informativa, ponendo così fine ad una complessa e annosa vicenda (prov. 27 aprile 2023 n. 170, doc. web n. 9898815).

Il Garante ha ritenuto accertato che la società conservava i dati personali contenuti nella biobanca in violazione dei principi di trasparenza e di responsabilizzazione, di cui all'art. 5, par. 1, lett. a) e par. 2, del RGPD, e dell'obbligo di fornire le informazioni agli interessati, di cui all'art. 14 del RGPD.

L'Autorità ha, in primo luogo, chiarito che la società era legittimamente entrata nel possesso dei dati e dei campioni biologici contenuti nella biobanca, a seguito del fallimento della società cedente, e quindi non era tenuta a richiedere il consenso degli interessati essendo la legittima cessionaria. Tuttavia, tale consenso era necessario per lo svolgimento delle ulteriori operazioni di trattamento necessarie al perseguimento di scopi di ricerca. Al riguardo, avendo la società lamentato di non poter definire, con il grado di dettaglio richiesto dalla disciplina di settore, lo scopo di ricerca scientifica rispetto al quale richiedere il consenso, specifico, degli interessati

6

(art. 7 del RGPD), l'Autorità ha osservato che per "ricerca scientifica" si intende un progetto di ricerca istituito in conformità con le pertinenti norme metodologiche e deontologiche settoriali, nonché con le buone prassi (cfr. linee guida 5/2020 sul consenso ai sensi del RGPD adottate dal CEPD, e *Opinion on scientific research* del GEPD del 6 gennaio 2020). In base alla documentazione in atti, è emerso che la società aveva acquisito la biobanca per il precipuo scopo di proseguire nello specifico progetto di ricerca in campo medico per il quale la biobanca era stata originariamente costituita, e che pertanto conosceva con sufficiente dettaglio gli scopi di ricerca che avrebbe dovuto quanto meno proseguire.

Anche se la società non aveva in concreto svolto ulteriori operazioni di trattamento per scopi di ricerca scientifica, a causa dei sequestri giudiziari all'epoca ancora in corso, il Garante ha tuttavia accertato che la stessa non aveva reso alcuna informativa agli interessati, né ai sensi dell'art. 13, comma 4, del Codice, vigente all'epoca dei fatti, né successivamente all'entrata in vigore del RGPD, ai sensi degli artt. 13 o 14 di quest'ultimo.

In merito all'asserita impossibilità di verificare il contenuto specifico della banca dati e degli ulteriori beni acquisiti, e conseguentemente di definire lo scopo e le operazioni di trattamento da svolgere, il Garante ha rilevato come l'informativa sia un documento del quale il titolare del trattamento può modificare e aggiornare il contenuto, nel corso del tempo, a seconda delle esigenze correlate al caso concreto. In particolare, tenuto conto che la società non aveva raccolto dati presso gli interessati, ma presso un soggetto terzo, tale obbligo avrebbe dovuto essere adempiuto nelle modalità di cui all'art. 13, comma 4 del Codice vigente all'epoca e, successivamente all'entrata in vigore del RGPD, in quelle previste all'art. 14 par. 5, lett. b), del RGPD, anche tramite idonee forme di pubblicità.

Il Garante ha ritenuto, inoltre, che l'assoluta inerzia dimostrata dalla società, pur nel contesto oggettivamente complesso e peculiare in cui si è svolta tutta l'articolata vicenda in esame, evidenziasse una condotta diametralmente opposta a quella ispirata al principio di responsabilizzazione introdotto dal RGPD e comportasse, pertanto, anche la violazione dell'art. 5, par. 2, del RGPD.

Merita di essere evidenziato in questa sede il provvedimento correttivo e sanzionatorio adottato nei confronti di un istituto privato di ricovero e cura a carattere scientifico (IRCCS), a seguito di specifici accertamenti ispettivi (prov. 14 settembre 2023, n. 400, doc. web n. 9941205). Il Garante ha rilevato l'illiceità del trattamento di dati personali effettuato dall'IRCCS in questione, in quanto effettuato in violazione dei principi di liceità, di minimizzazione, di *privacy by design* e *by default*, di integrità e riservatezza e di responsabilizzazione (artt. 5, par.1, lett. c) e f) e par. 2; 24, 25 e 32 del RGPD e 110 del Codice).

Il Garante ha stabilito che i trattamenti di dati personali, in particolare quelli necessari per le ricerche finanziate dal Ministero della salute, ai sensi dell'art. 12-bis, d.lgs. n. 502/1992 e nello specifico quelli di selezione, raccolta, archiviazione e pseudonimizzazione dei dati, erano stati svolti in termini generali in violazione del principio di responsabilizzazione e, in quanto rimessi quasi integralmente a operazioni manuali svolte dagli addetti, in violazione del principio di *privacy by design* e *by default* di cui all'art. 25 del RGPD. È stata infatti accertata l'inefficacia delle misure descritte rispetto all'obbligo di protezione dei dati per impostazione predefinita, laddove impartire specifiche istruzioni ai propri addetti e autorizzati costituisce un adempimento specifico e autonomo della normativa di riferimento (art. 29 del RGPD e 2-*quaterdecies* del Codice) che non può tuttavia sostituire o sopperire all'obbligo del titolare di adottare misure che, per impostazione predefinita e senza necessariamente l'intervento umano, favoriscano l'effettiva applicazione dei principi in materia di protezione dei dati di volta in volta rilevanti e la riduzione dei rischi

per i diritti e le libertà degli interessati, correlati al trattamento, ai sensi dell'art. 25 del RGPD.

L'Autorità ha inoltre accertato la violazione dell'art. 110, comma 1, del Codice, in quanto l'istituto non aveva svolto e pubblicato la valutazione di impatto ivi prescritta per ogni ricerca finanziata ai sensi dell'art. 12-*bis* del citato d.lgs. n. 502/1992. Alla luce delle violazioni accertate, il Garante ha ingiunto al titolare di conformare i trattamenti alle disposizioni del RGPD adottando specifiche misure correttive.

Il Garante ha, infine, reso parere favorevole sullo schema di decreto recante disposizioni concernenti le modalità di trasmissione telematica dei contenuti informativi relativi alla dichiarazione di consenso all'utilizzo del proprio corpo e dei tessuti *post mortem*, ai fini di studio, di formazione e di ricerca scientifica, in attuazione dell'art. 3 della l. n. 10/2020 (prov. 30 novembre 2023, n. 555, doc. web n. 9966628). Lo schema di decreto e il relativo disciplinare tecnico, sottoposti al Garante dal Ministero della salute, hanno tenuto conto delle osservazioni formulate dall'Ufficio nel corso delle numerose interlocuzioni con il Ministero. È prevista, in particolare, l'istituzione di una specifica sezione all'interno della banca dati delle Disposizioni anticipate di trattamento (DAT), tenuta presso il Ministero della salute, in qualità di titolare del relativo trattamento, dove le ASL dovranno inserire telematicamente e senza indugio le dichiarazioni di consenso dei donatori.

Oltre alle informazioni relative al donatore, le dichiarazioni di consenso dovranno contenere anche una serie di elementi quali i dati del fiduciario e del sostituto nominati dal donatore, l'accettazione della nomina da parte del fiduciario e del sostituto, la dichiarazione di consenso da parte di entrambi i genitori nel caso di donatori minorenni nonché le eventuali revoche. Le dichiarazioni dovranno essere redatte per atto pubblico o per scrittura privata autenticata, ovvero consegnate di persona dal donatore all'ufficio di stato civile del comune di residenza o alle strutture sanitarie, oppure comunicate attraverso videoregistrazione o dispositivi che permettano al donatore con disabilità di interagire. In tutti i casi le dichiarazioni dovranno comunque essere trasmesse all'ASL di appartenenza, cui spetta l'obbligo di conservarle e di trasmetterle telematicamente alla banca dati delle DAT. I dati, infine, potranno essere diffusi dal Ministero della salute solo in forma anonimizzata e aggregata e dovranno essere cancellati dopo dieci anni dal decesso del donatore, ovvero al compimento del 18esimo anno di età nel caso di donatori minorenni.

Lo schema di decreto prevede l'adozione di misure tecniche e organizzative al fine di garantire l'integrità e la riservatezza dei dati personali raccolti nella banca dati, conformemente agli obiettivi di protezione descritti nel disciplinare tecnico di cui all'all. 1 dello schema, nonché procedure di sicurezza relative al *software* e ai servizi telematici, in conformità alle linee guida contenenti le regole tecniche adottate ai sensi dell'art. 71 del CAD. Esso disciplina, infine, l'esercizio dei diritti previsti dagli artt. da 15 a 18 e dall'art. 21 del RGPD, secondo le modalità indicate nell'informativa fornita a cura dell'azienda sanitaria che raccoglie la dichiarazione, ai sensi dell'art. 13 del RGPD.

6

7 La statistica

7.1. La statistica ufficiale

Nell'ambito dei trattamenti svolti per finalità di statistica ufficiale merita di essere evidenziato il provvedimento di ammonimento e correttivo reso nei confronti dell'Istituto nazionale di statistica (ISTAT), a seguito degli accertamenti ispettivi svolti dall'Autorità al fine di verificare l'osservanza delle disposizioni in materia di protezione dei dati personali, con specifico riferimento alle modalità di implementazione delle misure di cui al provvedimento 23 gennaio 2020, n. 10 (doc. web n. 9261093). Con tale provvedimento, l'Autorità ha completato il processo di autorizzazione dei trattamenti di dati personali necessari alla realizzazione del censimento permanente, prescrivendo all'ISTAT, tra l'altro, di adottare tecniche di pseudonimizzazione idonee ad assicurare l'efficace attuazione dei principi di protezione dei dati personali, e in particolare dei principi di minimizzazione, di limitazione della finalità e della conservazione, in conformità agli obblighi di *privacy by design* e *by default* (artt. 5, par. 2, lett. b), c) ed e) e 25, del RGPD).

Il Garante nel citato provvedimento del 2020 aveva, tra le altre cose, rilevato specifiche criticità in relazione all'attribuzione di un codice univoco che identifica l'individuo nelle diverse banche dati dell'ISTAT; aveva quindi prescritto all'ISTAT di introdurre un meccanismo di disaccoppiamento gerarchico dei codici pseudonimi nelle varie basi di dati e di rotazione degli stessi nel tempo.

Nel richiamato provvedimento di ammonimento, il Garante ha in particolare accertato che, a seguito della classificazione dei dati degli archivi amministrativi, l'ISTAT non aveva previsto specifiche misure differenziate rispetto ai rischi correlati alle diverse classi di dati trattati, in violazione del principio di responsabilizzazione e degli obblighi di *privacy by design* e *by default*, di cui agli artt. 5, par. 2 e 25 del RGPD.

L'Autorità ha inoltre rilevato che l'Istituto, nonostante la mole di dati che gestisce per il perseguimento dei propri scopi istituzionali, al netto di misure di carattere organizzativo, nella gestione dei domini specifici di integrazione non aveva ancora previsto interventi di natura tecnica volti a rilevare in forma automatizzata la presenza di singolarità e a mitigare i rischi di re-identificazione che da queste discendono. L'assenza di specifiche misure tecniche volte a garantire l'effettiva applicazione del principio di minimizzazione ha determinato altresì la violazione degli artt. 5, par. 2, 24 e 25 del RGPD.

Il sistema di pseudonimizzazione implementato dall'Istituto rispetto a ciascuna unità statistica che confluisce nel Sistema integrato dei microdati si limita a calcolare un codice *hash*. Al riguardo, il Garante ha osservato che se la tecnica di *hashing* su un piano formale risulta idonea a garantire l'univocità degli pseudonimi, la circostanza che la creazione della chiave segreta, impiegata per la generazione degli pseudonimi, sia legata a un parametro estremamente volatile (quale l'ora corrente al millisecondo) rende la "reversibilità controllata" della tecnica di pseudonimizzazione inapplicabile su un piano concreto.

Inoltre, la pseudonimizzazione realizzata dall'ISTAT non prevedeva ancora l'impiego di chiavi segrete casuali diversificate per unità statistica; di conseguenza, in caso di incidente di sicurezza, anche su una sola unità statistica, nota la sintassi del dato, la compromissione del dominio d'integrazione sarebbe stata totale.

Il Garante ha inoltre osservato come, essendo stato realizzato un unico dominio di integrazione, non sia stato possibile verificare – a distanza di tre anni dall'adozione

del provvedimento oggetto di ottemperanza – l'introduzione del prescritto meccanismo di disaccoppiamento gerarchico dei codici nelle varie basi di dati e di rotazione degli stessi nel tempo, rilevando anche, in relazione a tale aspetto, la violazione degli artt. 25 e 32 del RGPD.

L'Autorità, pertanto, ai sensi dell'art. 57, par. 1, lett. a), del RGPD ha dichiarato l'illiceità del trattamento dei dati personali effettuato dall'ISTAT, ammonito l'Istituto per aver violato gli artt. 5, par. 2, 24, 25 e 32 del RGPD e ingiunto a quest'ultimo di conformare i trattamenti alle disposizioni del RGPD, adottando specifiche misure correttive (provv. 8 giugno 2023, n. 337, doc. web n. 9921184).

Con provvedimento 16 novembre 2023, n. 523 (doc. web n. 9966570) il Garante ha espresso parere favorevole condizionato sullo schema di Programma statistico nazionale 2023-2025 (PSN) presentato dall'ISTAT ai sensi degli artt. 58, par. 3, lett. b) e par. 2, lett. f), del RGPD, 6-*bis*, d.lgs. n. 322/1989 e 4-*bis* delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, all. A.4 al Codice.

Nello schema di PSN 2023-2025 sono indicati i lavori statistici che saranno condotti dall'ISTAT e da altri soggetti del SISTAN (Sistema statistico nazionale) nel corso della nuova programmazione triennale.

Nel parere il Garante ha preso atto che i prospetti informativi dei lavori statistici erano stati redatti utilizzando il nuovo schema di rappresentazione delle informazioni elaborato a seguito di un percorso di collaborazione istituzionale con l'Autorità, volto a rendere i predetti prospetti informativi più chiari e coerenti con il quadro normativo in materia di protezione dei dati personali (art. 6-*bis*, comma 1-*bis*, d.lgs. n. 322/1989).

Nonostante l'istruttoria svolta abbia riguardato il PSN quale atto normativo che incide sul trattamento di dati personali, per il quale è obbligatoriamente previsto il coinvolgimento del Garante in sede consultiva (art. 6-*bis*, d.lgs. n. 322/1989), come di consueto essa è stata orientata altresì ad assicurare l'effettiva conformità nell'ambito dei richiamati trattamenti ai principi in materia di protezione dei dati personali sanciti dal RGPD (artt. 5 e 25).

Il Garante ha formulato osservazioni su specifici lavori statistici a partire da quello denominato IST-02854 *Hate speech online*, in relazione al quale ha ritenuto necessario che nella sezione "obiettivo" del prospetto informativo venisse inserita nuovamente la precisazione che la classificazione dei dati operata attraverso strumenti di *machine learning* non sarà interamente automatizzata, ma sempre supervisionata umanamente, condizionando in tal senso il parere favorevole.

Il Garante ha quindi ricordato i vincoli, in termini di protezione dei dati e trasparenza, che dovrebbero essere rispettati con riferimento al trattamento di dati personali effettuati tramite strumenti di intelligenza artificiale, richiamando, anche sulla base di un'importante sentenza del Consiglio di Stato (Cons. St., sez. VI, 13 dicembre 2019, n. 8472): i) il principio di conoscibilità, per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardano e, in questo caso, a ricevere informazioni significative sulla logica utilizzata; ii) il principio di non esclusività della decisione algoritmica e iii) il principio di non discriminazione algoritmica, secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, nonché al fine di garantire la sicurezza dei dati personali, secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche, ovvero i fattori che comportano misure aventi tali effetti (cfr. anche il decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di intelligenza artificiale pubblicato dal Garante il 10 ottobre 2023, doc. web n. 9938038).

7

Programma statistico nazionale

7

È stata quindi ribadita la centralità della supervisione umana e come essa dovrebbe essere svolta da esperti altamente qualificati, al fine di assicurare il rispetto del diritto di non essere assoggettato a una decisione basata esclusivamente su un trattamento automatizzato. Al riguardo è altresì indispensabile, come indicato nel richiamato decalogo del Garante, che nell'addestramento e nell'utilizzo dell'algoritmo sia assicurata la qualità dei dati espressa anche in termini di completezza e di rappresentatività dei soggetti i cui dati si intendono analizzare.

Nell'ambito dell'istruttoria svolta in relazione allo schema di PSN in esame, l'Ufficio ha chiesto poi specifici chiarimenti in ordine alla qualificazione dei lavori statistici svolti dell'Istituto superiore di sanità (ISS) aventi per oggetto registri di patologia, nello specifico se trattasi di statistiche da indagini (SDI) o di statistiche da fonti amministrative e da nuove fonti di dati (SDA).

La differenza risulta particolarmente rilevante giacché la statistica da indagine (SDI) presuppone un contatto diretto con l'interessato e, dunque, la possibilità per quest'ultimo di non fornire riscontro alle domande relative ai dati sensibili o giudiziari (che, come noto, sono esenti dal cd. obbligo di risposta ai sensi dell'art. 7, comma 2, d.lgs. n. 322/1989) nonché il diritto per l'interessato di ottenere un'informazione dal rilevatore ai sensi dell'art. 13 del RGPD; per contro, nelle statistiche da fonti amministrative organizzate (SDA) l'ente SISTAN, titolare del lavoro statistico – in virtù del PSN, che funge da base giuridica del trattamento – può raccogliere dati personali, anche inerenti le particolari categorie, presso altri soggetti pubblici o privati, assolvendo agli oneri informativi attraverso il PSN medesimo il quale funge da informativa agli interessati (art. 6, comma 2, delle regole deontologiche).

Sulla base di tali chiarimenti, tenuto conto che i registri di patologia, indicati nel PSN e previsti dal d.P.C.M. 3 marzo 2017, vengono alimentati sulla base dell'obbligo giuridico, gravante secondo la specifica disciplina di settore in capo alle strutture sanitarie (regioni, ASL, centri clinici di riferimento), di trasmettere periodicamente determinate informazioni al titolare del registro medesimo (su base regionale o nazionale), l'Istituto ha ritenuto più corretto riqualificare taluni di detti lavori come statistiche da fonti amministrative (SDA) organizzate, correggendo in tal senso i relativi prospetti informativi del PSN.

Con riguardo, infine, al lavoro IST-00095- Indagine su decessi e cause di morte, in cui è precisato che la diffusione delle variabili in forma disaggregata è necessaria esclusivamente per finalità di ricerca, atteso che tale lavoro statistico include il trattamento di dati relativi alla salute, il Garante nel parere ha ritenuto necessario che l'Istituto rivalutasse la necessità di diffondere le variabili in forma disaggregata vagliando la possibilità di renderle disponibili in tale formato solo ai ricercatori, anche estranei all'ambito SISTAN, nelle forme e sulla base dei canali previsti dalla normativa vigente (art. 5-ter, d.lgs. n. 33/2013) e delle linee guida per l'accesso a fini scientifici ai dati elementari del SISTAN, adottate dal Comitato di indirizzo e coordinamento dell'informazione statistica - COMSTAT, ovvero motivasse tale esigenza in termini più chiari e rigorosi secondo i principi di minimizzazione dei dati e di responsabilizzazione.

Si segnala, da ultimo, che a seguito della deliberazione di promovimento delle nuove regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del SISTAN del 15 aprile 2021 (doc. web n. 9582086), il Garante, nell'anno di riferimento, ha completato la verifica dell'appartenenza alla categoria di soggetti legittimati all'adozione delle regole deontologiche, in riferimento a coloro che hanno manifestato il proprio interesse, ai sensi dell'art. 23, comma 2, del reg. del Garante n. 1/2019 (doc. web n. 9107633), e ha dato avvio alle riunioni di lavoro preordinate all'analisi dello schema preliminare delle nuove regole deontologiche portate alla sua attenzione (art. 25 del reg. del Garante n. 1/2019, cit.).

8 I trattamenti in ambito giudiziario e di sicurezza

8.1. Trattamenti in ambito giudiziario

Nei numerosi reclami ricevuti anche nel 2023 riguardanti la legittimità, dal punto di vista della normativa in materia di protezione di dati personali, della produzione di informazioni in giudizio, il Garante si è dichiarato “incompetente” e ha disposto l’archiviazione secondo un ormai consolidato orientamento. Infatti, l’art. 160-*bis* del Codice stabilisce che la validità, l’efficacia e l’utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali.

In proposito, l’Autorità ha costantemente ricordato che, al fine di salvaguardare l’indipendenza della magistratura nell’adempimento dei suoi compiti giurisdizionali (cfr. cons. 20 del RGPD), il Garante non è competente per il controllo dei trattamenti effettuati dalle autorità giudiziarie nell’esercizio delle loro funzioni giurisdizionali (cfr. artt. 55, par. 3, del RGPD e 154, comma 7, del Codice).

Di seguito si riportano in sintesi alcuni dei casi ove i principi suddetti hanno trovato applicazione.

Il primo riguarda un reclamo avverso una professionista incaricata di effettuare lavori di ristrutturazione dell’immobile di proprietà dello stesso reclamante che avrebbe prodotto in giudizio artatamente prova documentale di un consulente assicurativo che, già in precedenza, aveva prestato la propria attività in suo favore e che ora risultava controparte nel giudizio. L’Autorità ha innanzitutto rilevato che, in caso di devoluzione in giudizio di dati personali, spetta al Giudice adito valutare la liceità del trattamento dei dati personali dell’interessato ai sensi del citato articolo 160-*bis* del Codice. Inoltre il Garante, nell’archiviare il reclamo, ha precisato che la legittimità del trattamento dei dati in tale ambito è assicurata, per le particolari categorie di dati oggetto della documentazione, dall’art. 9, par. 1, lett. f), del RGPD secondo cui il trattamento è lecito se necessario per accertare, esercitare o difendere un diritto in sede giudiziaria e *a fortiori*, per tutti i dati personali, dall’art. 6, par. 1, lett. f), del medesimo RGPD secondo il quale il trattamento è lecito se necessario per perseguire un interesse legittimo del titolare.

Ancora, con riferimento ad una denuncia/querela relativa a un presunto accesso abusivo a un sistema informatico e trattamento illecito di dati, indirizzata anche al Garante, l’interessato aveva lamentato l’illecita acquisizione e produzione in un giudizio civile di dati personali contenuti in atti processuali riguardanti un diverso giudizio, da parte del difensore della controparte processuale, soggetto estraneo al procedimento a cui si riferivano i documenti in questione. Successivamente alla denuncia dei fatti, l’interessato aveva trasmesso all’Autorità il decreto di rinvio a giudizio della competente Procura della Repubblica nei confronti del predetto avvocato per i reati di cui agli artt. 615-*ter* c.p. e 167 del Codice.

Al riguardo, nell’archiviare il procedimento, il Garante ha rappresentato la necessità nel caso in esame di mantenere distinti il profilo del sindacato sulla liceità del trattamento dei dati personali dell’interessato devoluti in giudizio, da quello relativo all’acquisizione degli atti processuali riguardanti l’interessato e al successivo trattamento dei

Produzione di dati in giudizio

8

dati in essi contenuti da parte dell'avvocato. Proprio sotto quest'ultimo aspetto, l'Autorità ha dato atto dell'impossibilità di interferire con l'attività in corso dell'Autorità giudiziaria e dell'obbligo di rispettare i diritti dei soggetti coinvolti (quali, ad esempio, la facoltà di non rendere dichiarazioni a sé pregiudizievoli, *ex art. 64 c.p.p.*). Pertanto, il Garante ha chiarito che, nel caso di specie, non avrebbe potuto comunque effettuare gli accertamenti indispensabili per assumere le determinazioni di competenza, essendo queste ultime condizionate anche all'esito del procedimento penale, quantomeno in ordine all'accertamento dei fatti contestati che risultino di identica natura.

In altro reclamo era stato lamentato che un avvocato, incaricato di procedere al recupero di un credito, aveva comunicato al datore di lavoro dell'interessato che nei mesi successivi gli sarebbe stata notificata un'ingiunzione di pagamento. In seguito alla nota istruttoria inviata dall'Ufficio al fine di richiedere ogni elemento ritenuto utile per la trattazione dell'affare, il titolare aveva precisato che la comunicazione intercorsa con il datore di lavoro del reclamante era prodromica all'esecuzione del pignoramento presso terzi della retribuzione del debitore e dovuta alla necessità di individuare a quale dei due indirizzi indicati sul sito internet della società dovesse eseguirsi la notifica dell'atto.

Il Garante, valutate tutte le circostanze del caso, ha archiviato il reclamo rilevando che il trattamento di dati personali era occorso nell'ambito di un processo di esecuzione forzata (cfr. artt. 543 e ss. c.p.c.) al fine di realizzare la soddisfazione effettiva di un diritto accertato, nella sua esistenza giuridica, nella fase di cognizione. Pertanto sono state ribadite, da un lato, la legittimità del trattamento dei dati per difendere un diritto in giudizio (cfr. artt. 6, par. 1, lett. f) e 9, par. 1, lett. f), del RGPD), e dall'altro, l'incompetenza del Garante a valutare l'eventuale illiceità del trattamento di dati personali prodotti in un giudizio *ex art. 160-bis* del Codice.

Sempre in materia di procedure esecutive, un interessato aveva presentato reclamo al Garante lamentando un illecito trattamento dei propri dati personali in relazione alla vendita giudiziaria di un appartamento di sua proprietà. In particolare, il reclamante aveva rappresentato di aver rinvenuto su vari siti di aste *online*, tra cui quello del tribunale presso il quale era incardinato il procedimento giudiziario in esame, la pubblicazione dei propri dati identificativi (nome e cognome), dolendosi del comportamento negligente del custode giudiziario in merito alla gestione delle procedure di esecuzione forzata. Al riguardo l'Autorità, dando atto che il trattamento in questione risultava effettuato all'interno di un procedimento da parte dell'Autorità giudiziaria e che la figura del custode giudiziario rientra tra gli ausiliari del giudice aventi determinate responsabilità (artt. 65-67 c.p.c.), ha proceduto ad archiviare il reclamo per incompetenza (cfr. art. 55, par. 3, del RGPD e artt. 154, comma 7 e *160-bis* del Codice).

Sul tema in questione, in altra parte della Relazione si dà conto di un giudizio di opposizione avverso un provvedimento di archiviazione del Garante per i descritti motivi (cfr. par. 20.2). Ci riferiamo al caso deciso con sentenza 26 giugno 2023, n. 2 dal Tribunale de L'Aquila per gli aspetti appunto riferiti alla questione di competenza, motivo ulteriore per non accogliere il ricorso.

Con provvedimento 27 aprile 2023, n. 169 (doc. web n. 9896450), il Garante ha ammonito un avvocato per aver trattato illecitamente dati anche sensibili del reclamante a mezzo di notifica telematica di atti giudiziari, ai sensi della legge n. 53/1994, effettuata all'indirizzo PEC della società presso cui l'interessato prestava servizio, anziché a quello personale.

Con provvedimento 31 agosto 2023, n. 388 (doc. web n. 9938413), è stata comminata all'Ordine degli avvocati di Taranto la sanzione amministrativa pecuniaria di euro 20.000,00 per la violazione degli artt. 5, par. 1, lett. a), c) e f), e 10 del RGPD e *2-octies* del Codice, in ragione della divulgazione sul sito istituzionale dell'Ordine di dati giudiziari presenti negli statini d'udienza riferiti ad alcuni interessati. Nell'occasione, il Garante ha segnalato tale criticità al Tribunale di Taranto, al CSM e al

Trattamenti in ambito
forense

Ministero della giustizia, e a seguito di ciò il predetto Tribunale e il Ministero hanno adottato tre circolari indirizzate agli uffici giudiziari per sensibilizzare gli operatori della giustizia sull'importanza della tutela dei dati giudiziari.

Con provvedimento 28 settembre 2023, n. 431 (doc. web n. 9948262), il Garante ha accertato che un legale, in qualità di titolare del trattamento, aveva violato la disposizione di cui all'art. 12 par. 3, del RGPD, non avendo rispettato il termine legale di trenta giorni, stabilito dalla stessa norma, per fornire all'interessato le informazioni relative all'azione intrapresa ai sensi degli artt. da 15 a 22 del RGPD; né è risultato che il medesimo avesse comunicato all'interessato la necessità della proroga del termine per il riscontro alla richiesta di informazioni e dei motivi del ritardo, entro un mese dal ricevimento della richiesta, come pure previsto dal predetto art. 12. Considerando che non risultavano eventuali precedenti violazioni pertinenti commesse dallo stesso titolare, che il livello del danno subito dall'interessato appariva di lievissima entità e che non risultavano sussistere eventuali fattori aggravanti, quali benefici finanziari conseguiti o perdite evitate, direttamente o indirettamente, quale conseguenza della violazione, l'Autorità non ha ritenuto di infliggere una sanzione amministrativa pecuniaria; tuttavia, essendo comunque stata accertata l'illiceità del trattamento, ha applicato all'avvocato l'ammonizione di cui all'art. 58, par. 2, lett. b), del RGPD.

Con provvedimento 16 novembre 2023, n. 528 (doc. web n. 9973749), il Garante ha accertato l'illiceità del trattamento di dati personali sotteso ad una comunicazione di dati personali, effettuata da un avvocato in violazione degli artt. 5, par. 1, lett. c) e 6 del RGPD, e per l'effetto ingiunto al suddetto legale di pagare la somma di 500,00 euro a titolo di sanzione amministrativa pecuniaria; è emerso infatti che il legale aveva trasmesso per conto della sua cliente alla PEC aziendale del reclamante, che è risultata accessibile anche a soggetti terzi, atti relativi a un giudizio civile, inerenti in particolare un sequestro conservativo di una somma sul conto corrente del reclamante, a tutela del credito vantato dalla sua *ex* coniuge.

8.2. Trattamenti da parte di forze di polizia

Il Garante aveva ricevuto un reclamo sull'impiego, da parte di forze di polizia, di "videoriprese da cui sono state ricavate delle fotografie" ai fini di identificazione per la contestazione di illecito amministrativo. Il reclamo è stato archiviato in quanto, ai sensi dell'art. 13 della l. n. 689/1981, gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza, assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica. È stato anche precisato che l'utilizzo di apparecchi video-fotografici non configura l'impiego di sistemi di "riconoscimento facciale", come aveva sostenuto il reclamante, ossia di sistemi informatici specifici che consentono l'identificazione univoca o l'autenticazione di una persona fisica tramite il trattamento dei dati biometrici (cfr., cons. 51 del RGPD).

8.3. Pareri resi su schemi di decreti in ambito giudiziario o in relazione ad attività di polizia

Per quanto riguarda l'attività consultiva del Garante su schemi di decreti non aventi natura regolamentare o di atti amministrativi generali, ai sensi degli artt. 36, par. 4, del RGPD, 154, comma 5-*bis*, del Codice, e 37, comma 4, d.lgs n. 51/2018, il Garante, nel corso del 2023, ha espresso i seguenti pareri:

8

a) parere 17 maggio 2023, n. 254 (doc. web n. 9913657), su uno schema di decreto del Ministero della giustizia volto a definire le modalità di pagamento, anche per via telematica, delle pene pecuniarie applicate dal giudice con sentenza o decreto di condanna, ai sensi e per gli effetti di cui all'art. 181-*bis* del d.lgs. n. 271/1989, recante norme di attuazione, di coordinamento e transitorie del codice di procedura penale;

b) parere 22 giugno 2023, n. 278 (doc. web n. 9921438), su un provvedimento recante le specifiche tecniche del portale dedicato per il deposito di atti processuali e documenti per via telematica nei procedimenti di volontaria giurisdizione da parte delle persone fisiche che stanno in giudizio personalmente, ai sensi dell'art. 36, comma 4, d.l. n. 13/2023 (cd. tribunale *online*);

c) parere 18 luglio 2023, n. 309 (doc. web n. 9921455), reso ai sensi dell'art. 47, comma 1, d.lgs. n. 51/2018, sull'integrazione della convenzione tra Agenzia delle entrate e Ministero dell'interno volta a disciplinare l'accesso alla sezione dell'Anagrafe tributaria denominata Archivio dei rapporti finanziari. Con provvedimento 29 aprile 2021, n. 163 (doc. web n. 9670652), il Garante aveva reso il proprio parere sullo schema originario di convenzione in questione, che risultò favorevole, ma condizionato al recepimento di modifiche di carattere prettamente tecnico-informatico;

d) parere 12 ottobre 2023, n. 487 (doc. web n. 9953490), su un documento volto a definire le specifiche tecniche del portale albo CTU previste dall'art. 16-*novies*, commi 4 e 5, d.l. n. 179/2012, convertito con modificazioni con l. n. 221/2012: in considerazione della rilevata carenza strutturale del documento, e in particolare per la mancanza di indicazioni circa il ruolo e le responsabilità assunte dal Ministero nel trattamento dei dati e in particolare rispetto alla loro sicurezza e integrità, il Garante ha ritenuto che il parere reso non potesse essere positivo;

e) parere 16 novembre 2023, n. 524 (doc. web n. 9973657), su uno schema di provvedimento del Direttore della Direzione generale dei sistemi informativi automatizzati (DGSIA) volto a definire le specifiche tecniche del portale dedicato per il deposito di atti processuali e documenti per via telematica, nei procedimenti di volontaria giurisdizione, da parte delle persone fisiche che stanno in giudizio personalmente, da adottarsi ai sensi dell'art. 36, comma 4, d.l. n. 13/2023, convertito dalla l. n. 41/2023. Il testo trasmesso per il parere teneva conto delle indicazioni rese dal Garante con il parere 22 giugno 2023, n. 278, (doc. web n. 9921438, cit.) nel quale, in particolare, l'Autorità aveva evidenziato alcune lacune del testo originario, relativamente al ruolo assunto dal Ministero e dagli uffici giudiziari nell'ambito del sistema disciplinato, con particolare riferimento alle linee di responsabilità sotto il profilo della protezione dati; alle specifiche garanzie e misure sul piano organizzativo e tecnico necessarie in chiave di tutela degli interessati; ad alcuni riferimenti normativi. Pertanto, il Garante ha espresso parere favorevole sullo schema aggiornato;

f) parere 30 novembre 2023, n. 553 (doc. web n. 9967679), concernente uno schema di provvedimento recante specifiche tecniche per la presentazione delle domande e la tenuta dell'albo dei consulenti tecnici e dell'elenco nazionale dei consulenti tecnici, ai sensi dell'art. 13, quarto comma, delle disposizioni per l'attuazione del c.p.c. e dell'art. 24-*bis* delle stesse disposizioni di attuazione, come novellati dall'art. 4, comma 2, lettera b) e lettera g), d.lgs. n. 149/2022, nonché dell'albo dei periti presso il tribunale di cui all'art. 67 delle disposizioni per l'attuazione del c.p.p., novellato rispetto a quello già oggetto del parere 12 ottobre 2023, n. 487. Con quest'ultimo parere (cfr. *supra*, lett. d), reso sul testo originario delle specifiche tecniche in questione, il Garante aveva ritenuto necessario un chiarimento in ordine ai profili di eventuale responsabilità del Ministero, con particolare riguardo al servizio di presentazione delle domande e di tenuta degli albi dei consulenti tecnici, all'apparenza unico ed erogato dal medesimo dicastero, direttamente o tramite fornitori esterni.

8

Le scelte dell'amministrazione sul profilo della progettazione (art. 25 del RGPD) e delle misure di sicurezza tecniche e organizzative (art. 32 del RGPD) hanno, infatti, indubbe implicazioni sulla protezione dei dati personali (v., tra le altre, la lett. j) del par. 1 dell'art. 5 del RGPD). Si è ritenuto dunque plausibile che, ferma restando la titolarità dei trattamenti concernenti la tenuta dei propri albi da parte dei singoli tribunali, il Ministero della giustizia avesse comunque un ruolo sul trattamento dei dati realizzati mediante tali albi, in particolare per quanto attiene ai profili di sicurezza. Con riguardo a tale ultimo aspetto, il menzionato parere del 12 ottobre aveva richiesto di integrare il testo con la previsione di alcune, specifiche, misure applicative idonee a garantire un livello di sicurezza effettivamente adeguato ai rischi connessi al trattamento. Il provvedimento successivamente sottoposto si conformava a queste indicazioni, sicché il parere del Garante è stato favorevole.

8.4. *Il controllo sul CED del Dipartimento della pubblica sicurezza*

A seguito di segnalazioni ricevute, anche nel 2023 l'Autorità, nei limiti di quanto rimesso alle sue competenze in tale ambito, ha assicurato il riscontro da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e di uffici periferici di polizia alle richieste degli interessati, sia di accesso e comunicazione dei dati conservati presso il CED, sia di eventuale rettifica degli stessi, nel rispetto delle disposizioni previste dall'art. 10, l. n. 121/1981, cui fanno rinvio gli artt. 47 e 48 del d.lgs. n. 51/2018.

8.5. *Il controllo sul Sistema di informazione Schengen*

Il Sistema di informazione Schengen (SIS II) permette alle autorità nazionali di polizia, di controllo delle frontiere e doganali di scambiarsi agevolmente informazioni sulle persone che potrebbero essere coinvolte in reati gravi. Con l'eliminazione dei controlli alle frontiere interne, il SIS svolge un ruolo essenziale nel facilitare la libera circolazione delle persone nello spazio Schengen. Nel Sistema sono inoltre contenute segnalazioni sulle persone scomparse, soprattutto minori, e informazioni su determinati beni, quali banconote, automobili, furgoni, armi da fuoco e documenti di identità che potrebbero essere stati rubati, sottratti o smarriti.

8.5.1. *Follow up della valutazione Schengen relativa all'Italia*

Nell'ottobre del 2023 è pervenuto il *report* finale della Commissione europea risultante dalla valutazione dell'Italia condotta nel 2021, che aveva dato luogo a specifiche attività di verifica da parte del Garante di cui si è dato conto nella Relazione 2022, p. 96.

Per quanto riguarda la parte di competenza dell'Autorità, la valutazione è di conformità, pur richiedendo alcuni miglioramenti (*compliant but improvement necessary*). A tale proposito, la Commissione, considerando necessaria la predisposizione di regolari attività di verifica, ha sottolineato come l'Autorità non avesse predisposto un piano di ispezione annuale o pluriennale. Relativamente, poi, alle attività di audit sui dati trattati dalla sezione nazionale del SIS (N.SIS), il *team* di valutazione, pur riconoscendo che l'Autorità aveva iniziato a svolgere detta attività, ha tuttavia rilevato come la medesima non si fosse ancora conclusa ed ha quindi esortato l'Autorità a portarla a compimento.

A tale riguardo, sul finire dell'anno sono entrate in fase ultimativa le pertinenti istruttorie in vista della conclusione formale dell'attività di controllo del Garante sul N.SIS.

8

8.5.2. Attività di controllo e monitoraggio sul SIS II

Come noto, ai fini dell'esercizio dei diritti relativamente ai dati registrati nel SIS II, l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale dell'archivio Schengen, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto). L'intervento del Garante avviene in seconda battuta, qualora l'interessato gli si rivolga perché non si ritiene soddisfatto del riscontro fornito dal Dipartimento in questione.

Il Ministero invia trimestralmente all'Autorità *report* statistici, privi di dati di natura personale, contenenti informazioni di dettaglio (nazionalità dei richiedenti, uffici di polizia coinvolti, tipologia delle richieste, ecc.), idonee a monitorare il flusso delle istanze degli interessati e la conseguente attività di riscontro compiuta dal Dipartimento della pubblica sicurezza.

Nel corso del 2023, si è assistito ad un incremento del numero delle richieste degli interessati indirizzate direttamente al Garante rispetto all'anno precedente; tra queste poi sono risultate costanti in termini percentuali quelle di interessati che lamentano un insoddisfacente o erroneo riscontro alle proprie richieste da parte dell'autorità di polizia e, pertanto, ricorrono al Garante al fine di vederle soddisfatte.

Infine, si continua a rilevare un costante calo delle richieste di accesso da parte di autorità nazionali di controllo di altri Stati UE, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane.

Le relative informazioni vengono comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni di cui agli artt. 57 del reg. 1861/2018 e 71 del reg. 1862/2018.

9 L'attività giornalistica

L'Autorità ha continuato a dedicare particolare attenzione agli aspetti connessi alla libertà di manifestazione del pensiero, operando una costante attività di bilanciamento tra la libertà di informazione, da un lato, e il rispetto dell'identità personale e la protezione dei dati personali, dall'altro. Ciò è avvenuto attraverso l'esame del considerevole numero di reclami e segnalazioni pervenuti volti a lamentare violazioni connesse alla diffusione di notizie in rete e sui *social media* da parte degli organi di informazione.

9.1. Dati statistici e aspetti procedurali

Le istanze rivolte all'Autorità nel settore in esame sono pervenute, in numero sostanzialmente equivalente, sotto forma di segnalazioni e di reclami, rispetto ai quali, in talune ipotesi, è stato necessario richiedere la regolarizzazione a causa della mancanza dei necessari presupposti di forma e di sostanza richiesti dalla normativa di riferimento. In numerosi casi tale regolarizzazione ha interessato i reclami in materia di esercizio dei diritti di cui agli artt. 15-22 del RGPD, ove gli stessi sono risultati privi dell'interpello preventivo effettuato dall'interessato nei confronti del titolare del trattamento, così come previsto dall'art. 15 del reg. del Garante n. 1/2019.

Un numero significativo di istanze è pervenuto anche sotto forma di segnalazioni, alcune delle quali, a seguito di una valutazione preliminare, hanno dato impulso ad un'attività istruttoria secondo la procedura prevista per i reclami, essendo stata ravvisata la sussistenza dei presupposti di una possibile violazione di legge.

Sono altresì pervenute diverse istanze di natura mista (atti di diffida e/o interPELLI preventivi rivolti direttamente ai titolari del trattamento e trasmessi per conoscenza all'Autorità), così come diverse segnalazioni inviate dall'Autorità giudiziaria e riguardanti notizie di reato aventi una supposta rilevanza in materia di protezione dei dati personali.

Una considerevole parte dei reclami definita nel 2023 ha riguardato le istanze rivolte ai gestori dei motori di ricerca, — principalmente Google, per rilevanza e numero di casi — finalizzate ad ottenere la deindicizzazione di contenuti reperibili in associazione al nominativo dell'interessato (cd. *delisting*). Non sono mancate, in ogni caso, istanze che hanno riguardato altri motori di ricerca, quali Microsoft Corporation e Verizon Media Emea Limited, titolare del motore di ricerca Yahoo!.

Gli organi di informazione (testate giornalistiche, *blog*, siti di informazione, ecc.) sono stati destinatari di una parte ugualmente rilevante dei reclami. In tali casi gli interessati avevano principalmente lamentato la pubblicazione di articoli (ma anche *e-book*) contenenti dati personali ritenuti eccedenti, in particolare rispetto al principio di essenzialità dell'informazione nei trattamenti per fini giornalistici, o diffusi in violazione di specifici limiti (dati relativi alla salute, talvolta connessi alla diagnosi di Covid-19, nonché dati relativi a minori). Un ulteriore ambito di intervento ha riguardato la lamentata pubblicazione di fotografie, commenti e video anche sui *social network* in assenza del consenso dell'interessato o di un'altra idonea base giuridica.

Con specifico riguardo all'esercizio dei diritti di cui agli artt. 15-22 del RGPD, si è registrata, durante il procedimento, la frequente adesione da parte dei titolari del trattamento alle originarie richieste dei reclamanti; ciò ha consentito, in molti casi, di definire i reclami senza l'adozione di provvedimenti collegiali.

9

Nei casi in cui, invece, sono stati ravvisati i presupposti per interessare il Collegio, quest'ultimo si è dovuto esprimere operando un delicato bilanciamento tra le richieste del singolo e l'interesse pubblico generale all'informazione, ricorrendo – laddove necessario – all'uso dei poteri correttivi previsti dal RGPD.

Nelle circostanze di maggiore gravità il Garante ha ritenuto di applicare, rispetto alla rilevata illiceità della condotta del titolare del trattamento, anche misure sanzionatorie di tipo pecuniario, tenendo comunque conto delle peculiarità legate all'esercizio di tale potere correttivo in un ambito di particolare delicatezza come quello della libertà di manifestazione del pensiero.

9.2. *Trattamento di dati nell'esercizio dell'attività giornalistica*

9.2.1. *Dati giudiziari*

Nell'affrontare il tema ricorrente dell'utilizzo di immagini a corredo di articoli giornalistici di cronaca giudiziaria, l'Autorità ha ritenuto infondata la richiesta di un reclamante volta a far rimuovere da diverse testate giornalistiche un'immagine che ritraeva il suo volto in primo piano, unitamente ad analoghe fotografie di altre venti persone con lui indagate in un procedimento giudiziario e pubblicate in un momento immediatamente successivo all'esecuzione dell'ordinanza di custodia cautelare in carcere. Si è ritenuto, infatti, che la pubblicazione dell'immagine in questione appariva supportata da ragioni di interesse pubblico in considerazione della gravità delle accuse, rivelatesi poi fondate nel giudizio di primo grado. Inoltre, nel caso di specie, la pubblicazione della fotografia poteva ritenersi rispondente a esigenze di identificazione più precisa del soggetto indagato (provv.ti 23 febbraio 2023, n. 99, doc. web n. 9890255; n. 100, doc. web n. 9890983; n. 101, doc. web n. 9891143; n. 102, doc. web n. 9907828 e n. 103, doc. web n. 9892670).

9.2.2. *Illecita diffusione di dati sanitari*

Il tema della diffusione di informazioni connesse ai contagi da Covid-19 è stato oggetto di alcuni provvedimenti dell'Autorità anche nell'anno di riferimento.

In particolare, sono state ritenute fondate le doglianze di un interessato il quale aveva lamentato la pubblicazione, da parte di una testata giornalistica, di dati personali – il nome e cognome e la carica ricoperta all'interno di un ministero – unitamente all'informazione di essere “risultato positivo al *virus*, poi negativizzatosi, ma ancora in isolamento”. L'Autorità ha rilevato che, pur nel quadro di un legittimo esercizio del diritto di cronaca e di critica su fatti di interesse generale (l'osservanza delle disposizioni governative di contenimento dei contagi all'interno degli uffici pubblici e, in particolare, di quelli deputati a garantire il rispetto delle disposizioni stesse), l'esplicitazione dei dati identificativi del reclamante risultasse un trattamento eccedente, non giustificato da un ruolo di particolare rilievo pubblico da attribuirsi all'interessato. In ragione della violazione riscontrata, afferente a dati personali relativi allo stato di salute, il Garante, oltre a vietare l'ulteriore trattamento dei dati, ha comminato al titolare del trattamento una sanzione pecuniaria (provv. 11 gennaio 2023, n. 15, doc. web n. 9861268).

L'Autorità ha parimenti ritenuto fondato un reclamo e sanzionato un editore in relazione ad un servizio giornalistico nel quale erano stati pubblicati i dati personali (compresa la fotografia) della reclamante in associazione ad informazioni non esatte relative al proprio stato di salute (isolamento da tampone), pur a fronte di idonea documentazione fornita dall'interessata comprovante l'inesattezza del dato. Nel precisare che “l'aver eseguito un tampone costituisce un'informazione che il Garante ha ritenuto più volte riconducibile al dato sulla salute, indipendentemente

dal suo esito, in quanto legata all'esecuzione di una prestazione sanitaria", l'Autorità ha ricordato che è dovere del giornalista verificare l'attendibilità e correttezza delle informazioni e correggere le informazioni inesatte, come richiamato anche dall'art. 4 delle regole deontologiche. Il titolare del trattamento è stato altresì sanzionato per non aver fornito riscontro ad una preventiva istanza formulata dall'interessata nell'esercizio dei diritti di cui agli artt. 15-21 del RGPD (prov. 26 ottobre 2023, n. 506, doc. web n. 9955735 – provv. impugnato dinanzi al Trib. di Avellino).

L'Autorità è intervenuta dichiarando invece infondato un reclamo che lamentava, nel contesto di un articolo di cronaca, la diffusione di informazioni relative alla contrazione del *virus* Covid-19 da parte di un assessore comunale, non avendo ritenuto eccedente il trattamento dei dati relativi allo stato di salute dell'interessato in ragione del ruolo pubblico rivestito da quest'ultimo nella comunità locale di riferimento e della valenza del richiamo al suo stato di salute rispetto alla regolare funzionalità degli organi dell'amministrazione comunale. I dettagli forniti nell'articolo, inoltre, non si erano rivelati lesivi della dignità dell'interessato e, nella versione cartacea, la notizia aveva avuto diffusione unicamente in ambito locale. L'Autorità ha ritenuto non eccedente anche la pubblicazione, a corredo del menzionato articolo, della fotografia del reclamante in ragione della circostanza che la stessa risultava pubblicata sul sito web dell'amministrazione, ovvero presente in diversi siti di informazione (prov. 2 marzo 2023, n. 63, doc. web n. 9874436).

Nel 2023 l'Autorità è inoltre intervenuta d'ufficio attraverso l'adozione di provvedimenti di limitazione provvisoria nei confronti di alcune testate che avevano pubblicato dettagli (compreso il referto medico) della patologia da cui risultava affetto un pericoloso criminale. La limitazione imposta ha avuto riguardo all'ulteriore diffusione dei dati sanitari indicati negli articoli in esame. Successivamente l'Ufficio, alla luce degli elementi emersi nel corso dell'istruttoria, ha confermato i provvedimenti di limitazione provvisoria adottati vietando ogni ulteriore trattamento dei dati sanitari diffusi (prov. 13 aprile 2023, n. 134, doc. web n. 9896877 – impugnato dinanzi al Tribunale di Roma – n. 135, doc. web n. 9897055 e n. 136, doc. web n. 9892869).

Sempre in relazione alla diffusione di dati sanitari, l'Autorità è intervenuta vietando la diffusione di dati personali contenuti in un articolo che descrivevano in modo estremamente particolareggiato le condizioni relative alla salute del reclamante in seguito ad una caduta in bicicletta nel 2014, a seguito della quale lo stesso si era rotto una spalla e per la quale aveva chiesto e ottenuto, mediante sentenza di primo grado, un cospicuo risarcimento (prov. 23 marzo 2023, n. 110, doc. web n. 9894184).

9.2.3. Dati relativi a minori

Una particolare attenzione è stata riservata, anche nel periodo di riferimento, alla tutela dei minori, con particolare riguardo al rispetto delle garanzie previste dalle regole deontologiche (art. 7) e dalla Carta di Treviso.

Ad esempio, i genitori di un minore deceduto avevano lamentato la pubblicazione, unitamente alla notizia del decesso, di una serie di informazioni tra cui la (presunta) malattia che ne sarebbe stata causa, nonché di ulteriori dati relativi ai membri della famiglia. Pur avendo preso atto sia dell'avvenuta rimozione, nel corso dell'istruttoria, degli URL che rimandavano agli articoli oggetto di doglianza, sia delle motivazioni avanzate dagli editori circa l'intento di rendere partecipe della tragedia la piccola comunità di appartenenza del minore stesso, l'Autorità ha ritenuto di dover imporre il divieto di ogni ulteriore diffusione dei dati oggetto del procedimento, anche *online*, ivi compreso l'archivio storico, procedendo altresì a comminare una sanzione pecuniaria nei confronti degli editori coinvolti (prov. 8 giugno 2023, n. 247, doc. web n. 9909715 e n. 248, doc. web n. 9909732).

9

9

Sono state ritenute parimenti fondate le segnalazioni di un genitore che lamentava una violazione delle disposizioni a tutela dei minori in relazione alla pubblicazione, da parte di due testate giornalistiche, di una fotografia ritraente la figlia e altre sue compagne a corredo della notizia delle molestie subite dalle stesse durante un viaggio in treno, nel corso del quale si erano imbattute in un gruppo di ragazzi che avevano partecipato a un raduno, degenerato in risse e atti di violenza. Il Garante ha ricordato che il rispetto del principio di essenzialità dell'informazione è da interpretarsi con maggior rigore nei casi in cui le notizie riguardano soggetti minori di età, il cui superiore interesse deve ritenersi prevalente, a maggior ragione quando questi si trovino coinvolti in fatti di cronaca in qualità di vittime di azioni criminose, fattispecie nelle quali deve essere garantito il loro anonimato, evitando qualsiasi elemento informativo idoneo a consentirne l'identificazione anche indiretta (art. 114, comma 6, c.p.p.; art. 7, comma 1, regole deontologiche e Carta di Treviso). Nel caso di specie, l'Autorità ha ritenuto che tali principi erano stati violati e ha quindi vietato l'ulteriore trattamento dei dati e comminato una sanzione alle testate interessate dalla segnalazione (provv. ti 31 agosto 2023, n. 390, doc. web n. 9944538 e n. 391, doc. web n. 9944579). Tali provvedimenti sono stati impugnati dinanzi all'Autorità giudiziaria che, con riguardo a un editore, ha confermato le valutazioni del Garante riducendo tuttavia la sanzione comminata (cfr. Trib. Bologna, I sez. civile, sent. 16 febbraio 2024). Riguardo ad altro editore il procedimento è in corso.

La fondatezza dell'istanza è stata rilevata anche in un caso nel quale l'interessata – minore di età all'epoca alla quale si riferivano i fatti e al momento della presentazione del reclamo – aveva lamentato l'illiceità del trattamento effettuato da una testata giornalistica che aveva pubblicato alcune immagini e un video nel canale YouTube dell'editore, riguardanti un raduno non autorizzato interrotto dall'arrivo delle Forze dell'ordine. Le riprese video erano state effettuate da una distanza che consentiva l'identificazione delle persone presenti, nonostante i loro tentativi di non essere riconosciute. La reclamante aveva eccepito di avere subito un rilevante pregiudizio derivante anche dalla connotazione negativa che l'articolo attribuiva a tutti i partecipanti all'evento. L'Autorità ha accolto il reclamo ponendo a carico del titolare un divieto di ulteriore trattamento dei dati dell'interessata, che erano stati comunque rimossi nel corso del procedimento, nonché il pagamento di una sanzione pecuniaria. È stata ravvisata infatti la violazione del principio di essenzialità dell'informazione, non apparendo rilevante ai fini informativi la diretta identificabilità dell'interessata, alla quale, peraltro, proprio in virtù della sua minore età, doveva essere garantita una particolare tutela in considerazione degli effetti che la sua esposizione, specie se connotata negativamente, poteva avere su un equilibrato sviluppo psico-fisico. È stato inoltre rilevato che, benché fosse possibile che il giornalista, al momento delle riprese, non avesse consapevolezza della minore età dei soggetti ripresi, di tale circostanza l'editore era stato edotto nel momento in cui era stato investito di una richiesta di rimozione, proveniente dall'interessata anteriormente alla presentazione del reclamo, alla quale però non aveva fatto seguito alcun intervento sostanziale (provv. 22 giugno 2023, n. 265, doc. web n. 9910270).

9.2.4. *Dati di personaggi noti*

Nel periodo di riferimento l'Autorità ha avuto modo di precisare l'ambito di un corretto trattamento per finalità giornalistiche anche laddove esso riguardi dati personali relativi a personaggi noti. L'occasione è stata offerta, in particolare, da un reclamo avente ad oggetto la lamentata diffusione, tramite una rivista, di immagini che ritraevano l'interessata in momenti di vita privata mentre si trovava all'interno della propria abitazione con alcuni ospiti. L'Autorità ha accolto il reclamo e sanzionato l'editore, rilevando un uso non corretto di tecniche invasive (art. 3 delle regole deon-

tologiche) e un trattamento di dati personali, anche strettamente privati, eccedente, con un sacrificio della sfera privata della segnalante non proporzionato rispetto alla finalità giornalistica perseguita (prov. 8 giugno 2023, n. 246, doc. web n. 9907956).

9

9.2.5. Notizie di rilevante interesse pubblico e rispetto dell'essenzialità dell'informazione

Anche nel periodo di riferimento l'esame di reclami e segnalazioni riguardanti vicende di cronaca ha costituito occasione per un intervento dell'Autorità teso a ribadire i principi fondamentali della disciplina relativa alla protezione dei dati personali in ambito giornalistico. Tra questi, in particolare, assume rilievo il principio di "essenzialità dell'informazione" – sancito sia nel Codice (art. 137) sia nelle regole deontologiche (artt. 6, 8, 10 e 11) – il quale deve orientare il giornalista per un'informazione corretta e rispettosa dei diritti della persona.

In applicazione del predetto principio l'Autorità ha accolto il reclamo di un interessato che lamentava la pubblicazione dei propri dati identificativi nell'ambito di un articolo riportante la notizia di un furto subito dal medesimo. Ciò è in linea con un principio consolidato che mira a tutelare i dati idonei a identificare vittime di reati (prov. 13 aprile 2023, n. 139, doc. web n. 9897854).

Sempre con riferimento all'essenzialità dell'informazione è stato parimenti ritenuto fondato un reclamo relativo alla diffusione in un articolo, apparso sul sito internet del quotidiano, contenente una riproduzione fotografica del testamento olografo in cui erano visibili il nominativo, la data, il luogo di nascita, l'indirizzo di residenza e la qualifica di testimone assunta, ai fini della procedura testamentaria, dalla reclamante (prov. 31 agosto 2023, n. 366, doc. web n. 9932951). Fondato è stato ritenuto anche un caso in cui veniva lamentata la pubblicazione, a corredo di un articolo di cronaca riguardante un consigliere regionale, di una fotografia con il nome della strada in cui si trovava la sua abitazione e l'evidenza del relativo ingresso, in ragione dell'ubicazione dell'immobile in una zona caratterizzata da una ridotta densità abitativa che ne consentiva a chiunque l'immediata riconoscibilità (prov. 22 giugno 2023, n. 332, doc. web n. 9924481).

Analogamente è stato valutato un reclamo riguardante un'ipotesi di diffusione, sui *social* di una giornalista ed opinionista, di immagini, successivamente riprese anche da diversi siti *online*, raccolte attraverso la telecamera di un telefono cellulare, e riferibili a due passeggeri durante un volo di linea, allo scopo di documentarne il mancato utilizzo dei necessari dispositivi di protezione nel periodo pandemico. Nel caso di specie non era stato reso evidente il ruolo di giornalista di chi aveva ripreso le immagini, né le finalità della raccolta, in violazione degli obblighi di cui all'art. 2 delle regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica. Inoltre non erano stati adottati opportuni accorgimenti per evitare l'identificabilità dei soggetti interessati, in violazione del principio di essenzialità dell'informazione (prov. 6 luglio 2023, n. 336, doc. web n. 9925450).

L'Autorità è inoltre intervenuta con una declaratoria di fondatezza rispetto ad un reclamo con cui si lamentava l'illiceità del trattamento posto in essere attraverso la pubblicazione di un articolo e di un *e-book* nei quali erano stati diffusi, in violazione del principio di essenzialità dell'informazione, non solo i dati identificativi degli interessati, ma anche altre informazioni personali, nel contesto di una vicenda risalente a molti anni prima in cui era stato coinvolto solo il padre dei reclamanti per abusi perpetrati nel mondo dello sport (prov. 6 marzo 2023, n. 62, doc. web n. 9880427 - confermato dal Trib. Milano, I sez. civile, sent. 30 novembre 2023).

La fondatezza del reclamo è stata valutata anche in relazione a un caso nel quale l'interessata aveva lamentato una violazione della disciplina rilevante con riguardo al trattamento di dati per finalità giornalistiche da parte di un editore che, nel narrare un fatto di cronaca che la riguardava (una rapina avvenuta nel suo appartamento),

9

aveva riportato, sia nella versione cartacea che in quella digitale dell'articolo, numerose informazioni idonee ad identificarla. La testata aveva, in particolare, pubblicato il nominativo dell'interessata e la sua immagine tratta dal profilo Facebook, nonché numerosi dettagli relativi alla sua abitazione e alla scuola frequentata dalla figlia minore in netto contrasto con il principio di essenzialità dell'informazione, ponendo peraltro in una situazione di rischio la medesima e le persone con lei conviventi. Sono stati pertanto imposti un divieto di ulteriore trattamento dei dati in questione e una limitazione all'accessibilità della copia cartacea dell'articolo, conservata nell'archivio della testata (prov. 16 novembre 2023, n. 534, doc. web n. 9967845).

Nessuna eccedenza informativa è stata invece ravvisata nel trattamento posto in essere dall'editore di una testata giornalistica attraverso la pubblicazione di un articolo riportante per esteso le generalità del reclamante e di altri protagonisti di una vicenda relativa alle modalità di accesso a un concorso universitario. L'interessato, infatti, seppure estraneo al procedimento giudiziario in questione, risultava aver rivestito un ruolo di primaria importanza nel caso narrato e la finalità giornalistica connessa alla diffusione dei suoi dati risultava dunque proprio quella di fornire un quadro chiaro di tale contesto. Nell'articolo, peraltro, si ricostruiva la vicenda senza indugiare in commenti o particolari lesivi della dignità del reclamante (prov. 23 marzo 2023, n. 94, doc. web n. 9883685).

È stata ritenuta parimenti infondata la richiesta di rimozione di un articolo pubblicato in tempi molto recenti da una nota testata giornalistica e di cui veniva eccepita la falsità del contenuto e la portata diffamatoria e offensiva, senza, tuttavia, offrire all'Autorità elementi oggettivi di valutazione. Il medesimo interessato rilevava altresì la violazione del principio di essenzialità dell'informazione in quanto l'articolo riportava anche dettagli ultronei, quali l'indirizzo di abitazione e le abitudini di vita. L'Autorità, condividendo le deduzioni avanzate dal titolare del trattamento, ha rigettato il reclamo, affermando, per i profili rilevanti in materia di protezione dei dati personali, l'avvenuto rispetto da parte dell'editore dei principi rilevanti in tale ambito, tenuto conto della sussistenza di un interesse pubblico alla conoscibilità delle notizie ivi contenute (prov. 21 dicembre 2023, n. 618, doc. web n. 9984512).

L'infondatezza della pretesa è stata altresì dichiarata con riguardo a un reclamo relativo alla richiesta di provvedimenti correttivi e sanzionatori a seguito della pubblicazione delle generalità e dell'età del protagonista di una vicenda giudiziaria, definita con una sentenza (recente) di non luogo a procedere per la remissione degli atti di querela, ma di interesse generale, nel pur circoscritto ambito territoriale, in considerazione del profilo di denuncia di comportamenti relativi al contesto scolastico, ai rapporti tra insegnanti e studenti ed all'uso non corretto dei *social* (prov. 21 dicembre 2023, n. 620, doc. web n. 9985641).

Parzialmente infondato è stato giudicato, invece, un caso in cui l'interessato lamentava l'avvenuta pubblicazione delle proprie generalità su alcune testate giornalistiche relativamente a un procedimento penale nel quale era stato coinvolto. Detta diffusione era avvenuta anche in un *blog* nel quale era stato pubblicato il testo di un'ordinanza cautelare emessa, tra gli altri, nei confronti del reclamante, il quale aveva asserito di aver da ciò subito un rilevante pregiudizio. Nell'ordinanza pubblicata, infatti, erano riportati anche dati quali gli indirizzi di residenza ed il numero di utenza cellulare in uso all'interessato, da ritenersi eccedenti rispetto alla finalità informativa connessa all'esercizio del diritto di cronaca. Veniva inoltre contestata l'assenza di un'adeguata informativa all'interno di uno dei siti coinvolti, con specifico riferimento alla mancata indicazione di canali di contatto utili per l'esercizio dei diritti da parte degli interessati. L'Autorità si è pronunciata dichiarando la manifesta infondatezza del reclamo con riferimento alla richiesta di rimozione del nominativo dell'interessato pubblicato dalle testate coinvolte, ribadendo un principio più volte

pronunciato, ovvero che la pubblicazione dei dati identificativi delle persone a carico delle quali è instaurato un procedimento penale non è preclusa dall'ordinamento vigente e va inquadrata nell'ambito delle garanzie volte ad assicurare trasparenza e controllo da parte dei cittadini con riguardo all'attività di giustizia. Con riferimento, invece, al trattamento consistente nella pubblicazione del testo del provvedimento cautelare, ha precisato che l'art. 114, comma 2, del c.p.p. esclude le ordinanze cautelari dal più generale divieto di pubblicazione integrale di atti del procedimento penale non più coperti da segreto istruttorio, rilevando tuttavia l'illiceità del trattamento di alcuni dati ivi contenuti, ritenuti in contrasto con i principi di cui all'art. 137, comma 3, del Codice e all'art. 6, comma 1, delle regole deontologiche, e ponendo un divieto di ulteriore trattamento dei dati in capo al titolare destinatario anche di un ammonimento per le violazioni accertate (provv. 26 ottobre 2023, n. 505, doc. web n. 9954906).

9

9.2.6. Istanze di cancellazione rivolte agli editori

Alcuni provvedimenti dell'Autorità hanno riguardato istanze di cancellazione dei dati rivolte agli editori in sede di esercizio dei diritti (art. 17 del RGPD) e rimaste insoddisfatte. Rispetto a tali fattispecie il Garante ha ritenuto, quale misura proporzionata di bilanciamento tra il diritto all'oblio invocato dal reclamante e la salvaguardia delle finalità di informazione invocate dagli editori, l'adozione da parte di questi ultimi di specifiche misure tecniche volte ad interdire l'indicizzazione degli articoli oggetto di doglianza - salvaguardando tuttavia l'integrità delle notizie, debitamente aggiornate, all'interno degli archivi dei quotidiani.

Ciò è avvenuto con riferimento a un reclamo relativo ad alcuni articoli nei quali il coinvolgimento dell'interessato in una vicenda giudiziaria (nel frattempo definitasi in termini a lui favorevoli) era stato particolarmente circoscritto ("sole due righe, in cui compare con nome e cognome e con le sue qualifiche") rispetto a quello di altri soggetti, menzionati negli articoli in termini assai più ampi (provv. 26 gennaio 2023, n. 29, doc. web n. 9867661).

L'adozione delle citate misure tecniche è stata prevista anche rispetto a un altro reclamo rivolto a diversi editori con il quale l'interessato aveva lamentato la lesività derivante dalla reperibilità, in associazione al proprio nome e cognome, di URL riportanti stralci di un'intercettazione telefonica che fornivano di per sé una lettura idonea ad attribuire al reclamante responsabilità significative, se non determinanti, nell'ambito delle indagini connesse al crollo del ponte Morandi di Genova. Tali responsabilità, tuttavia, non avevano trovato conferma negli esiti delle indagini stesse e nei successivi sviluppi del procedimento, non risultando il reclamante tra le persone indagate e poi imputate in tale ambito (provv. 23 marzo 2023, n. 105, doc. web n. 9893743; n. 106, doc. web n. 9894160; n. 107, doc. web n. 9895432; n. 108, doc. web n. 9895464 e n. 109, doc. web n. 9896373).

Sempre in relazione ai profili relativi alle richieste di esercizio dei diritti di cui agli artt. 15-22 del RGPD, l'Autorità ha adottato un provvedimento di avvertimento nei confronti di un editore che non aveva fornito riscontro a un'istanza dell'interessata (volta ad ottenere la cancellazione di un servizio, risalente nel tempo e lesivo della sua dignità, ripetutamente trasmesso dall'editore nel corso di una rubrica televisiva satirica) argomentando a propria difesa che l'istanza non era stata inviata all'indirizzo *e-mail* indicato nell'informativa resa disponibile sul proprio sito. In particolare l'Autorità ha rilevato che, benché la reclamante avesse utilizzato un canale di comunicazione (la PEC della società) diverso da quello indicato nella menzionata informativa, esso costituiva il recapito elettronico ufficiale (domicilio digitale) del titolare e del relativo Gruppo societario di appartenenza, destinato alla trasmissione di atti aventi valore legale. Il canale utilizzato non risultava dunque estraneo a un

9

possibile impiego anche per l'esercizio dei diritti previsti dalla normativa in materia di protezione dei dati personali, anche alla luce della sua idoneità a fornire una data certa di ricezione della comunicazione stessa (cfr. par. 55 e 57 delle linee guida sul diritto di accesso adottate dal CEPD in data 23 marzo 2023; provv. 26 novembre 2023, n. 535, doc. web n. 9968111).

L'Autorità ha invece ritenuto infondata la richiesta di cancellazione di un servizio televisivo nel quale veniva riproposto un video ed erano rievocati fatti afferenti a un procedimento penale che aveva visto coinvolto, tra gli imputati, il reclamante, e che si era concluso nel 2017 con l'assoluzione dell'interessato. L'Autorità, esaminato il servizio alla luce della disciplina giornalistica e del principio di "essenzialità dell'informazione" sopra ricordato, ha ritenuto che esso fornisce un quadro informativo aggiornato dei fatti e del procedimento penale coinvolgente il reclamante (menzionando anche gli esiti a lui favorevoli). Ciò era avvenuto attingendo a un documento pubblico (sentenza del Tribunale di Milano del 2017, pubblicata anche dal reclamante stesso) nel quale erano riportate informazioni aventi un significativo interesse generale, a prescindere dalla rilevanza penale o meno dei fatti attribuiti al reclamante, il quale aveva la disponibilità di informazioni destinate a essere riservate, relative a personaggi appartenenti al mondo della politica e o dello spettacolo, grazie ad azioni di hackeraggio attribuite a terzi (provv. 13 aprile 2023, n. 140, doc. web n. 9907900).

9.3. *Trattamento di dati da parte dei motori di ricerca*

Come già accennato, i reclami proposti nei confronti dei gestori di motori di ricerca hanno costituito, nel periodo di riferimento, una parte considerevole dei reclami complessivamente pervenuti all'Autorità con riferimento al settore della libertà di informazione.

La maggior parte delle richieste di *delisting* pervenute ha riguardato trattamenti posti in essere tramite il motore di ricerca gestito da Google LLC, cui ha fatto seguito l'attivazione di altrettanti procedimenti. Diversamente, con riguardo alle società che gestiscono altri motori di ricerca – in particolare Microsoft Corporation con riferimento a Bing e Verizon Media con riguardo a Yahoo! – si è fatto ricorso, laddove non fosse stato possibile definire il reclamo a seguito di una richiesta di informazioni preliminare, al meccanismo di cooperazione, avviando pertanto un'interlocuzione diretta con l'autorità capofila ai sensi degli artt. 56 e 60 del RGPD.

Rispetto alle richieste avanzate nei confronti di Google occorre rilevare che, in taluni casi, le stesse sono state soddisfatte a seguito di un'adesione spontanea del titolare del trattamento successiva alla trasmissione del reclamo da parte dell'Autorità, mentre nei restanti casi si è provveduto tramite provvedimento collegiale.

Tale possibilità di soluzione "nazionale" è stata resa possibile dalla scelta effettuata da Google di mantenere i propri *server* relativi al motore di ricerca al di fuori dell'UE, consentendo così alle singole autorità dei Paesi nei quali il reclamante risulta stabilito di avviare e gestire autonomamente i casi di rispettiva competenza.

Le decisioni assunte dall'Autorità nel periodo di riferimento presentano, come tipologia, un numero sostanzialmente equivalente di valutazioni di infondatezza e di accoglimento, anche solo parziale, delle istanze avanzate dagli interessati.

Le doglianze espresse da questi ultimi hanno riguardato, in via principale, il pregiudizio subito dagli stessi a causa della reperibilità in rete di informazioni riguardanti vicende giudiziarie nelle quali erano stati coinvolti e che avevano avuto nel tempo un'evoluzione tale da determinare uno scostamento tra quanto riferito all'interno dei relativi articoli di giornale e la loro situazione attuale. Ciò è stato determinato, in

alcuni casi, dal successivo accertamento dell'assenza di coinvolgimento dell'interessato o della sua non colpevolezza, mentre in altri casi, pur essendo intervenuta una sentenza di condanna a carico del medesimo, il mutamento del quadro complessivo della posizione giudiziaria di quest'ultimo ha determinato una sostanziale inesattezza della notizia originaria.

Con riferimento alla prima ipotesi, si può riportare il caso di un interessato che aveva avanzato una richiesta di rimozione di URL collegati a contenuti riguardanti una vicenda giudiziaria rispetto alla quale era stato assolto alcuni anni prima. Il reclamante, in particolare, lamentava il pregiudizio subito per effetto della perdurante reperibilità di informazioni riguardanti reati, da lui asseritamente commessi, rispetto ai quali era stato invece dichiarato estraneo. Di quest'ultima circostanza non era stata tuttavia fatta alcuna menzione nei commenti contestati, né risultavano reperibili in rete ulteriori informazioni aggiornate in merito alla vicenda. L'Autorità ha accolto l'istanza ritenendo che il diritto dell'interessato dovesse reputarsi prevalente rispetto alle ragioni di interesse pubblico dedotte dal titolare del trattamento, in quanto la perdurante diffusione di informazioni risalenti e non aggiornate costituiva un trattamento particolarmente pregiudizievole per la sfera giuridica del reclamante e idoneo a fornire agli utenti della rete una rappresentazione inesatta e fuorviante in ordine al coinvolgimento del medesimo. Quest'ultimo aveva altresì domandato l'accoglimento della propria richiesta anche con riferimento ai domini extraeuropei (cd. deindicizzazione globale); tuttavia, nel caso in esame, l'Autorità ha rilevato un'eccessiva genericità delle motivazioni poste a fondamento di tale richiesta che non hanno consentito di apprezzare l'effettività del pregiudizio dedotto dall'interessato (prov. 23 marzo 2023, n. 111, doc. web n. 9883613).

Occorre considerare, in termini generali, che il trattamento di dati giudiziari è soggetto, anche quando effettuato da gestori di motori di ricerca, all'adozione di opportune cautele dettate dalla natura particolare dei dati in questione. In questa direzione si è orientata anche la Corte di giustizia dell'Unione europea che nella sentenza 24 settembre 2019, pronunciata nella causa C-136/17, ha evidenziato la necessità che anche i gestori dei motori di ricerca osservino le cautele indicate nell'art. 10 del RGPD bilanciando in modo particolarmente rigoroso le esigenze connesse alla necessità di garantire l'informazione pubblica con la garanzia dei diritti dell'interessato in un ambito particolarmente delicato.

Tale orientamento risulta condiviso anche dal legislatore nazionale che, tramite recenti riforme dell'ordinamento giudiziario penale, ha indicato, quale via di elezione, quella di minimizzare il trattamento di dati giudiziari al fine di evitare che un utilizzo improprio di questi possa dare vita a fenomeni di spettacolarizzazione che in qualche modo anticipino o influenzino il corso degli accertamenti di competenza della magistratura.

Sono state altresì emanate specifiche disposizioni (cfr. art. 64-ter disp. att. c.p.p., introdotto dal d.lgs. n. 150/2022) finalizzate a limitare, *ab origine* o in via successiva, la circolazione di informazioni giudiziarie riferite a persone che abbiano poi visto mutare favorevolmente la loro posizione per effetto di provvedimenti definitivi del procedimento che ne abbiano escluso la responsabilità, quali decreti di archiviazione o sentenze di assoluzione. Il richiamo, contenuto nella norma, ai limiti previsti dall'art. 17 del RGPD ha posto dei dubbi sull'idoneità di essa a sottrarre al giudizio di bilanciamento le richieste che presentino le caratteristiche sopra descritte.

L'interpretazione resa sul punto dal Garante – contenuta nel parere formulato con riguardo allo schema di decreto legislativo di attuazione della l. n. 134/2021, recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari (parere 1° settembre 2022, n. 292, doc. web n. 9802612) – ha trovato poi concreta

9

9

applicazione in occasione della decisione di alcuni reclami valutati dall'Autorità. Tra questi, si ritiene utile richiamare il caso di un interessato che aveva avanzato nei confronti del gestore di un motore di ricerca una richiesta di deindicizzazione di alcuni URL collegati ad articoli associati al proprio nome e cognome concernenti una vicenda giudiziaria che lo aveva visto coinvolto e che si era poi conclusa con un decreto di archiviazione.

L'interessato aveva ottenuto dalla cancelleria del giudice competente l'apposizione di un'annotazione formale in calce al decreto di archiviazione, quale titolo idoneo per ottenere la deindicizzazione da parte del motore di ricerca. A fronte del diniego opposto dal gestore, motivato con l'attualità della notizia, peraltro aggiornata, e con l'attinenza della stessa al ruolo pubblico ricoperto dall'interessato, quest'ultimo si era rivolto all'Autorità che, nel caso di specie, ha condiviso la posizione espressa dal titolare del trattamento dichiarando il reclamo infondato. Le ragioni poste dall'Autorità alla base della decisione sono da ascrivere al fatto che il richiamo all'art. 17 del RGPD, contenuto nell'art. 64-ter disp. att. c.p.p., è da intendersi come una clausola di salvaguardia delle deroghe previste dallo stesso art. 17 all'esercizio del diritto di cancellazione, tra le quali rientra quella legata alla necessità di garantire il corretto dispiegamento della libertà di espressione e di informazione con cui il diritto all'oblio deve essere opportunamente bilanciato. Nel caso esaminato, è stato ritenuto che la notizia, recente ed aggiornata, fosse ancora di interesse pubblico in quanto connessa al ruolo professionale tuttora ricoperto dal reclamante, il quale aveva peraltro rinnovato l'interesse per la vicenda richiamandola apertamente nel corso di un'intervista resa a un giornale (prov. 28 settembre 2023, n. 430, doc. web n. 9946736 – provv. impugnato dinanzi al Tribunale di Napoli).

In un altro caso, in cui l'interessato aveva parimenti invocato l'applicazione dell'art. 64-ter disp. att. c.p.p., è emersa, nel corso del procedimento, la mancanza dell'annotazione apposta sul provvedimento da parte della cancelleria del giudice competente, da intendersi quale presupposto formale per accedere a tale opportunità. Nel merito della vicenda, l'Autorità ha comunque ritenuto che non vi fossero le basi per ritenere prevalente il diritto dell'interessato, tenuto conto del fatto che i contenuti oggetto di richiesta erano di pubblicazione recente, aggiornati – peraltro per effetto di una dichiarazione del legale dell'interessato riportata nell'articolo – e attinenti al ruolo professionale svolto dal medesimo (prov. 21 dicembre 2023, n. 616, doc. web n. 9981652).

Diversamente, il Garante ha ritenuto fondato il reclamo con cui l'interessato, destinatario di un provvedimento favorevole, ha chiesto la deindicizzazione di contenuti non aggiornati riferiti a fasi precedenti del procedimento (provvedimento di amministrazione giudiziaria della società di cui il reclamante era amministratore delegato, provvedimento poi revocato; risultanze di indagini coinvolgenti anche il medesimo, poi definitesi nei suoi confronti con l'archiviazione). Il reclamo era stato presentato prima dell'entrata in vigore dell'art. 64-ter disp. att. c.p.p., ma dopo l'entrata in vigore della legge delega, contenente il principio ispiratore della disposizione. Il provvedimento di accoglimento del Garante nel caso di specie (prov. 21 dicembre 2023, n. 619, doc. web n. 9979832) si colloca nel quadro di un bilanciamento tra diritto all'oblio e accessibilità alle informazioni effettuato dall'Autorità per fattispecie analoghe anche prima di tale novità legislativa (cfr. provv. ti 10 febbraio 2022, n. 52, doc. web n. 9750669; 20 ottobre 2022, n. 352, doc. web n. 9838182).

L'operazione di bilanciamento sottesa alla valutazione delle richieste di rimozione deve tenere conto, da un lato, delle esigenze di tutela espressa dagli interessati e, dall'altro, della necessità di garantire agli utenti della rete l'accessibilità ad informazioni utili riguardo ai medesimi. Al fine di poter apprezzare la sussistenza di un interesse pubblico attuale alla conoscibilità di determinate informazioni, occorre

tenere in considerazione l'effettiva rilevanza della notizia e la sua idoneità a contribuire in modo efficace alla costruzione di un profilo dell'interessato rispondente alla sua attuale identità.

Tale idoneità è tuttavia risultata assente in alcune delle fattispecie sottoposte all'attenzione del Garante. In particolare è stata ordinata la deindicizzazione di due URL rinvianti ad alcune pagine di un sito di aggregazione di notizie contenenti l'anteprima di due articoli integralmente consultabili solo dagli abbonati; anteprima avente limitato contenuto informativo e nella quale i dati identificativi del reclamante non erano riportati, anche se comparivano nel cd. *snippet*. L'Autorità ha rinvenuto in tale risultato di ricerca un trattamento di dati personali ultroneo rispetto ai contenuti resi disponibili nelle anteprime rivolte alla generalità degli utenti non registrati al sito (provv. 22 marzo 2023, n. 104, doc. web n. 9892698).

A questi casi si sono poi aggiunte altre fattispecie nelle quali l'Autorità, in considerazione delle caratteristiche specifiche della vicenda rappresentata, non ha ravvisato la sussistenza di ragioni di interesse pubblico prevalenti rispetto al diritto all'oblio invocato dagli interessati (tra gli altri, provv.ti 27 aprile 2023, n. 176, doc. web n. 9916702; 17 maggio 2023, n. 204, doc. web n. 9903127 e 30 novembre 2023, n. 563, doc. web n. 9979890).

Alla luce del criterio del prevalente interesse pubblico, l'Autorità è giunta a diversa conclusione nel caso di un interessato che aveva chiesto la deindicizzazione di alcuni URL riferibili a pagine di enciclopedie *online* contenenti informazioni a lui riferibili, ivi incluse quelle riguardanti vicende giudiziarie in cui lo stesso era stato coinvolto e definite con decisioni per lui favorevoli. L'Autorità, condividendo la posizione espressa dal titolare del trattamento, ha dichiarato l'infondatezza del reclamo ritenendo la perdurante sussistenza di un interesse pubblico a conoscere le relative informazioni, tenuto conto del fatto che le pagine oggetto di contestazione contenevano non solamente dati giudiziari (aggiornati alla luce degli sviluppi successivi), ma anche informazioni di varia natura che contribuivano a ricostruire il profilo del reclamante, pure con riguardo al ruolo politico dallo stesso svolto (provv. 16 novembre 2023, n. 533, doc. web n. 9972735).

L'Autorità ha poi dichiarato infondati: un reclamo volto a ottenere la rimozione di un URL che rimandava a un articolo – ritenuto invece ancora attuale – corredato da immagini relative a esternazioni di gioventù effettuate in pubblico dal reclamante, che si era anche candidato a posizioni politico-amministrative (provv. 22 giugno 2023, n. 268, doc. web n. 9919295); una richiesta di deindicizzazione di alcuni URL risalenti al 2017 riguardanti l'attività politica svolta dal reclamante all'interno di un partito politico, che il Garante ha ritenuto mantenessero un interesse per la collettività, anche in ragione del poco tempo trascorso dalle vicende ivi rappresentate e in considerazione della naturale dimensione pubblica di ogni attività politica (provv. 26 ottobre 2023, n. 507, doc. web n. 9955703); un reclamo con il quale è stato invocato l'oblio rispetto a URL rinvianti a notizie risalenti al 2019 che riferivano della misura cautelare disposta dall'Autorità giudiziaria nei confronti del reclamante nell'ambito di un'indagine della Guardia di finanza, dalla quale sarebbero emerse presunte condotte corruttive nei confronti di magistrati tributari coinvolgenti anche l'interessato – giornalista e personaggio di rilievo nell'ambiente televisivo – in collegamento alla propria attività professionale (provv. 13 aprile 2023, n. 138, doc. web n. 9897822).

La sussistenza di un interesse pubblico attuale è stata rilevata, inoltre, in relazione al caso di un interessato che chiedeva la rimozione di alcuni URL rinvianti a contenuti reperibili in associazione al proprio nome e cognome, anche unitamente ad altri criteri di ricerca non riferibili a dati personali del medesimo, riguardanti vicende che avevano coinvolto alcune società, dichiarate fallite, alla cui gestione si era dichiarato

9

9

estraneo, lamentando il discredito personale e professionale derivante alla propria persona da tale accostamento. L'Autorità, nel limitare la propria valutazione ai soli risultati di ricerca reperibili attraverso il nominativo dell'interessato, ha dichiarato l'infondatezza del reclamo essendo emerso che l'interessato aveva esercitato un ruolo professionale specifico all'interno della società poi fallita e che quest'ultima risultava comunque collegata ad altra della quale il medesimo era stato socio di minoranza e la cui rappresentanza era in capo a suoi congiunti. L'interesse pubblico alla conoscibilità delle notizie contestate è stato peraltro correlato all'attività professionale tuttora svolta dal reclamante nel medesimo settore (prov. 21 dicembre 2023, n. 613, doc. web n. 9981324).

L'Autorità è stata chiamata a pronunciarsi, da ultimo, in merito alla richiesta di deindicizzazione di URL attinenti a diverse vicende coinvolgenti il reclamante, accogliendo l'istanza nei casi in cui le relative pagine riportavano contenuti non aggiornati con le misure disposte a favore dell'interessato (riabilitazione, provvedimenti di archiviazione e di non luogo a procedere), e invece rigettando l'istanza con riferimento alle pagine in cui veniva dato conto dei predetti aggiornamenti; a tale determinazione si è giunti in ragione dell'interesse alla conoscenza da parte del pubblico considerato il ruolo pubblico del reclamante, comprovato dai numerosi incarichi, anche di vertice, assunti negli anni presso enti pubblici e privati e dalla sua attuale attività professionale (prov. 21 dicembre 2023, n. 619, doc. web n. 9979832).

10 Cyberbullismo e *revenge porn*

Le segnalazioni in materia di cyberbullismo pervenute nel 2023 hanno riguardato principalmente la pubblicazione di *post* denigratori e diffamatori, nonché la creazione di falsi profili *social*.

Le istanze sono state trattate mediante la formulazione di specifiche richieste di intervento al titolare del trattamento/gestore del sito coinvolto, anche prendendo contatti telefonici o via *e-mail* con il segnalante allo scopo di acquisire informazioni aggiuntive o per fornire allo stesso indicazioni utili rispetto alla vicenda segnalata. Si sono registrati, inoltre, alcuni casi in cui non sono stati ravvisati i presupposti per poter procedere, talvolta in ragione della mancata indicazione da parte del segnalante degli elementi necessari all'invio della relativa richiesta al gestore della piattaforma coinvolta e, in talune ipotesi, a causa della carenza dei requisiti minimi previsti dalla legge 29 maggio 2017, n. 71 per qualificare una condotta come atto di cyberbullismo.

Si è notevolmente intensificato anche l'impegno del Garante per prevenire e contrastare il fenomeno della diffusione, con intenti vendicativi e comunque in assenza del consenso della persona interessata, di immagini a contenuto sessualmente esplicito (*revenge porn*) ai sensi dell'art. 144-*bis* del Codice.

Sul sito istituzionale dell'Autorità è stata implementata un'apposita procedura di segnalazione *online* che, agevolando le modalità di comunicazione da parte degli interessati, ha contribuito al notevole incremento delle segnalazioni ricevute (circa 650) nel corso del periodo di riferimento.

Le segnalazioni sono state trattate fornendo indicazioni agli interessati e, laddove si è reso necessario, chiedendo le opportune integrazioni per la successiva trattazione, ivi compresa, in talune ipotesi, la trasmissione del materiale a contenuto sessualmente esplicito la cui acquisizione è prevista dall'art. 144-*bis* del Codice. In alcuni casi il materiale inviato dai segnalanti non è risultato idoneo (come nel caso di *screenshot* di videochiamate o di *chat*) all'invio alle piattaforme interessate, stante la possibilità per la persona malintenzionata di caricare l'immagine originale in suo possesso.

L'esame delle segnalazioni ha portato, in quasi la metà dei casi, all'adozione in via d'urgenza di una determinazione dirigenziale (nel complesso, circa 300), successivamente ratificata da parte del Collegio, diretta ai gestori delle piattaforme coinvolte per ottenere l'intervento di blocco preventivo del materiale a contenuto sessualmente esplicito oggetto della temuta attività di diffusione.

È stata infine effettuata un'attività di verifica a campione volta a valutare il corretto adempimento dei provvedimenti di blocco preventivo in materia di *revenge porn* adottati dall'Autorità. In tale contesto, è stata fatta richiesta ad alcuni gestori delle piattaforme di fornire informazioni sulle misure attuate a seguito della notifica di specifici provvedimenti trasmessi nel corso del periodo di riferimento.

11 *Marketing e trattamento di dati personali*

11.1. *Il fenomeno del telemarketing indesiderato e l'azione di contrasto*

Nonostante la forte attività di contrasto portata avanti dall'Autorità nel corso del tempo e in particolare negli ultimi anni con il pieno utilizzo dei nuovi strumenti, anche di carattere sanzionatorio, offerti dal RGPD, il fenomeno del *telemarketing* indesiderato non mostra cenni di sensibile regressione.

Anche il 2023 è stato quindi caratterizzato da molteplici azioni nei confronti degli operatori (dalla committenza, agli intermediari, fino all'ultimo anello della catena, ossia i *call center*), che hanno portato a confermare le criticità sin qui riscontrate, ossia, soprattutto, la carenza di una vera e propria catena di controllo che impedisca alle imprese di "introytare" contratti originati da contatti effettuati in violazione delle norme.

In numerosissimi casi relativi a segnalazioni per telefonate promozionali provenienti da soggetti, o effettuate per conto di committenti, non individuati, o per le quali non è stata indicata la numerazione chiamante e/o altri elementi essenziali ai fini di un'attività di controllo dell'Autorità, nonché in rapporto al fenomeno delle telefonate cd. mute, sono stati forniti, come di consueto, riscontri attraverso note standard contenenti chiarimenti e indicazioni operative ovvero riferimenti alle iniziative già avviate dal Garante a vario titolo negli scorsi anni (in particolare, le FAQ pubblicate nel sito istituzionale dell'Autorità concernenti le telefonate mute).

In altri casi, in cui le segnalazioni e i reclami pervenuti sono risultati puntuali, riconducibili a specifici titolari e di rilevanza in tema di protezione dei dati personali, il Garante ha avviato istruttorie, anche lunghe e complesse, all'esito delle quali ha adottato provvedimenti correttivi e/o sanzionatori, illustrati nei successivi paragrafi.

L'Autorità ha adottato diversi provvedimenti originati da istruttorie relative al *marketing* indesiderato realizzato mediante canale telefonico o tramite posta elettronica, alla gestione dell'esercizio dei diritti degli interessati ed alle criticità riguardo ai principi di *accountability*, *privacy by design* e sicurezza dei dati.

In numerosi casi le istruttorie hanno riguardato il trattamento di dati personali forniti ai titolari da soggetti terzi (*list provider*) in assenza di verifiche in ordine ai presupposti di liceità del trattamento, con particolare riferimento all'informativa resa e ai consensi acquisiti dagli interessati.

A seguito della ricezione di un reclamo concernente una telefonata indesiderata avente ad oggetto la promozione di servizi di manutenzione caldaie offerti da una società, l'Autorità ha adottato un provvedimento in cui ha dato atto dell'assenza tra titolare e fornitore di un contratto o di un altro atto giuridico idoneo a regolare i rispettivi ruoli *privacy* nei trattamenti contestati. Nell'ambito della medesima istruttoria è stato rilevato che i dati personali acquisiti dal *list provider* venivano conservati nei sistemi aziendali per almeno un anno, senza una ragione giustificativa. Alla società è stata comminata una sanzione di 3.000 euro (provv. 9 marzo 2023, n. 71, doc. web n. 9880336).

Analoghe violazioni sono state riscontrate nel provvedimento adottato nei confronti di una società attiva nella promozione e diffusione di iniziative artistiche anche per conto di terzi (provv. 9 marzo 2023, n. 61, doc. web n. 9873408). Tale provvedimento è risultato collegato a un'istruttoria parallela, relativa ad altro titolare,

all'esito della quale è stato possibile appurare che tale soggetto, presentandosi con false generalità, proponeva la veicolazione di *e-mail* promozionali utilizzando liste realizzate senza alcuna idonea base giuridica (prov. 2 marzo 2023, n. 60, doc. web n. 9880317). La sanzione comminata, di 5.000 euro, non è risultata pagata e, pertanto, è stato avviato il procedimento per l'iscrizione a ruolo.

L'Autorità ha poi inflitto a una società una sanzione amministrativa per aver effettuato telefonate promozionali indesiderate in assenza dei requisiti di liceità del trattamento, con particolare riferimento agli adempimenti dell'informativa (inidonea con riguardo al testo utilizzato per i contatti telefonici) e del consenso al *marketing*. Dall'istruttoria è emerso che la lista contenente i dati del reclamante proveniva da una società americana con la quale il titolare sarebbe entrato in contatto per il tramite di un proprio *partner* commerciale, e che le criticità inerenti l'informativa e il consenso sussistevano sia in riferimento alle liste fornite dalla società americana, sia riguardo alle anagrafiche reperite dai *partner* italiani, non rilevando le garanzie offerte nei contratti né la sede dello stabilimento principale del titolare (italiano o *extra UE*). Pertanto l'Autorità ha chiarito che, indipendentemente dalla provenienza dei dati, è onere del titolare verificare e comprovare il rispetto delle norme in materia di protezione dei dati personali (principio di *accountability*) e ha imposto una sanzione amministrativa pecuniaria di euro 10.000 (prov. 26 ottobre 2023, n. 503, doc. web n. 9964761).

Sempre al fine di contrastare il *telemarketing* selvaggio, l'Autorità è intervenuta nei confronti di un *call center* per violazioni attinenti all'obbligo di informativa, comminando una sanzione di 10.000 euro (prov. 6 luglio 2023, n. 334, doc. web n. 9927358).

Nel corso delle attività istruttorie e in sede provvedimentale l'Autorità ha più volte ricordato che l'effettuazione di telefonate indesiderate soggiace all'obbligo del consenso in virtù della *lex specialis* di cui all'art. 130 del Codice, non potendo essere invocata dal titolare la condizione di liceità del legittimo interesse. Allo stesso tempo è stato ribadito che i dati presenti in elenchi pubblici non possono essere utilizzati per finalità promozionali. Pertanto, a una società del settore dell'editoria è stato vietato ogni ulteriore trattamento dei dati così raccolti, nonché prescritto di cancellare tali dati e di adottare misure che garantiscano il pieno ed effettivo riscontro all'esercizio dei diritti degli interessati. Alla luce di ciò, il Garante ha ritenuto congrua l'applicazione di una sanzione amministrativa pecuniaria di 15.000 euro (prov. 6 luglio 2023, n. 294, doc. web n. 9941250).

L'Autorità ha poi svolto un'istruttoria nei confronti di una società attiva nel settore della comparazione *online* a seguito della quale è stata adottata una sanzione amministrativa pecuniaria di 40.000 euro. L'istruttoria è scaturita da un reclamo con il quale era stata lamentata la ricezione insistente di telefonate promozionali su un'utenza iscritta al RPO, anche dopo che l'interessato si era espressamente opposto nel corso dei contatti indesiderati e mediante formali istanze di esercizio dei diritti rimaste prive di riscontro. Le principali criticità rilevate dall'Autorità hanno riguardato l'informativa (assente nel corso del primo contatto telefonico e inidonea con riguardo al sito internet) e la raccolta dei consensi, che venivano acquisiti attraverso il sito internet societario e che erano riferiti anche ad attività di trattamento non concretamente svolte dalla società (quale la profilazione). Sotto il profilo delle misure correttive individuate, l'Autorità ha vietato il trattamento dei dati personali per i quali non fosse stato acquisito un idoneo consenso per l'attività di profilazione, disponendone anche la cancellazione, e ha ingiunto al titolare di adottare adeguate procedure volte a verificare costantemente, anche mediante controlli a campione, che i dati personali forniti dal *provider* fossero trattati nel pieno rispetto delle disposizioni in materia, nonché di facilitare l'esercizio dei diritti degli interessati, recependo le istanze già al momento

11

11

del contatto telefonico. Inoltre, è stato ingiunto al titolare di fornire agli interessati – tanto nell’ambito delle telefonate quanto in apposita sezione del sito web – un’idonea informativa che indicasse le operazioni di trattamento effettivamente svolte dalla società (prov. 18 luglio 2023, n. 322, doc. web n. 9921112).

Infine, con riguardo alle numerose segnalazioni per telefonate promozionali l’Autorità ha avviato una serie di istruttorie parallele volte ad accertare l’esistenza ed adeguatezza delle misure tecniche e organizzative adottate da alcuni titolari per contrastare il *telemarketing* selvaggio e assicurare il controllo della filiera dal contatto al contratto. L’iniziativa è stata intrapresa nei confronti di vari attori del settore telefonico, energetico, di TV interattiva e di vendita porta a porta. Questi titolari sono stati destinatari di alcune richieste di informazioni, ai sensi dell’art. 157 del Codice, volte ad ottenere un elenco delle proposte di acquisto provenienti dalle rispettive reti di vendita e che hanno determinato l’attivazione dei relativi servizi o la vendita di prodotti. Per una valutazione completa dei trattamenti, l’Autorità ha coinvolto la Fondazione Ugo Bordoni (FUB) richiedendo la verifica dell’iscrizione delle numerazioni chiamate nel RPO e, quindi, l’eventuale violazione dell’art. 130, commi 3 e 3-bis, del Codice, riguardante le comunicazioni elettroniche, nonché, più in generale, degli artt. 5, par. 1, lett. a) e 6, par. 1, lett. a), del RGPD, con riguardo al principio di liceità e alla base giuridica del consenso per fini promozionali.

11.1.1. Il telemarketing illegale nel settore telefonico

Nel corso del 2023 sono state definite alcune importanti istruttorie volte a contrastare il fenomeno delle chiamate promozionali illecite alimentato dal cd. sottobosco del *telemarketing*, ovvero da tutti quei soggetti che procacciano clienti e contratti per la rete ufficiale di vendita delle grandi compagnie telefoniche ed energetiche.

Nell’ambito degli accertamenti in materia di *telemarketing* nel settore dei servizi di telefonia, l’Autorità ha adottato un provvedimento correttivo e sanzionatorio di importo pari a 100.000 euro, rilevando lacune nelle informative fornite agli interessati, con la conseguente violazione dei principi di correttezza e di trasparenza; la carenza della base giuridica del trattamento dei dati per alcune attività di trattamento; alcune criticità nel ricorso al cd. *soft spam* svolto mediante lo strumento degli SMS anziché mediante posta elettronica, unica modalità ammessa per rivolgere offerte di prodotti e servizi analoghi a quelli già acquistati dagli interessati, pur in assenza di uno specifico, libero, preventivo e documentato consenso per la finalità di *marketing* (v. art. 130, comma 4, del Codice); l’inadeguatezza dei tempi di conservazione dei dati trattati per fini di *marketing* e profilazione (prov. 18 luglio 2023, n. 321, doc. web n. 9920942).

Con specifico riferimento alla suddetta conservazione, è stato rilevato il contrasto del trattamento con i principi di finalità, di minimizzazione e di limitazione della conservazione, avendo la società individuato termini eccessivamente dilatati. Nell’occasione, il Garante ha stabilito che, come peraltro sostenuto dalla società, il provvedimento del 24 febbraio 2005 “*Fidelity card* e garanzie per i consumatori”, sebbene non più di carattere vincolante, era da considerarsi ancora applicabile con valore di linea guida e, pertanto, lo era anche la tempistica ivi prevista (24 mesi per i dati relativi al *marketing*; 12 mesi per i dati relativi alla profilazione). Peraltro, pur valorizzando il principio di *accountability*, anche con riferimento alla delicata materia della *data retention*, non si può certo giungere alla conclusione che un titolare, in base a tale principio che necessita di essere contemperato con gli altri fondamentali principi previsti dal Regolamento, possa discostarsi in modo eccessivo dalle suddette previsioni senza incorrere nella violazione del principio di limitazione della conservazione (v. art. 5, par.1, lett. d), del RGPD). Inoltre, a giudizio dell’Autorità, non poteva darsi rilievo ai precedenti citati dalla società (v. provv.ti 24 aprile 2013, doc.

web n. 2499354 e 30 maggio 2013, doc. web n. 254783), in quanto provvedimenti adottati dal Garante in condizioni diverse e riferiti ai tempi di conservazione dei dati relativi all'acquisto di beni di lusso, ossia in relazione a fattispecie non adattabili al caso in questione. Nel calcolare la sanzione pecuniaria (euro 100.000) si è tenuto conto di alcuni fattori quali la tempestiva adozione di misure correttive, alcune delle quali avviate subito dopo la conclusione degli accertamenti ispettivi; la costante e proficua collaborazione con il Garante; la grave crisi socio-economica sperimentata dal settore e i suoi pesanti riflessi anche sulla situazione economico-finanziaria della società, che, tuttavia, al contempo, aveva deciso di mantenere inalterata la propria forza lavoro e aveva provveduto all'internalizzazione del personale di altre aziende, destinato altrimenti al licenziamento. In tal modo è stata valorizzata anche la funzione socio-economica dell'attività del Garante.

A completamento dell'attività istruttoria che aveva già portato all'adozione di un provvedimento prescrittivo e sanzionatorio nei confronti di una compagnia telefonica (provv. 12 novembre 2020, n. 224, doc. web n. 9485681), il Garante ha adottato un altro provvedimento (provv. 23 febbraio 2023, n. 50, doc. web n. 9871886) nei confronti di un'agenzia della rete di vendita di tale compagnia telefonica. Questa infatti aveva acquisito e comunicato alla società committente, fra il 2019 e il 2020, liste di contatti contenenti dati personali di circa 4,3 milioni di utenti del settore telefonico. All'agenzia è stato contestato di aver operato, nell'ambito dell'attività di procacciamento delle liste di anagrafiche, nella veste di autonomo titolare del trattamento e non quale responsabile della compagnia telefonica, ruolo che aveva assunto soltanto in relazione alle attività di contatto telefonico degli utenti, a fini promozionali. Con il provvedimento è stato accertato che l'agenzia aveva acquisito da soggetti terzi liste anagrafiche entrando in contatto in maniera autonoma con tali soggetti, sottoscrivendo in proprio i relativi contratti e riversando poi tali liste nel sistema della compagnia telefonica. In tale modo si è realizzato il cd. doppio passaggio dei dati, dal fornitore delle liste all'agenzia e dall'agenzia alla compagnia telefonica, l'ultimo dei quali in carenza di un consenso libero, specifico, informato e inequivocabile degli interessati, a nulla rilevando, per dimostrare il ruolo di mero responsabile rivestito dall'agenzia, la destinazione esclusiva dei dati medesimi (che rappresentava solamente una garanzia nell'interesse del fornitore) e la preventiva autorizzazione e successiva validazione dei dati da parte della compagnia telefonica (funzionale esclusivamente all'ingresso delle liste nei *database* societari).

Con il provvedimento, oltre all'applicazione di una sanzione amministrativa pecuniaria, l'Autorità ha imposto all'agenzia il divieto di ogni ulteriore trattamento dei dati acquisiti e l'adozione di una procedura di acquisizione delle liste anagrafiche che rendesse chiare per gli interessati la titolarità dei diversi trattamenti posti in essere e la base giuridica delle eventuali comunicazioni di dati.

11.1.2. Il telemarketing illegale nel settore energetico

Anche il *telemarketing* illecito nel settore energetico è stato oggetto, nel 2023 dell'azione di contrasto da parte del Garante. In particolare, in tale ambito è risultata più penetrante l'azione di agenzie abusive che, spendendo il nome delle compagnie energetiche, realizzano contatti telefonici in totale spregio delle disposizioni in tema di RPO e acquisiscono contratti che poi riescono a far confluire nei sistemi di gestione della clientela delle compagnie energetiche, sfruttando le debolezze di tali sistemi sotto il profilo della protezione dei dati e delle misure di sicurezza.

In relazione alle situazioni sopra descritte, il Garante ha adottato il provvedimento 13 aprile 2023, n. 184 (doc. web n. 9893718), all'esito di una lunga e articolata attività ispettiva originata da verifiche avviate dalla Guardia di finanza e poi proseguite dall'Autorità. Con il provvedimento sono state sanzionate quattro società operanti

11

nel territorio toscano e veneto che avevano creato una capillare organizzazione parallela in grado di operare in nome di numerose compagnie energetiche, contattando i vari clienti e proponendo continui cambi di operatore, anche in assenza di offerte economicamente più vantaggiose, al fine di lucrare sulle provvigioni. Le diverse agenzie erano tra loro collegate, in alcuni casi anche a livello societario, e nessuna di queste, tranne una, era ricompresa ufficialmente nella rete di vendita delle compagnie energetiche: tutte agivano senza alcun formale incarico e in base a un sistema di distribuzione delle responsabilità in ambito *privacy* fittizio, meramente formalistico e con gravissime carenze nell'adozione di efficaci misure di sicurezza per la protezione dei propri sistemi. Con il provvedimento, il Garante, per la prima volta, ha applicato alle società coinvolte la sanzione accessoria della confisca delle banche dati e delle liste anagrafiche utilizzate per i contatti e le promozioni indesiderate, in ragione della tipologia delle medesime, della loro illecita provenienza e dell'elevata probabilità di un loro riuso nonostante il divieto di trattamento, avendo le società strutturato l'intera propria attività imprenditoriale sulla sistematica violazione delle disposizioni in materia di protezione dei dati personali.

Con riferimento al *marketing* nel settore energetico, è stato adottato un provvedimento nei confronti di un *call center* attivo nel settore del *teleselling* per la conclusione di contratti di energia elettrica. Lo stesso *call center* era già stato destinatario di un provvedimento sanzionatorio nel 2022, per mancato riscontro alla richiesta di informazioni *ex art.* 157 del Codice (provv. 20 ottobre 2022, n. 350, doc. web n. 98325449). Dall'attività istruttoria è emersa l'assenza di informativa e consenso e l'inadeguata gestione delle istanze di esercizio dei diritti (stante il fatto che la PEC preposta a tal fine non è risultata funzionante), nonché la mancata verifica delle utenze da contattare nel RPO. L'Autorità ha ritenuto di imporre una sanzione amministrativa pecuniaria di euro 60.000 tenuto conto che la società, nonostante il provvedimento sanzionatorio del 2022 e anche dopo la contestazione mossi, ha continuato a eludere la normativa in materia di protezione di dati personali (provv. 30 novembre 2023, n. 561, doc. web n. 9971433).

Il Garante ha inoltre adottato provvedimenti nei confronti di due ulteriori società operanti nel settore energetico (provv. 14 aprile 2023, nn. 181 e 182, docc. web nn. 9893693 e 989463), destinatarie di sanzioni rispettivamente per euro 676.956 ed euro 237.800, per non aver adottato misure idonee a garantire la tracciabilità di tutte le operazioni svolte sulle piattaforme di caricamento delle proposte contrattuali e per non aver dimostrato la piena contezza di tutti i trattamenti effettuati nell'ambito della filiera del *telemarketing*.

11.1.3. Attivazione illecita di schede telefoniche

Nel corso dell'anno è continuata anche l'attività di contrasto alle attivazioni illecite di schede telefoniche, fenomeno che ha registrato un rilevante incremento determinando gravi violazioni della disciplina in materia di protezione dei dati personali e che risulta potenzialmente idoneo a creare ulteriori e ben più allarmanti indotti di illiceità e a costituire un ostacolo alle attività di prevenzione e repressione di reati anche di natura associativa.

A seguito di un'istruttoria inizialmente avviata nei confronti di una compagnia telefonica, l'Autorità ha adottato il provvedimento 14 settembre 2023, n. 405 (doc. web n. 9936215) nei confronti di uno dei principali *dealer* della predetta compagnia: si è avuto modo, infatti, di accertare che questi, che aveva i propri esercizi commerciali in Campania, aveva attivato alcune schede telefoniche intestandole a un cittadino residente in Lombardia, senza che quest'ultimo si fosse mai recato in tali negozi, utilizzando una copia del documento d'identità del cliente di ignota origine e inserendo nei sistemi della compagnia telefonica dati bancari formalmente corretti

ma non riconducibili al medesimo interessato. Con il provvedimento, il Garante ha applicato al *dealer* una sanzione amministrativa pecuniaria e ha imposto il divieto di ogni ulteriore trattamento dei dati dell'interessato.

11

11.1.4. Utilizzo di call center ubicati fuori dall'Unione europea

Anche nel corso del 2023, con immutata consistenza numerica, sono pervenute notifiche da parte dei titolari che si avvalgono di *call center* ubicati al di fuori dell'Unione europea, in conformità a quanto previsto dall'art. 24-*bis* del d.l. n. 83/2012, come sostituito dall'art. 1, comma 243 della legge 11 dicembre 2016, n. 232.

11.1.5. Scenari evolutivi nel settore del telemarketing illegale: il codice di condotta

Un importante momento nella lotta al *telemarketing* selvaggio si è registrato con l'approvazione del codice di condotta per le attività di *telemarketing* e *teleselling* promosso da associazioni rappresentative di committenti, *call center*, *teleseller*, *list provider* e di consumatori (provv. 9 marzo 2023, n. 70, doc. web n. 9868813). Il codice acquisterà efficacia una volta conclusa la fase di accreditamento dell'Organismo di monitoraggio (ODM) e la successiva pubblicazione in Gazzetta ufficiale.

L'Autorità ha costantemente lavorato con le associazioni proponenti per fornire alcuni chiarimenti che hanno poi consentito di presentare correttamente la documentazione approvata dal Garante.

Sotto altro profilo, a seguito della piena operatività del sistema automatizzato di segnalazioni in materia di *telemarketing*, avviato nel portale istituzionale nel novembre 2022, l'Autorità ha avviato sistematiche e periodiche estrazioni di dati dalle migliaia di doglianze ricevute. A partire dalle prime risultanze di tali estrazioni sono state avviate indagini, tuttora in corso, confrontando i dati con alcuni elementi raccolti presso i titolari del trattamento nel corso di attività ispettive o altre indagini. Il sistema di raccolta delle segnalazioni *online* si candida quindi a divenire uno strumento essenziale a sostegno delle attività di indagine del Garante in tale settore. Tenendo conto dei numerosi *feedback* giunti dagli utenti sul suo funzionamento, sono state esaminate possibili soluzioni migliorative del sistema al fine di facilitarne la fruibilità e l'utilizzo (introducendo, ad es., la facoltà di autenticazione tramite SPID). A tutti i segnalanti, come già accennato, sono stati forniti, in via automatizzata, puntuali informazioni in merito al fenomeno del *telemarketing* selvaggio e suggerite alcune possibili misure di carattere operativo per adottare una prima azione di contrasto già da parte dell'utente.

11.1.6. Marketing e profilazione

L'Autorità ha individuato e promosso istruttorie e accertamenti ispettivi volti alla verifica di eventuali criticità nei trattamenti dei dati personali nel contesto delle *fidelity card*.

In tale ambito il Garante ha sanzionato per 240.000 euro una nota azienda italiana operante nel campo dell'abbigliamento (provv. 27 aprile 2023, n. 188, doc. web n. 9902472), per aver trattato illecitamente i dati personali di un numero rilevante di clienti ed *ex* clienti, mediante una conservazione senza limiti temporali di dati personali (dettagli degli scontrini e punti accumulati) ai fini di *marketing* e di profilazione e in assenza di adeguate misure di sicurezza. Dalle verifiche effettuate è emerso che il *database* gestionale era accessibile da tutti gli addetti dei negozi del gruppo, presenti in 7 Paesi europei, da qualunque dispositivo connesso alla rete internet, tramite un'unica *password* e un unico *account*. Considerato l'elevato numero degli interessati e la notevole durata delle violazioni, è stato ingiunto alla società di adottare tutte le misure necessarie per conformarsi alla normativa *privacy*, di cancellare o anonimizzare i dati degli *ex* clienti risalenti a più di 10 anni (fatti salvi i contenziosi

11

in atto) e di predisporre adeguate soluzioni organizzative e misure di sicurezza volte ad assicurare la corretta conservazione dei dati dei clienti e degli *ex* clienti nel rispetto dei principi di finalità e minimizzazione del RGPD.

L'Autorità ha adottato un provvedimento anche nei confronti di una nota società *multibrand* (provv. 8 giugno 2023, n. 253, doc. web n. 9909907), sanzionando alcune violazioni della disciplina in materia di conservazione dei dati per finalità di *marketing* e di profilazione e di quella relativa alla valutazione d'impatto sui diritti degli interessati. Il Garante è intervenuto a seguito della segnalazione di una cliente che, dopo un alterco con un'addetta dello *store*, si era vista annullare la *fidelity card* erogata anni addietro e attivarne una nuova, non richiesta, intestata a persona inesistente, in violazione dei principi di integrità e riservatezza, correttezza e liceità. Inoltre, nell'informativa non veniva indicata l'attività svolta mediante Facebook-Meta, che prevedeva l'inoltro degli indirizzi *e-mail* dei clienti alla società americana.

Riguardo all'attività di *e-commerce* presente sul sito, pur svolgendo un'attività di profilazione ad ampio raggio, non è risultato che la società avesse predisposto la procedura di valutazione d'impatto prevista dal RGPD. L'Autorità ha prescritto al titolare di definire tempi differenziati di conservazione, distinguendo fra trattamenti a fini di *marketing* e trattamenti a fini di profilazione e cancellando, o anonimizzando, i dati che fossero risultati conservati al di là dei termini stabiliti. Nel definire l'importo della sanzione in 300.000 euro, l'Autorità ha considerato l'elevato numero dei soggetti coinvolti dalle violazioni (circa 2.400.000 i soggetti risultati registrati negli *store* fisici oppure nel sito web), la loro durata e la capacità economica della società.

L'Autorità ha sanzionato una società in ragione di riscontrate violazioni in merito all'informativa (inidonea con riguardo al sito internet e riferibile ad attività non concretamente svolte dalla società); ai consensi acquisiti attraverso il *form online*, ai fini di *marketing* e profilazione, in quanto non liberi; alla procedura di gestione del diritto d'opposizione, che veniva recepito nell'ambito delle telefonate promozionali, e dell'istanza di esercizio dei diritti; all'assenza di controlli dei presupposti di liceità nell'ambito della filiera dei *partner* promotori dei prodotti della società. In ragione del mancato pagamento, anche in misura ridotta, della sanzione comminata, è stato avviato il procedimento per l'iscrizione a ruolo (ai sensi dell'art. 16, comma 3, del reg. del Garante n. 1/2019) (provv. 18 luglio 2023, n. 323, doc. web n. 9925674).

Infine, a seguito della ricezione di numerosi reclami e segnalazioni, il Garante è intervenuto nei confronti di un istituto universitario nell'interesse del quale venivano inviati SMS promozionali. Gli interessati, oltre a lamentare la ricezione di comunicazioni indesiderate, avevano rappresentato anche il mancato riscontro alle richieste di esercizio dei diritti. All'esito dell'istruttoria, non essendo stato adottato alcun intervento correttivo da parte del titolare e perdurando l'errata convinzione dello stesso di poter utilizzare il legittimo interesse come base giuridica per l'invio di SMS promozionali, è stato adottato un provvedimento correttivo e inibitorio con sanzione pecuniaria di 75.000 euro (provv. 18 luglio 2023, n. 393, doc. web n. 9939507).

11.1.7. Marketing attraverso modelli oscuri (dark pattern) e banche dati illecite

All'esito di un'attività ispettiva incentrata sul più generale controllo delle banche dati utilizzate per il *marketing*, il Garante ha adottato un provvedimento correttivo e sanzionatorio con il quale si è espresso per la prima volta sull'utilizzo di modelli oscuri (*dark pattern*) per la realizzazione di interfacce al fine di raccogliere dati e consensi, materia sinora trattata prevalentemente in ambito consumeristico ma di notevole importanza anche per valutare la libertà del consenso rilasciato per il trattamento dei dati personali. Il provvedimento inoltre ha espresso principi e chiarimenti per gli operatori riguardo alla realizzazione di banche dati per il *marketing* e ai ruoli

nel trattamento svolti dai diversi soggetti della filiera, con particolare riguardo alle responsabilità in fase di selezione dei fornitori di banche dati. Alla società è stata comminata una sanzione di 300.000 euro (provv. 23 febbraio 2023, n. 51, doc. web n. 9870014).

Il Garante ha adottato un provvedimento di divieto e sanzionatorio all'esito di una serie di accertamenti volti ad identificare il soggetto che, presentandosi con false generalità, proponeva la veicolazione di *e-mail* promozionali utilizzando liste realizzate in assenza di un'ideale base giuridica. È stata pertanto comminata al titolare una sanzione di 5.000 euro, imponendo il divieto di utilizzo dei dati raccolti (provv. 2 marzo 2023, n. 60, doc. web n. 9880317).

All'esito di un'attività ispettiva il Garante ha adottato un provvedimento correttivo nei confronti di un titolare che realizza banche dati per il *marketing* attraverso un sito web di annunci gratuiti. Tenuto conto che non erano emerse illecite rilevanti, sono state date prescrizioni – veicolando principi di carattere generale – soprattutto in merito alla corretta gestione dei ruoli dei vari soggetti coinvolti nella filiera del trattamento dei dati (provv. 11 gennaio 2023, n. 9, doc. web n. 9861941).

Sempre con riferimento alle banche dati realizzate illecitamente per finalità di *marketing*, il Garante, a seguito di un reclamo, ha adottato un provvedimento di divieto e sanzionatorio con il quale sono stati altresì illustrati principi di carattere generale quanto all'uso del legittimo interesse per le attività di *marketing* e all'illiceità delle condotte basate sull'utilizzo per finalità promozionali di dati rilasciati dagli utenti per altre finalità. Alla società è stata comminata una sanzione di 10.000 euro (provv. 17 maggio 2023, n. 202, doc. web n. 9899880).

11.1.8. Attività svolte nell'ambito della tutela del consumatore nei servizi di comunicazione elettronica

Il Garante è presente tra le autorità competenti a cooperare nel *network* europeo CPC (*Consumer Protection and Cooperation*) in base al reg. (UE) 2017/2394 del Parlamento europeo e del Consiglio sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori e che abroga il reg. (CE) 2006/2004, entrato in vigore il 12 dicembre 2017 e applicabile a decorrere dal 17 gennaio 2020.

In particolare, il Garante è competente a intervenire in caso di violazione delle norme di cui all'art. 13 della dir. 2002/58/CE, attuato dall'art. 130 del Codice in materia di comunicazioni indesiderate. A tal fine, l'Autorità ha preso parte a una serie di incontri con la Commissione europea e con altre autorità europee competenti in materia di tutela del consumatore. Gli incontri sono stati finalizzati ad avviare tavoli di studio e confronto sulle tematiche di comune interesse e sui possibili margini di cooperazione.

Il Garante partecipa anche alla *Task Force Consumer & Competition* (TF C&C), al fine di aumentare le occasioni di coordinamento a livello europeo tra le materie oggetto di tutela delle autorità di protezione dati e quelle di competenza delle autorità di tutela della concorrenza e del consumatore. Al momento i lavori della TF C&C sono incentrati sulla realizzazione di linee guida in merito all'interrelazione fra il RGPD e il *Data Markets Act* (DMA) (cfr. cap. 21).

11

12 Servizi di comunicazioni elettroniche e internet

12.1. *Meta Election Day Information (EDI)*

Il Garante ha adottato un provvedimento d'urgenza nei confronti di Meta in relazione alla funzionalità *Election Day Information* (EDI) applicata in occasione delle elezioni per il rinnovo del Parlamento italiano a settembre 2022 (provv. 21 dicembre 2022, n. 448, doc. web n. 9853406).

A seguito di tale provvedimento, sono state attivate dal Garante due distinte procedure volte a ottenere il riconoscimento della competenza nazionale esclusiva a procedere. L'Autorità irlandese ha riconosciuto tale competenza del Garante avendo valutato che i trattamenti posti in essere da Meta mediante la funzionalità EDI incidono in modo sostanziale unicamente sugli interessati italiani (conformemente a quanto previsto dall'art. 56, par. 2, RGPD). L'Autorità ha quindi notificato le contestazioni delle presunte violazioni ai sensi dell'art. 166 del Codice, con contestuale avvio del relativo procedimento.

12.2. *Conservazione di dati di traffico*

All'esito di un'attività ispettiva avviata sulla base di un reclamo e di una segnalazione, il Garante è intervenuto nei confronti di un titolare, operatore di comunicazione elettronica accessibile al pubblico, che offre servizi di invio di SMS tramite web. Nel provvedimento, correttivo e sanzionatorio, è stata dichiarata l'illiceità della conservazione del contenuto degli SMS, sono state rilevate misure inadeguate per la conservazione dei dati di traffico ed è stata espressa una pronuncia in merito alle basi giuridiche da utilizzare per effettuare controlli antifrode, fornendo alcuni preliminari chiarimenti rispetto all'uso del legittimo interesse quale base giuridica. Alla società è stata comminata una sanzione di 80.000 euro (provv. 11 gennaio 2023, n. 12, doc. web n. 9864063).

12.3. *Data retention per finalità giudiziarie*

Anche nel corso del 2023 sono pervenute, seppur in numero minore rispetto agli anni precedenti, segnalazioni e reclami in materia di *retention* di dati del traffico telefonico, e in particolare, di mancato o tardivo riscontro ad istanze di accesso ai tabulati per finalità giudiziarie (civili e penali).

Per tali ultimi casi, è stata inviata una nota, con cui è stato informato il segnalante/reclamante che, *ictu oculi*, in base alla normativa di riferimento (essenzialmente artt. 123 e 132 del Codice, come modificato dal d.l. n. 132/2021, convertito in legge il 30 novembre 2021), è possibile ottenere l'accesso ai tabulati tramite la magistratura ordinaria in sede di procedimento penale e non più rivolgendosi direttamente alla compagnia telefonica.

L'Autorità ha curato il seguito giudiziario dei provvedimenti adottati, fra il 2020 e il 2022, nei confronti di una nota compagnia telefonica (impugnati dalla medesima) riguardanti la normativa previgente (art. 132 del Codice), che riconosceva all'imputato/indagato la possibilità di rivolgersi all'Autorità in caso di diniego (totale o parziale),

da parte della compagnia, della richiesta di accesso effettuata dall'interessato (cfr. cap. 20.2).

12

12.4. Cookie e altri strumenti di tracciamento di dati personali

In tema di strumenti di tracciamento dei dati personali, è stato avviato un procedimento teso a verificare la liceità dell'implementazione da parte dei principali gruppi editoriali italiani di un meccanismo di *cookie wall* in cui la mancata prestazione del consenso alla ricezione dei *cookie* impedisce l'accesso ai siti di informazione. A seguito di informazioni raccolte presso quattro tra i principali gruppi editoriali nazionali, attese le relative possibili violazioni, l'Autorità ha proceduto ad inviare le previste contestazioni ai sensi dell'art. 166, comma 5, del Codice.

Parallelamente, il Garante ha aperto un'istruttoria – relativa al tema in argomento – anche nei confronti di un fornitore di servizi di posta elettronica. Anche per tale procedura, l'Autorità ha inviato la comunicazione con le contestazioni delle presunte violazioni emerse in fase istruttoria.

L'Autorità ha altresì avviato accertamenti da remoto in merito alla conformità di numerosi siti web agli obblighi in materia di trattamento dei dati personali degli utenti per il tramite di *cookie* e altri strumenti di tracciamento, anche a seguito della ricezione di un significativo numero di segnalazioni e reclami. In particolare l'Autorità, in collaborazione con il Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza, ha svolto una serie di verifiche puntuali volte ad accertare il rispetto, da parte di diversi siti web, delle indicazioni contenute nelle linee guida in materia di *cookie* e altri strumenti di tracciamento adottate il 10 giugno 2021 ed entrate in vigore a gennaio 2022 (cfr. par. 19.2).

12.5. Trattamento di dati personali in rete

Il Garante è intervenuto nei confronti di una ditta individuale che, all'esito di lunghe e complesse indagini, è risultata intestataria di un sito web nel quale erano da anni pubblicati, in forma di elenco, numerosissimi dati personali come nominativi, indirizzi e numeri di telefono anche appartenenti a soggetti non presenti negli elenchi telefonici pubblici. Il sito era oggetto dal 2012 di numerose segnalazioni da parte di persone che erano state inserite in tale elenco a loro insaputa e non erano riuscite a esercitare il diritto di cancellazione. Con riguardo a un altro sito web, risultato appartenere allo stesso intestatario, era stato adottato un analogo provvedimento di divieto e sanzionatorio il 26 maggio 2022, n. 204 (doc. web n. 9780409). L'assoluta mancanza di riferimenti nel sito e l'utilizzo di *server* sempre diversi ubicati all'estero hanno reso necessarie lunghe indagini per individuare il soggetto intestatario di detti siti web. Alla ditta individuale, data la gravità delle violazioni rilevate, l'elevato nocumento e la condotta dolosa, è stata comminata una sanzione di 60.000 euro. Con il provvedimento in esame il Garante ha chiarito che è illecita la creazione di elenchi telefonici pubblici ricavati da informazioni che non siano state estratte dal *database* unico - DBU (prov. 17 maggio 2023, n. 201, doc. web n. 9903067).

L'Autorità ha richiesto al Nucleo speciale *privacy* della Guardia di finanza un accertamento ispettivo presso la sede legale di un titolare, che si occupava di pubblicizzare, mediante sito internet, le opere di artisti e i profili di quest'ultimi. L'azienda in questione non aveva fornito riscontro alla richiesta di informazioni formulata dall'Autorità successivamente a un reclamo, con il quale l'interessato aveva lamentato la perdurante presenza nel sito internet dei suoi dati personali nonostante

12

l'istanza di cancellazione e l'avvenuta cessazione del contratto di pubblicazione. Con l'atto di avvio del procedimento, ai sensi dell'art. 166, comma 5, del Codice, è stata contestata la violazione di disposizioni del RGPD, in particolare la diffusione di dati personali nel web in assenza di una idonea base giuridica, il mancato riscontro all'istanza di esercizio dei diritti formulata dall'interessato e l'omessa tempestiva registrazione della relativa opposizione, oltre alla conservazione ingiustificatamente prolungata dei dati del reclamante.

Da un reclamo in materia di diritto all'oblio concernente portali e motori di ricerca, è emersa la necessità d'indagare, prima mediante richieste cartolari e, poi, non essendosi queste rivelate risolutive, mediante accertamento *in loco*, i trattamenti di dati riconducibili ai titolari dei detti motori, con particolare riguardo alla conservazione dei dati di navigazione e alla loro comunicazione a Google nonché alle attività di *marketing* e profilazione indicate nei rispettivi siti web. Dall'accertamento condotto sono emersi i presupposti di alcune violazioni (con riferimento non solo al citato passaggio di dati, ma anche alla loro raccolta (e ai successivi trattamenti) mediante i *form* relativi a siti web e *cookies*, venendo in rilievo alcuni meccanismi di consenso non libero e specifico per le singole finalità di trattamento perseguite.

Nel provvedimento, l'Autorità ha affrontato anzitutto il profilo relativo al servizio di motore di ricerca offerto all'interno dei predetti portali e riconducibile a Google LLC, anche con riferimento ai corrispondenti ruoli nel trattamento dei dati di navigazione; a tal riguardo è stata debitamente interessata anche l'Autorità irlandese, quale autorità capofila ai sensi dell'art. 56, par. 1, del RGPD rispetto ai trattamenti della società americana. Sono stati considerati anche ulteriori distinti aspetti, quali la gestione dei consensi per finalità di *marketing* e profilazione, il trattamento di dati di minori in occasione dell'attivazione di *account* di posta elettronica e il trattamento di dati eccedenti (quali il documento di identità) per la chiusura di caselle di posta elettronica. Essendo la società intervenuta autonomamente per correggere molte delle problematiche sopra indicate, si è ritenuto di ingiungere, soltanto con riferimento ai trattamenti condivisi con Google LLC connessi alla ricerca in internet, di fornire un'idonea informativa con la quale descrivere tali trattamenti e i relativi ruoli, anche con riguardo alla gestione dei diritti degli interessati.

12.6. *Trattamento di dati personali mediante dispositivi connessi*

A seguito della collaborazione, già avviata nel 2021, con l'Autorità di protezione dei dati irlandese sull'analisi degli *Smart glasses Ray-ban stories*, un dispositivo connesso ed indossabile nonché dotato di assistente vocale, progettato e commercializzato da Facebook/Meta in collaborazione con un'azienda italiana specializzata nella produzione e nel commercio di occhiali, il Garante ha concluso la relativa istruttoria, raccogliendo le diverse informazioni. In particolare, l'intervenuta integrazione degli occhiali intelligenti con il servizio di messaggistica WhatsApp, le caratteristiche del dispositivo e le sue modalità di funzionamento, hanno fatto concludere per l'applicabilità alla fattispecie della normativa speciale di cui alla direttiva *e-Privacy*.

Non trovando pertanto applicazione il meccanismo dello sportello unico di cui all'art. 60 del RGPD, il Garante ha esercitato i propri poteri per condurre un'investigazione mirata sotto tale prospettiva rilevando diverse possibili violazioni, tra le quali quelle relative all'art. 122 del Codice e ai principi generali disciplinati dal RGPD. Tali presunte violazioni sono state notificate e comunicate al titolare, ai sensi dell'art. 166, comma 5, del Codice, per l'avvio del relativo procedimento.

12.7. Attività in materia di trattamento dati mediante sistemi di intelligenza artificiale

12

L'esigenza di assicurare la tutela dei diritti e delle libertà degli interessati è emersa con particolare rilievo a fronte dei nuovi rischi derivanti dal trattamento di dati personali su larga scala connessi alla creazione e al funzionamento di servizi di intelligenza artificiale generativa.

Con riferimento a tale ambito, l'Autorità è intervenuta nei confronti di una società statunitense che gestisce un noto modello di intelligenza artificiale relazionale in grado di simulare ed elaborare conversazioni umane. Attesa l'assenza di una informativa agli utenti e a tutti gli interessati i cui dati erano stati raccolti dal titolare e trattati nell'ambito del servizio, l'assenza di una base giuridica idonea a giustificare la raccolta e la conservazione massiva di dati personali allo scopo di "addestrare" gli algoritmi sottesi al funzionamento della piattaforma, la non corrispondenza di alcune delle informazioni fornite dal servizio al dato reale e la conseguente inesattezza dei dati personali oggetto delle attività di trattamento del titolare, nonché l'assenza di qualsivoglia filtro per la verifica dell'età degli utenti, il Garante ha adottato un provvedimento urgente di limitazione provvisoria del trattamento dei dati personali degli interessati stabiliti nel territorio italiano (provv. 30 marzo 2023, n. 112, doc. web n. 9870832).

A fronte delle informazioni acquisite e della disponibilità manifestata dal titolare a porre in essere una serie di misure concrete a tutela dei diritti e delle libertà degli interessati l'Autorità ha adottato un successivo provvedimento di sospensione della limitazione provvisoria (provv. 11 aprile 2023, n. 114, doc. web n. 9874702) a condizione che il titolare adottasse un'informativa nei termini e con le modalità di cui all'art. 12 del RGPD e la rendesse facilmente disponibile, attraverso un *link*, sin dalla fase di registrazione e in una posizione che ne consentisse la lettura prima di procedere alla registrazione; predisponesse misure idonee a garantire l'esercizio dei diritti degli interessati e uno strumento attraverso il quale poter chiedere e ottenere la correzione di eventuali dati personali ovvero procedere alla cancellazione degli stessi; offrisse uno strumento facilmente accessibile attraverso il quale esercitare il diritto di opposizione al trattamento dei propri dati acquisiti in sede di utilizzo del servizio per l'addestramento degli algoritmi qualora la base giuridica fosse il legittimo interesse; modificasse la base giuridica del trattamento dei dati personali degli utenti ai fini dell'addestramento degli algoritmi, eliminando ogni riferimento al contratto e assumendo come base giuridica del trattamento il consenso o il legittimo interesse, in relazione alle valutazioni di competenza della società, in una logica di *accountability*; inserisse un filtro basato sull'età degli utenti (*age gate*) che escludesse, sulla base dell'età dichiarata, gli utenti minorenni; sottoponesse al Garante un piano per l'adozione di strumenti di *age verification*; promuovesse una campagna di informazione, di natura non promozionale, su tutti i principali mezzi di comunicazione di massa italiani.

Nei confronti dello stesso titolare l'Autorità sta proseguendo l'attività istruttoria anche nell'ambito di una *task force* costituita *ad hoc* in seno al Comitato europeo per la protezione dei dati personali.

Sempre con riferimento al trattamento dei dati personali attraverso servizi che si basano su LLM (*large language models*) l'Autorità aveva altresì adottato un provvedimento urgente di limitazione provvisoria del trattamento dei dati personali degli interessati stabiliti nel territorio italiano effettuato da una società statunitense che offre un *chatbot*, con interfaccia scritta e vocale, basato sull'intelligenza artificiale che genera un amico virtuale (provv. 2 febbraio 2023, n. 39, doc. web n.9852214) rilevando l'assenza, nelle informazioni fornite agli utenti, dell'indicazione degli elementi essenziali, l'assenza di una base giuridica idonea a giustificare le varie operazioni

12

di trattamento, nonché di qualsivoglia filtro per la verifica dell'età degli utenti sia in fase di registrazione al servizio che di utilizzo dello stesso.

In esito alle successive interlocuzioni con il titolare, il Garante ha disposto la sospensione della predetta limitazione provvisoria (provv. 22 giugno 2023, n. 280, doc. web n. 10013893) a condizione che il titolare presentasse agli utenti italiani una informativa aggiornata, implementasse un filtro per la verifica dell'età (*age gate*) in tutte le pagine di registrazione ai servizi correlato a un "periodo di raffreddamento" (*cooling-off period*) volto ad evitare che i minorenni inserissero una data di nascita diversa quando fosse stato loro negato l'accesso ai servizi, predisponesse a favore degli utenti in Italia la possibilità di esercitare in modo semplice ed efficace i propri diritti in materia di protezione dei dati personali, e sottoponesse al Garante un piano per lo sviluppo di un processo volto ad impedire l'accesso al servizio a soggetti di età inferiore ai 18 anni, eventualmente corredato da un meccanismo di analisi del linguaggio avente efficacia interdittiva successiva, nonché un piano per l'implementazione di funzioni che consentissero agli utenti di segnalare i contenuti inappropriati. Anche nei confronti di tale titolare l'Autorità sta proseguendo l'attività istruttoria.

Da ultimo, il Garante ha avviato un'indagine conoscitiva in materia di *web scraping* che si concluderà nel 2024 allo scopo di acquisire osservazioni, commenti ed eventuali proposte operative sulle misure adottate ed adottabili dai gestori di siti internet e di piattaforme, sia pubblici che privati, rispetto alla raccolta massiva di dati personali, effettuata appunto attraverso tecniche di *web scraping*, da parte di società che sviluppano sistemi di intelligenza artificiale generativa, per finalità di addestramento dei relativi algoritmi (provv. 21 dicembre 2023 n. 621, doc. web n. 9972593).

12.8. *Schemi di decisione finale ai sensi dell'art. 60, par. 7 o 8, del RGPD*

L'Autorità ha adottato lo schema di decisione finale ai sensi dell'art. 60, par. 8, del RGPD in un caso relativo a una società con sede a Cipro (provv. 27 aprile 2023, n. 174, doc. web n. 9908362) sulla scorta di un progetto di decisione presentato dall'Autorità cipriota in cui si proponeva l'archiviazione di un reclamo italiano, in quanto non era stata ravvisata alcuna violazione da parte del titolare che, nel procedimento, si era dichiarato estraneo rispetto alla condotta lamentata dal reclamante. Tuttavia, con tale decisione si è ritenuto opportuno segnalare all'Autorità cipriota che il fenomeno delle chiamate indesiderate volte a promuovere attività di *trading online* (oggetto di doglianza) sta assumendo in Italia proporzioni sempre più rilevanti e, da alcune segnalazioni e reclami giunti all'attenzione del Garante, si ricava, spesso, il coinvolgimento, in varie forme, di titolari o responsabili stabiliti a Cipro. Pertanto è stato chiesto all'Autorità cipriota, che in questi casi è la capofila (LSA) ai sensi del RGPD, di monitorare il fenomeno e di predisporre tutte le misure e strategie adatte per espletare un'efficace azione di controllo.

12.9. *Procedure di cooperazione europea relative a trattamenti transfrontalieri di dati personali effettuati da fornitori di servizi della società dell'informazione*

Il meccanismo dello sportello unico, meglio conosciuto nella formulazione inglese *one stop shop*, rappresenta un sistema decisionale condiviso, unico nel suo genere a livello europeo, che si basa sui due principi complementari di cooperazione (tra autorità di controllo) e di coerenza (tramite l'intervento del CEPD e, in alcuni casi, della Commissione europea). Tale meccanismo, giunto al quinto anno di applicazione,

12

grazie all'esperienza maturata e a una serie di linee guida adottate dal Comitato, costituisce un sistema amministrativo pan-europeo ormai rodato e di costante, crescente rilevanza, sia in termini quantitativi che qualitativi; si deve infatti evidenziare che i casi di trattamento transfrontaliero di dati personali sono ormai ordinari, specialmente nell'ambito dei servizi della società dell'informazione, in relazione ai quali il principio giuridico di territorialità nazionale ha perso, da tempo, pregnanza ed efficacia.

Nell'anno 2023 le procedure di cooperazione nel settore delle reti telematiche sono aumentate del 23% circa (cfr. sez. IV., tab. 16) con un forte incremento dei casi con procedura di risoluzione amichevole (*amicable settlement*), una procedura di definizione bonaria delle controversie che coniuga il perseguimento di una celere e soddisfacente tutela dei reclamanti con l'esigenza di deflazionare il carico di lavoro che grava sulle autorità di controllo. Tale procedura viene utilizzata, in quanto prevista nelle rispettive legislazioni nazionali, dalle Autorità irlandese ed olandese, sulla base delle linee guida del CEPD 6/2022 sull'*amicable settlement* e delle linee guida del CEPD 2/2022 sull'applicazione dell'art. 60 del RGPD. In tali istruttorie l'autorità di controllo assume un ruolo di mediazione tra titolare e reclamante, al fine di risolvere, ove possibile, la doglianza sollevata in un reclamo, in particolar modo con riferimento ai reclami concernenti i diritti di cui agli artt. da 15 a 22 del RGPD, in cui l'adempimento da parte di un titolare all'esercizio di un diritto di un interessato, in assenza di criticità sistematiche, può giustificare la chiusura del caso senza pregiudizio per la tutela del diritto fondamentale.

Nel merito, le tematiche trattate nell'ambito dei meccanismi di cooperazione e coerenza sono di precipuo interesse e spaziano dalla base giuridica per il trattamento dei dati personali per finalità di pubblicità comportamentale, alla tutela dei minori nella società dell'informazione, al trattamento di dati di geolocalizzazione sino al tema del trasferimento dei dati personali verso Paesi terzi.

Nel periodo di interesse, con specifico riferimento alle tendenze generali delle procedure di cooperazione, è stata confermata la prevalenza delle procedure di vera e propria cooperazione (artt. 60 e ss. RGPD) rispetto alle pur numerose procedure preliminari ai sensi dell'art. 56 del RGPD, ovvero sia le procedure relative alla fase iniziale di individuazione dell'autorità capofila e delle autorità interessate. Tale fenomeno è dovuto principalmente al fatto che, con riferimento ai titolari del trattamento più conosciuti (si pensi ai grandi fornitori statunitensi di servizi della società dell'informazione e di *social network* stabiliti in Irlanda), le rispettive autorità capofila sono ormai pacificamente note e i reclami per i quali le stesse sono competenti vengono trasmessi direttamente. Nello specifico, un numero considerevole di procedure trattate dall'Autorità in relazione ai reclami proposti da interessati italiani nei confronti di titolari stabiliti in Irlanda è da attribuire all'attività di cooperazione con l'Autorità di controllo irlandese. Con riferimento a tale tipologia di procedure è stata riscontrata una più efficiente gestione dei casi grazie a una trattazione standardizzata, sebbene sempre personalizzata, delle comunicazioni che intercorrono tra il Garante e l'Autorità di controllo irlandese nonché tra quest'ultima e i reclamanti, tramite il Garante.

Nel contesto delle procedure di vera e propria cooperazione è emerso un costante incremento, in linea con le linee guida 2/2022 sull'art. 60 del RGPD, della ricerca di un consenso condiviso tra autorità capofila e autorità di controllo interessate sin dalle fasi istruttorie e pre-decisorie, mediante condivisione delle relazioni investigative finali e l'anticipazione dei progetti di decisione (i quali, come noto, sono sottoposti a una procedura assai rigida connotata da strettissimi termini perentori) attraverso procedure di consultazione informale o di assistenza reciproca rispettivamente ai sensi degli artt. 60 e 61 RGPD. La cooperazione è stata rafforzata anche dall'attuazione, a seguito delle decisioni assunte nella riunione delle autorità tenutasi a Vienna

12

nell'aprile 2022 (v. Relazione 2022, p. 177), del particolare regime previsto per i casi di importanza strategica (*strategic cases*) dal CEPD sulla scorta di una predefinita procedura di selezione. Il Garante è stato attivamente coinvolto, in collaborazione con altre autorità di controllo, nella trattazione congiunta di un caso che l'Autorità aveva già delineato come prioritario per la tematica correlata (*Internet of Things*).

Lo strumento della consultazione informale è stato utilizzato, in particolare, dall'Autorità irlandese per condividere la documentazione relativa alla fase esecutiva (ordini di messa in conformità) delle decisioni finali *ex art.* 65, par. 6, del RGPD, adottate in ottemperanza delle decisioni vincolanti del CEPD 2 e 3 del 2022 relative alla questione della base giuridica per il trattamento di dati personali per finalità di pubblicità comportamentale da parte di Meta in relazione ai servizi Facebook e Instagram. Come noto, il dibattito sulle condizioni di validità del consenso in relazione al modello *cd. pay or ok* è tuttora in corso e viene seguito con attenzione dal Garante. Il dibattito si è ulteriormente arricchito in concomitanza con la pubblicazione dell'elaborato della Commissione UE sul *cd. cookie pledge*, nonché con la recente approvazione da parte della plenaria del CEPD del documento nel quale ha espresso il proprio parere in merito (cfr. par. 21.2).

Nel 2023 sono giunte a decisione, in esito al meccanismo di coerenza, importanti indagini nei confronti di grandi titolari internazionali stabiliti nell'Unione europea. Si tratta di decisioni che esprimono l'efficacia e la vitalità del meccanismo dello sportello unico e la forza del contraddittorio tra autorità su tematiche di indiscutibile complessità e attualità.

Tra le numerose decisioni finali cui il Garante ha cooperato, particolare interesse rivestono le due decisioni vincolanti del CEPD nei confronti di Meta Platforms Ireland Ltd. (di seguito Meta) e TikTok Technology Ltd. (di seguito TikTok) alla cui stesura il Garante ha partecipato in qualità di autorità di controllo interessata.

La prima decisione vincolante (1/2023) si riferisce a un progetto di decisione condiviso dall'Autorità irlandese relativo al trasferimento di dati personali verso gli Stati Uniti da parte di Meta in relazione al servizio Facebook. Il progetto di decisione ha avuto origine da una istruttoria d'ufficio avviata il 28 agosto 2020 con riferimento alla liceità dei trasferimenti internazionali di dati personali di interessati nell'area SEE che visitano, accedono, utilizzano o interagiscono con il servizio Facebook, effettuati da Meta sulla base di clausole contrattuali tipo, ai sensi dell'art. 46, par. 2, lett. d), del RGPD, successivamente alla sentenza della Corte di giustizia dell'UE pronunciata il 16 luglio 2020 nella causa C-311/18 (*cd. sentenza Schrems II*). A seguito della presentazione di alcune obiezioni motivate e pertinenti, in data 19 gennaio 2023, l'Autorità di controllo irlandese ha sottoposto la controversia al CEPD ai sensi dell'art. 60, par. 4, del RGPD, avviando così la procedura di risoluzione delle controversie ai sensi dell'art. 65, par. 1, lett. a), del RGPD stesso. Con decisione 13 aprile 2023, il CEPD ha invitato l'Autorità di controllo irlandese a imporre a Meta una sanzione amministrativa pecuniaria per la violazione (già accertata dall'Autorità irlandese nel progetto di decisione) dell'art. 46, par. 1, del RGPD, in linea con i principi di efficacia, proporzionalità e dissuasività, sulla base della valutazione dei fattori di cui all'art. 83, par. 2, del RGPD, dettagliatamente delineati, nonché dei fattori aggravanti di cui all'art. 83, par. 2, lett. a), b), g), d) e k), del RGPD. Applicando per la prima volta i principi espressi nelle proprie linee guida 4/2022 sul calcolo delle sanzioni pecuniarie, il CEPD ha qualificato la violazione *de qua* di elevata gravità e ha indicato l'importo iniziale per l'ulteriore calcolo della sanzione a un livello compreso tra il 20 e il 100 % del massimo edittale applicabile, prendendo come riferimento il fatturato consolidato del gruppo guidato da Meta Platforms, Inc. Quanto alle misure correttive, il CEPD nella decisione vincolante citata ha invitato l'Autorità di controllo irlandese a includere nella sua decisione finale un ordine

di messa in conformità dei trattamenti al Capo V del RGPD, prescrivendo al titolare di cessare, entro sei mesi dalla data di notifica della decisione definitiva, il trattamento illecito, compresa la conservazione, dei dati personali degli utenti dell'area SEE trasferiti in violazione del RGPD negli Stati Uniti.

In data 12 maggio 2023 l'Autorità irlandese, conformandosi alla decisione vincolante del CEPD, ha modificato il proprio progetto di decisione e adottato la decisione finale ai sensi dell'art. 65, par. 6, del RGPD, infliggendo a Meta una sanzione amministrativa pari a 1,2 miliardi di euro (la sanzione più alta in assoluto dall'entrata in vigore del RGPD) e ordinando la messa in conformità dei trasferimenti verso Paesi terzi ai sensi dell'art. 58, par. 2, lett. d), del RGPD nel termine di sei mesi.

La seconda decisione vincolante (2/2023) del CEPD si riferisce a un progetto di decisione condiviso dall'Autorità irlandese nei confronti di TikTok. Tale progetto di decisione ha avuto origine da una istruttoria d'ufficio avviata il 14 settembre 2021 in merito al rispetto da parte di TikTok degli obblighi di cui agli artt. 5, 12, 13, 24 e 25 del RGPD in relazione al trattamento di dati personali degli utenti registrati nella piattaforma TikTok di età compresa tra 13 e 17 anni, nonché alcune questioni relative al trattamento dei dati personali relativi a minori di età inferiore a 13, nel periodo temporale compreso tra il 31 luglio ed il 31 dicembre 2020. A seguito della presentazione di alcune obiezioni pertinenti e motivate, in data 10 maggio 2023 l'Autorità di controllo irlandese ha sottoposto la controversia al CEPD ai sensi dell'art. 60, par. 4, del RGPD, avviando così la procedura di risoluzione delle controversie ai sensi dell'art. 65, par. 1, lett. a), di quest'ultimo.

Con decisione 2 agosto 2023, il CEPD ha invitato l'Autorità di controllo irlandese a includere nella sua decisione finale l'ulteriore violazione del principio di correttezza di cui all'art. 5, par. 1, lett. a), del RGPD, con conseguente estensione dell'ordine di messa in conformità originariamente previsto nel progetto di decisione con riferimento ai *pop-up* di registrazione e di pubblicazione dei video nella piattaforma TikTok. In merito all'art. 25 del RGPD, il CEPD ha invece ritenuto, sulla base degli elementi a sua disposizione nel contesto della procedura di coerenza, di non disporre di informazioni sufficienti per valutare in modo definitivo la sussistenza di una violazione del principio di *privacy by design* nel periodo di riferimento e ha invitato l'Autorità irlandese a modificare la conclusione del progetto di decisione in tal senso.

È parimenti rilevante la partecipazione dell'Autorità, sempre in sede di CEPD, alla stesura della decisione vincolante d'urgenza (1/2023), ai sensi dell'art. 66, par. 2, del RGPD, approvata dal CEPD in data 27 ottobre 2023 relativa a una richiesta avanzata dall'Autorità norvegese di adozione di misure definitive in merito al trattamento dei dati personali degli interessati in Norvegia, per finalità di pubblicità comportamentale (*online behavioural advertising* - OBA) senza adeguata base giuridica da parte di Meta in relazione al servizio Facebook. In esito alla procedura di coerenza, il CEPD ha ritenuto necessario disporre un divieto di trattamento ai sensi dell'art. 58, par. 2, lett. f), del RGPD relativamente al trattamento dei dati, ai fini di OBA, da parte di Meta sulla base dell'art. 6, par. 1, lett. b) e f), del RGPD in tutta l'area SEE.

Da ultimo, risulta degna di menzione l'attività di cooperazione svolta in merito alla procedura condotta dall'Autorità francese con riferimento a una società specializzata in *retargeting advertising*, mediante tracciamento della navigazione degli utenti in internet nei siti web *partner*, per l'offerta in tempo reale (*real time bidding*) di annunci pubblicitari personalizzati. Il procedimento era stato avviato dall'Autorità francese a seguito della presentazione di una serie di reclami da parte di *Privacy International* e NOYB e si è concluso con una decisione finale (condivisa da tutte le autorità di controllo, senza intervento del CEPD) con cui l'Autorità francese, accertata la violazione dell'art. 7, par. 1, del RGPD, per mancanza di un valido consenso degli utenti per il trattamento dei loro dati per finalità di pubblicità personalizzata,

12

nonché degli artt. 12, par. 1 e 13 del RGPD, per carenze informative in merito alla base giuridica e alle finalità del trattamento, ha inflitto alla società una sanzione amministrativa pari a 40 milioni di euro.

13 La protezione di dati personali nel rapporto di lavoro privato e pubblico

13.1. *Trattamento di dati mediante la posta elettronica*

Il Garante ha adottato numerosi provvedimenti riguardanti il trattamento dei dati personali effettuato mediante la posta elettronica nell'ambito del rapporto di lavoro.

Al riguardo è stato ribadito che, in tale contesto, il trattamento deve conformarsi al rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato, in particolare se riguarda comunicazioni effettuate mediante l'*account* di posta elettronica, considerate le particolari tutele che l'ordinamento ricollega alle diverse forme di comunicazione. Non vi è dubbio, infatti, che la protezione della vita privata riguardi anche l'ambito lavorativo, nel quale si sviluppano relazioni dove si esplica la personalità del lavoratore (v. artt. 2 e 41, comma 2, Cost.), tenuto anche conto che la linea di confine tra ambito lavorativo/professionale e ambito strettamente privato non sempre può essere tracciata con chiarezza (si pensi, al riguardo, all'ampia giurisprudenza della Corte EDU sul punto – per tutte, v. Copland v. UK, 3 aprile 2007 (ric. n. 62617/00), spec. par. 41, e Bărbulescu v. Romania [GC], 5 settembre 2017 (ric. n. 61496/08), spec. par. 70-73).

Tutta questa materia si colloca al crocevia fra la disciplina di protezione dei dati e le norme di settore in materia di controlli a distanza, alle quali il legislatore nazionale ha fatto rinvio esplicito in sede di adeguamento dell'ordinamento nazionale alle norme del RGPD (artt. 113, 114 e 171 del Codice; art. 88 del RGPD; artt. 4 e 8, l. n. 300/1970 e succ. mod.).

Nell'anno di riferimento il Garante ha adottato un provvedimento nei confronti di una società che, in qualità di titolare del trattamento, aveva mantenuto attivo, successivamente alla cessazione della collaborazione (e non rapporto di lavoro subordinato) con la reclamante, l'*account* di posta elettronica a lei assegnato con estensione riferita alla società; era stato predisposto anche un sistema automatico di inoltro al direttore commerciale delle comunicazioni in entrata, che consentiva di prendere visione del contenuto dello stesso *account*, tanto da avere prodotto in giudizio *e-mail* inviate nel corso della collaborazione.

Il Garante ha accertato che la condotta del titolare era stata posta in essere in assenza di un idoneo criterio di legittimazione per l'effettuazione del trattamento, quindi in violazione degli artt. 5, par. 1, lett. a) e 6 del RGPD.

Considerato inoltre che non è emerso che il titolare avesse fornito all'interessata un'idonea informativa sul trattamento effettuato sull'*account* di posta elettronica, l'Autorità ha accertato la violazione degli artt. 12 e 13 del RGPD, in proposito precisando che anche nell'ambito di trattative precontrattuali l'obbligo di informare gli interessati è altresì espressione del principio generale di correttezza (art. 5, par. 1, lett. a), del RGPD). È stato inoltre accertato che la società, non avendo fornito un idoneo riscontro all'istanza di cancellazione presentata dalla reclamante, aveva violato l'art. 12, par. 4, del RGPD con riferimento all'art. 17 di quest'ultimo.

Per le violazioni riscontrate il Garante ha comminato una sanzione pecuniaria.

Il titolare del trattamento ha impugnato la decisione davanti all'Autorità giudiziaria ordinaria. Con sentenza 20 luglio 2023 il Tribunale di Reggio Emilia ha confermato il provvedimento del Garante, relativamente alla contestazione degli artt. 5, par. 1, lett. a) e 12 anche con riferimento agli artt. 17, 13 del RGPD, seppure riducendo

Trattamento dell'*account* di posta elettronica assegnato nell'ambito di una collaborazione

**Trattamento
dell'*account* di posta
elettronica assegnato
nell'ambito di un
rapporto di tirocinio**

l'entità della sanzione pecuniaria, dichiarando l'insussistenza della violazione di cui agli artt. 5, par. 1, lett. c) e 6 del RGPD (provv. 11 gennaio 2023, n. 8, doc. web n. 9861827).

Il tema del trattamento dell'*account* di posta elettronica individualizzato è stato affrontato dal Garante anche con riferimento al rapporto di tirocinio, a fronte di un reclamo con il quale è stato lamentato l'illecito trattamento dell'*account* che era stato assegnato al reclamante nell'ambito di un tale rapporto.

Il Garante ha accertato che un consorzio aveva mantenuto attivo l'*account* predetto accedendo alle relative comunicazioni successivamente alla interruzione del tirocinio; è emerso inoltre che il consorzio aveva impedito all'interessato di accedere al contenuto dell'*account* e non gli aveva fornito idonea informativa sul trattamento dei dati. Con il provvedimento, si è stabilito che la condotta tenuta dal titolare del trattamento aveva violato gli artt. 5, par. 1, lett. a) e c); 12 e 13 del RGPD.

In proposito è stato precisato che l'orientamento del Garante, secondo il quale è da ritenersi conforme ai principi in materia di protezione dei dati personali che, dopo la cessazione del rapporto di lavoro, il titolare provveda alla rimozione dell'*account* di posta elettronica individualizzato, previa disattivazione dello stesso e contestuale adozione di sistemi automatici volti ad informarne i terzi e a fornire a questi ultimi indirizzi alternativi riferiti alla sua attività professionale, trova applicazione anche con riferimento a relazioni ricollegate all'ambito lavorativo, quali il tirocinio. Pur non traducendosi nell'instaurazione di un rapporto di lavoro subordinato e pur non caratterizzate da una relazione di dipendenza, esse attribuiscono comunque al titolare del trattamento un ampio potere organizzativo, sia interno che esterno. Il titolare del trattamento, resta inteso, anche con riferimento a tali situazioni, non può prendere visione delle comunicazioni in entrata sull'*account* individualizzato assegnato all'interessato.

L'Autorità, in tale occasione, ha inoltre sottolineato che “la legittima necessità di assicurare l'ordinario svolgimento e la continuità dell'attività aziendale nonché di provvedere alla dovuta conservazione di documentazione in base a specifiche disposizioni dell'ordinamento è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale con i quali, attraverso l'adozione di appropriate misure organizzative e tecnologiche, individuare i documenti che, nel corso dello svolgimento dell'attività lavorativa, devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile. [...] I sistemi di posta elettronica non consentono, per loro stessa natura, di assicurare tali caratteristiche”.

L'Autorità ha ritenuto di dover ribadire che il legittimo interesse a trattare dati personali per difendere un proprio diritto in giudizio non può comportare un aprioristico annullamento del diritto alla protezione dei dati personali riconosciuto agli interessati considerato, tra l'altro, che il contenuto dei messaggi di posta elettronica, così come i dati esteriori delle comunicazioni e i *file* allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente.

L'Autorità ha applicato, per le violazioni accertate, una sanzione amministrativa pecuniaria (provv. 9 marzo 2023, n. 68, doc. web n. 9877754).

In un caso particolare oggetto di reclamo all'Autorità presentato da un collaboratore (non dipendente), è emerso che la direzione aziendale di una società, effettuando l'accesso sistematico ad *account* non individualizzati (anche se utilizzati da singoli dipendenti e collaboratori) riconducibili alla società stessa e a una diversa società controllata, aveva potuto visualizzare scambi di *e-mail* avvenuti anche mediante *account* individualizzati, attraverso la ricostruzione a ritroso della “catena” dei messaggi inviati. Con tale configurazione del sistema di gestione degli indirizzi *e-mail* la società ha fornito indicazioni, chiesto chiarimenti ed espresso commenti e

**Accesso del titolare
alle comunicazioni via
e-mail aziendale**

valutazioni (spesso di biasimo) sull'operato di dipendenti e collaboratori, lasciando e/o mettendo in copia tutti gli interlocutori della comunicazione originaria (in alcuni casi inserendone altri), in modo tale che tutti i partecipanti alla conversazione ne apprendessero il contenuto, compresi i soggetti terzi (clienti e consulenti).

Il Garante ha ritenuto illecito il trattamento in relazione ad una pluralità di profili (in particolare per la violazione dei principi di liceità, correttezza, minimizzazione e l'omessa informativa di cui gli artt. 5, par. 1, lett. a) e c), 13 del RGPD), ed ha stabilito che la legittima necessità di garantire la continuità dei flussi comunicativi all'interno dell'azienda può e deve essere perseguita attraverso modalità proporzionate di gestione dei messaggi di posta elettronica, astenendosi dall'effettuare l'intervento sistematico sull'operato di singoli dipendenti e collaboratori, reso noto anche ad altri colleghi/collaboratori, utilizzando in alcuni casi espressioni lesive della dignità anche professionale dei destinatari e realizzando in tal modo un'interferenza nella sfera privata e professionale di collaboratori e dipendenti. Alla società è stata applicata una sanzione amministrativa pecuniaria (provv. 23 marzo 2023, n. 93, doc. web n. 9888206).

L'Autorità si è pronunciata su un reclamo presentato da un collaboratore (non dipendente) di una società che, a seguito dell'accertamento di un'anomalia potenziale indice di un pericolo per la sicurezza dei sistemi, aveva lamentato l'effettuazione di accertamenti da parte dell'amministratore di sistema, pur gradualmente, che avevano portato all'identificazione del reclamante quale utente dei medesimi sistemi, alla sospensione cautelativa del suo *account* e, successivamente, al blocco della casella di posta elettronica e della SIM.

Con il provvedimento è stato ribadito che il datore di lavoro ha l'onere di indicare ai propri dipendenti e collaboratori, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo ritenute corrette degli strumenti messi a disposizione e se, in che misura e con quali modalità, anche all'esito di eventi imprevedibili o eccezionali, vengano effettuati controlli che devono comunque essere conformi ai principi di liceità, proporzionalità e gradualità (v. linee guida del Garante per posta elettronica e internet, provv. 1° marzo 2007, n. 13, doc. web n. 1387522). Nell'ambito del rapporto di lavoro, indipendentemente dalla natura di quest'ultimo, l'obbligo di informare gli interessati circa i trattamenti effettuati o che ci si riserva di effettuare costituisce altresì espressione del principio generale di correttezza (art. 5, par. 1, lett. a), del RGPD).

Con la decisione adottata, il Garante ha stabilito che la società, nel caso concreto, aveva omesso di informare il reclamante circa la specifica modalità di trattamento effettuata mediante i controlli svolti sull'uso dei dispositivi informatici e l'analisi dei dati contenuti all'interno dei dispositivi oggetto di riconsegna (successivamente sottoposti ad attività di indagine forense), in violazione di quanto previsto dall'art. 13 del RGPD nonché dell'art. 5, par. 1, lett. a), del RGPD. Alla società è stata applicata una sanzione amministrativa pecuniaria (provv. 13 aprile 2023, n. 127, doc. web n. 9891673).

Continua ad essere numerosa la casistica sottoposta al Garante relativa alla gestione degli *account* di posta elettronica aziendale dopo la cessazione del rapporto di lavoro.

Il Garante ha accertato che una società, in conformità alla *policy* aziendale interna, aveva mantenuto attivi gli *account* assegnati a due reclamanti per circa due anni a decorrere dal giorno successivo alla cessazione del rapporto di lavoro, previa disattivazione e contestuale reindirizzamento degli stessi su diverso indirizzo aziendale. Con riferimento alle finalità del trattamento così effettuato, l'Autorità ha in primo luogo ritenuto che, in relazione ai fatti oggetto di reclamo, la società non avesse fornito evidenze degli specifici elementi che, subito dopo le dimissioni dei reclamanti,

13

Obbligo di informativa

Gestione di *account* di posta elettronica dopo la cessazione del rapporto di lavoro

13

avrebbero provocato l'insorgere di "numerosi sospetti" nei confronti della correttezza dell'operato degli stessi, e la conseguente decisione di adottare "misure straordinarie", rispetto alle procedure ordinarie di trattamento dei dati personali degli *ex* dipendenti. In realtà la società, in base a quanto accertato, aveva previsto in ogni caso la persistente attività dell'*account* aziendale, senza alcun riferimento a specifiche finalità perseguite dall'*ex* datore di lavoro e senza stabilire la durata del trattamento effettuato mediante il reindirizzamento.

Il Garante ha pertanto stabilito che la sistematica persistente attività dell'*account* aziendale a suo tempo assegnato, anche dopo la cessazione del rapporto di lavoro, mediante il reindirizzamento su *account* di altro dipendente dell'azienda, in assenza della indicazione di alcuna specifica, esplicita e legittima finalità perseguita, non è conforme al principio di minimizzazione dei dati (art. 5, par. 1, lett. c), del RGPD) e di limitazione delle finalità (art. 5, par. 1, lett. b), del RGPD).

Inoltre l'assenza di determinazioni in ordine alla durata del trattamento, individuata in base a quanto ritenuto congruo in relazione alle finalità perseguite, non è conforme al principio di limitazione della conservazione (art. 5, par. 1, lett. e), del RGPD). L'aver inviato, poi, ai terzi mittenti di messaggi diretti all'*account* dell'*ex* dipendente o collaboratore, un messaggio contenente l'indicazione che "l'indirizzo di posta non è più attivo", non risulta conforme al principio di correttezza (art. 5, par. 1, lett. a), del RGPD) in quanto può indurre i suddetti terzi a ritenere che i messaggi non siano oggetto di trattamento da parte della società.

Con riguardo, infine, all'obbligo di informare circa le modalità di gestione della posta elettronica aziendale anche dopo la cessazione del rapporto di lavoro, l'Autorità ha ritenuto che il semplice inserimento di documenti informativi all'interno di una *community* il cui accesso è riservato ai dipendenti, previa iscrizione, non è sufficiente ad adempiere all'obbligo informativo previsto dal RGPD. Il titolare del trattamento avrebbe dovuto quantomeno invitare tutti i dipendenti, con adeguata periodicità, a visionare i documenti contenenti regole interne sulla gestione della posta elettronica e di internet, evidenziandone l'importanza. I trattamenti effettuati dalla società hanno pertanto violato quanto previsto dall'art. 13 del RGPD nonché dall'art. 5, par. 1, lett. a), del RGPD che stabilisce il principio generale di correttezza dei trattamenti. Alla società è stata applicata una sanzione amministrativa pecuniaria (prov. 27 aprile 2023, n. 171, doc. web n. 9909235).

In un caso diverso il Garante, a seguito di una complessa istruttoria avviata a fronte della presentazione di una segnalazione, ha accertato che un'agenzia di assicurazione, dopo aver interrotto il rapporto di collaborazione con due agenti, aveva mantenuto attivi gli *account* di posta elettronica a loro assegnati durante il rapporto di collaborazione per un periodo di tempo considerevole (pari a 120 giorni). Durante questo periodo, le *e-mail* in transito sui predetti *account* venivano reindirizzate all'*account* di un altro collaboratore, con funzioni di "responsabile smistamento", al fine di procedere alla distribuzione dei clienti dei collaboratori cessati. Tale attività aveva, quindi, comportato la conoscibilità del contenuto dei messaggi, ricevuti sugli *account* dei due *ex* collaboratori, da parte di terzi non autorizzati, per un periodo temporale che il Garante ha giudicato eccessivo e non commisurato alle effettive esigenze organizzative, in considerazione del fatto che l'agenzia aveva dichiarato, nel corso dell'istruttoria, che la distribuzione del portafoglio clienti, inizialmente assegnato ai due segnalanti, si era conclusa in un arco temporale di 30 giorni. Per tali motivi, il Garante ha ritenuto che la condotta dell'agenzia era stata posta in essere in violazione dei principi di liceità e di limitazione della conservazione di cui all'art. 5, par. 1, lett. a) ed e), del RGPD.

Con il provvedimento in esame, il Garante ha avuto modo di ribadire alcuni principi fondamentali che regolano, in generale, la gestione degli *account* di posta

elettronica aziendale, sia con riferimento alla conservazione della corrispondenza che transita sugli *account* aziendali di tipo individualizzato sia con riferimento alla reperibilità delle *e-mail* per mere finalità di continuità dell'attività aziendale.

Rispetto a tali questioni, l'istruttoria svolta ha permesso di accertare che l'agenzia, nei documenti informativi predisposti per i propri dipendenti e collaboratori, aveva previsto una conservazione sistematica senza limiti temporali dei *log* di accesso a internet e alla posta elettronica, nonché del contenuto della posta elettronica "e di altre risorse informatiche" assegnata agli *ex* collaboratori, giustificandola con l'esigenza di assicurare un regolare svolgimento dell'attività lavorativa. Pertanto, con riferimento al caso di specie, è stata dichiarata l'illiceità della condotta posta in essere per violazione dei principi di liceità, di minimizzazione dei dati, di limitazione della conservazione, ed è stato prescritto di conformare i trattamenti alle disposizioni e ai principi in materia di protezione dei dati personali. È stata inoltre disposta una sanzione amministrativa pecuniaria (provv. 22 giugno 2023, n. 263, doc. web n. 9920814).

Anche in relazione a un reclamo presentato da una *ex* dipendente di un fondo pensione l'Autorità aveva avviato un'istruttoria al termine della quale è emerso che il titolare del trattamento aveva tenuto una condotta non conforme alla disciplina di protezione dei dati con riferimento al trattamento dell'*account* di posta elettronica aziendale individualizzato assegnato alla reclamante nell'ambito del rapporto di lavoro. In particolare, è stato accertato che il fondo pensione, dopo la cessazione del rapporto di lavoro con la reclamante, per un periodo di tempo significativo, aveva attivato un sistema di inoltramento automatico a un *account* condiviso delle comunicazioni elettroniche pervenute sull'*account* assegnato alla reclamante, in tal modo avendo contezza del contenuto delle comunicazioni. Ciò è stato confermato, oltre che dalle dichiarazioni del fondo stesso, anche dalla selezione di alcune conversazioni ritenute di interesse personale per la reclamante trasmesse dal fondo a quest'ultima su diverso indirizzo di posta elettronica. Il fondo, per un periodo piuttosto ampio, aveva avuto la piena operatività sull'*account* individualizzato assegnato alla reclamante nonché l'effettiva possibilità di gestirlo senza alcuna limitazione, attivando un sistema di inoltramento delle comunicazioni in entrata sul medesimo *account* ad un suo diverso indirizzo al quale potevano accedere una molteplicità di soggetti.

Tale condotta è stata ritenuta in violazione della disciplina di protezione dei dati personali, in particolare dei principi di liceità, di minimizzazione e di limitazione della conservazione di cui all'art. 5, par. 1, lett. a), c) ed e), del RGPD.

Attraverso la pratica dell'inoltramento il fondo ha acceduto, tra l'altro, successivamente alla cessazione del rapporto di lavoro, anche a dati appartenenti a categorie particolari di dati *ex* art. 9 del RGPD riferiti alla reclamante - e a terzi - (in particolare, dati relativi alla salute) in assenza di un idoneo criterio di legittimazione ed in violazione dell'art. 9 del RGPD. Non è risultato, infatti, che la reclamante abbia fornito, dopo la cessazione del rapporto di lavoro, alcun consenso ai sensi dell'art. 9, par. 2, lett. a), del RGPD al trattamento, da parte del fondo, di dati relativi alla salute. È stato rilevato altresì che la condotta del fondo è stata posta in essere in assenza di idonea informativa in merito al controllo che il datore di lavoro avrebbe effettuato, successivamente alla cessazione del rapporto di lavoro, sugli strumenti elettronici assegnati alla reclamante.

Il Garante, in proposito, ha rammentato che il titolare deve regolamentare come verranno effettuati i trattamenti conformemente alla disciplina di protezione dei dati, prima che gli stessi vengano posti in essere, esplicitando ciò in documenti idonei di informativa. Inoltre, il contenuto dell'informativa deve essere conforme alla disciplina di protezione dei dati in quanto non è sufficiente informare l'interessato delle caratteristiche essenziali del trattamento, ma è anche essenziale

13

13

che le informazioni fornite delineino operazioni di trattamento di per sé lecite. Il Garante ha pertanto ritenuto la condotta tenuta dal fondo in contrasto con l'art. 13 del RGPD (corollario del principio di trasparenza di cui all'art. 5, par. 1, lett. a), dello stesso RGPD) e con il principio generale di correttezza (v. art. 5, par. 1, lett. a), del RGPD) ed è ha disposto l'applicazione di una sanzione amministrativa pecuniaria (art. 58, par. 2, lett. i), del RGPD) (provv. 21 dicembre 2023, n. 602, doc. web n. 9978536).

Nel settore assicurativo, si segnala, inoltre, un provvedimento di ammonimento nei confronti di una compagnia di assicurazioni per il trattamento illecito dei dati di un dipendente (uso e conservazione di *e-mail* aziendale) a seguito della violazione degli artt. 5, par. 1, lett. a) c) e) ed f); 12 e 13 del RGPD (provv. 31 agosto 2023, n. 464, doc. web n. 9942133); nello specifico, considerati la durata limitata della violazione, il coinvolgimento di un solo interessato nonché l'avvenuta cancellazione dell'*account* di posta elettronica richiesta dall'interessato, il caso è stato qualificato come "violazione minore" (ai sensi del cons. 148 del RGPD).

13.2. *Esercizio dei diritti*

Anche nell'anno di riferimento è stata significativa la casistica relativa all'omesso o inadeguato riscontro alle istanze di esercizio dei diritti presentate in relazione a trattamenti effettuati nel corso del rapporto di lavoro.

Il Garante, nel ribadire i propri consolidati orientamenti in materia, ha più volte richiamato le *Guidelines 01/2022 on data subject rights - Right of access*, 2.0., adottate dal CEPD il 28 marzo 2023.

In particolare, l'Autorità ha ribadito che in capo al titolare del trattamento sussiste l'obbligo di fornire riscontro alle istanze di esercizio dei diritti presentate dall'interessato fornendo le informazioni richieste entro il termine indicato dall'art. 12, par. 3, del RGPD o, qualora non possa ottemperare alla richiesta, informando l'interessato senza ritardo e comunque entro un mese dall'istanza in merito ai motivi dell'inottemperanza e alla possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale (art. 12, par. 4, del RGPD).

Inoltre, è stato rammentato che il diritto dell'interessato di accedere alle informazioni previste dall'art. 15 del RGPD non può ritenersi soddisfatto per il solo fatto di aver fornito le informazioni previste dagli artt. 13 e 14 del RGPD, in quanto tale diritto e il cd. diritto di informativa, seppur posizioni giuridiche correlate, costituiscono diritti sanciti da distinte disposizioni dell'ordinamento, rispondenti ad esigenze di tutela e garanzia dell'interessato non completamente sovrapponibili.

A seguito di un reclamo presentato nei confronti di una società, l'Autorità ha accertato che la medesima non aveva fornito idoneo riscontro a un'istanza di accesso e di cancellazione con riguardo ai dati acquisiti da un sistema di videosorveglianza presso un condominio. In particolare, la società titolare del trattamento è stata ammonita per non avere rispettato quanto previsto dall'art. 12 del RGPD con riferimento agli artt. 15 e 17 del RGPD perché, a fronte di una istanza presentata tramite PEC e in assenza di evidenze della volontà dell'interessato di ricevere informazioni in proposito oralmente, non è emerso che sia stato fornito un riscontro per iscritto o con altri mezzi idonei.

Il Garante ha evidenziato che in sede di riscontro alle istanze di esercizio dei diritti il titolare deve adattare alla specifica condizione dell'interessato quanto indicato in termini necessariamente generali nell'informativa (o nel registro dei trattamenti), declinando le informazioni alla luce delle concrete operazioni di trattamento effettuate (provv. 26 gennaio 2023, n. 27, doc. web n. 9865404).

**Diritto di accesso
e diritto alla
cancellazione**

A seguito della presentazione di un reclamo nei confronti di una società poi oggetto di fusione per incorporazione, l'Autorità, visto l'art. 2504-*bis* c.c. e considerate le prescrizioni in materia di operazioni di fusione e scissione fra società adottate dall'Autorità (provv. 8 aprile 2009, doc. web n. 1609999), ha ammonito la società incorporante per non avere fornito idoneo riscontro all'istanza di accesso al documento di valutazione della reclamante. Il riscontro fornito, infatti, era privo di alcune informazioni oltre che dei dati richiesti.

Il Garante in proposito ha richiamato l'orientamento della giurisprudenza di legittimità in base al quale il diritto di accesso ai dati "non può intendersi, in senso restrittivo, come il mero diritto alla conoscenza di eventuali dati nuovi ed ulteriori rispetto a quelli già entrati nel patrimonio di conoscenza e, quindi, nella disposizione dello stesso soggetto interessato al trattamento dei propri dati, atteso che lo scopo del [diritto] è garantire, a tutela della dignità e riservatezza del soggetto interessato, la verifica *ratione temporis* dell'avvenuto inserimento, della permanenza ovvero della rimozione di dati, indipendentemente dalla circostanza che tali eventi fossero già stati portati per altra via a conoscenza dell'interessato, verifica attuata mediante l'accesso ai dati raccolti sulla propria persona in ogni e qualsiasi momento della propria vita relazionale" (Corte cass. 14 dicembre 2018, n. 32533). La richiesta del lavoratore di accedere al proprio fascicolo personale costituisce, infatti, un diritto soggettivo tutelabile in quanto tale che trae la sua fonte dal rapporto di lavoro. Secondo i giudici di legittimità il suddetto diritto deriva, ancora prima che dalla normativa in materia di protezione dei dati personali, dal "rispetto dei canoni di buona fede e correttezza che incombe sulle parti del rapporto di lavoro ai sensi degli artt. 1175 e 1375 c.c." (Corte cass. 7 aprile 2016, n. 6775). Considerato che il titolare aveva dichiarato, senza avere prodotto evidenza alcuna, di avere fornito all'interessata oralmente, durante un colloquio, alcune delle informazioni richieste con l'istanza di accesso, l'Autorità ha rammentato che l'art. 12, par. 1, del RGPD precisa che i riscontri del titolare del trattamento all'interessato devono essere forniti per iscritto o con altri mezzi, anche se del caso, con mezzi elettronici e che, solo qualora venga richiesto dall'interessato, le informazioni possono essere fornite oralmente.

Il Garante ha rammentato che l'art. 5, par. 1, lett. a), del RGPD dispone che i dati personali devono essere trattati in modo trasparente (anche qualora il trattamento venga effettuato nell'ambito del rapporto di lavoro); in tale ambito, l'obbligo di trattare i dati in modo trasparente discende anche dal principio di correttezza, cosicché il titolare del trattamento, a fronte di una specifica richiesta dell'interessato, è tenuto a adeguare informazioni anche in merito alle modalità del trattamento dei dati. Nel caso di specie tali informazioni sono state fornite in modo adeguato solo nel corso dell'istruttoria.

Anche in tale occasione è stato precisato che il diritto, riconosciuto all'interessato, di accedere alle informazioni previste dall'art. 15 del RGPD non può ritenersi soddisfatto per il solo fatto di aver fornito l'informativa di cui agli artt. 13 e 14 del RGPD. La condotta tenuta dalla società è risultata pertanto in contrasto con gli artt. 5, par. 1, lett. a) e 15 del RGPD (provv. 2 marzo 2023, n. 55, doc. web n. 9873272).

All'esito di un procedimento avviato a seguito della presentazione di alcuni reclami da parte di dipendenti di una società che avevano lamentato l'omesso riscontro a reiterate richieste di accesso ai propri dati contenuti nel sistema di rilevazione delle presenze tramite *badge*, l'Autorità ha accertato, anche attraverso ispezioni delegate al Nucleo speciale *privacy* e frodi tecnologiche della Guardia di finanza, che il titolare non aveva fornito alcun riscontro agli interessati nonostante avesse sostenuto il contrario in sede istruttoria.

In particolare, l'Autorità ha ritenuto il riscontro mediante consegna *brevi manu* dei dati oggetto delle menzionate richieste non conforme agli artt. 12 e 5, par. 2, del

**Diritto di accesso
al documento di
valutazione**

**Accesso alle timbrature
del *badge***

13

**Diritto di accesso ai dati
e termini per la notifica
delle violazioni**

RGPD posto che la comunicazione non è stata documentata ed è stata contestata dai reclamanti. Il Garante, inoltre, dopo aver ribadito che la disciplina vigente non prevede che l'istanza di esercizio dei diritti debba rivestire una particolare veste formale, ha rappresentato che il titolare è tenuto a fornire riscontro all'interessato anche nel caso in cui non ottemperi alle richieste di quest'ultimo (ad es. poiché non detiene più i dati), specificandone i motivi e informando circa la possibilità di presentare reclamo all'autorità di controllo e di proporre ricorso giurisdizionale (art. 12, par. 4, del RGPD).

Infine con il provvedimento è stato ritenuto che l'intervenuta sottoscrizione di un verbale di conciliazione, relativo alla posizione di uno dei reclamanti, avendo a oggetto profili prettamente lavoristici e non relativi alla protezione dei dati, non è idonea a determinare l'archiviazione del procedimento nei confronti della società, tenuto anche conto che il potere di accertamento attribuito al Garante non è subordinato all'iniziativa di parte (v. sul punto Cass., ord. 22 settembre 2021, n. 40635; sebbene riferita al quadro normativo antecedente alle modifiche di cui al d.lgs. n. 101/2018, i vigenti artt. 57 del RGPD e 154 del Codice regolano analogamente i poteri dell'Autorità). Nei confronti della società per le violazioni accertate è stata adottata una sanzione amministrativa pecuniaria (provv. 9 marzo 2023, n. 66, doc. web n. 9874604).

Sempre in materia di esercizio dei diritti, l'Autorità, a seguito della presentazione di dieci reclami da parte di cinquanta dipendenti, ha adottato un provvedimento con il quale ha sanzionato una società per non avere fornito alcun riscontro alle istanze di accesso ad alcuni dati tra cui quelli relativi alle buste paga. Solo a seguito dell'apertura dell'istruttoria la società aveva dato riscontro ai reclamanti dichiarando di non avere ritenuto "opportuno" rispondere alle istanze di esercizio dei diritti, considerato quanto previsto dall'art. 2-undecies, comma 1, lett. e), del Codice. Esaminata la condotta del titolare, il Garante ha disposto una sanzione amministrativa pecuniaria per la violazione degli artt. 12 e 15 del RGPD e ha inoltre ingiunto alla società di soddisfare integralmente le richieste di accesso dei reclamanti integrando quelle già fornite nel corso dell'istruttoria.

Per quanto concerne i dati che la società aveva ritenuto essere autonomamente reperibili dai reclamanti, il Garante ha ritenuto che il titolare avrebbe dovuto fornire riscontro, seppur con la mera indicazione della piattaforma sulla quale reperire i dati richiesti; ciò anche in ragione del fatto che, diversamente da quanto sostenuto dal titolare, l'ostensione dei dati richiesti non avrebbe comportato un pregiudizio effettivo e concreto all'esercizio di un diritto in sede giudiziaria. Pertanto, con riferimento a questi specifici dati non poteva, in concreto, ritenersi sussistente il presupposto di cui alla lett. e) del comma 3 dell'art. 2-undecies del Codice.

Per quanto riguarda, poi, i dati che la società aveva ritenuto di non potere fornire in quanto l'ostensione degli stessi le avrebbe comportato un pregiudizio in termini di difesa in giudizio, tale condotta è stata ritenuta in contrasto con l'art. 12, par. 4, del RGPD con riferimento all'art. 15 del RGPD, come più volte ricordato dal Garante (v. *supra*). Inoltre, in base all'art. 2-undecies del Codice l'esercizio ritardato, la limitazione o l'esclusione dell'esercizio dei diritti riconosciuti dal RGPD possono essere disposti solo per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, con comunicazione motivata e resa senza ritardo all'interessato. Si può non inviare la predetta comunicazione solo qualora la stessa "possa compromettere la finalità della limitazione". Circostanza, quest'ultima, che si è ritenuto non essere presente nel caso di specie.

È stato infine ricordato che l'ambito temporale della limitazione del diritto di accesso è circoscritto a quanto strettamente necessario ad evitare un pregiudizio all'esercizio del diritto (cfr. art. 2-undecies, comma 3, del Codice) e pertanto, una volta venute meno le ragioni del pregiudizio, nessun ostacolo può essere frapposto

all'esercizio del diritto previsto dall'art. 15 del RGPD.

L'Autorità ha altresì evidenziato che al procedimento davanti alla stessa non si applica il termine di 90 giorni di cui alla l. n. 689/1981, art. 14, ma quello specificamente individuato dal Garante, ai sensi dell'art. 154, comma 3 e dell'art. 166, comma 9 del Codice, con il reg. del Garante n. 2/2019 (provvti 22 giugno 2023, n. 264, doc. web n. 9909702 e 16 novembre 2023, n. 529, doc. web n. 9960854).

Il Garante si è occupato di due istanze di accesso a dati personali contenuti in una relazione investigativa commissionata dal datore di lavoro.

In un caso in cui l'attività istruttoria ha riguardato solo il profilo relativo all'esercizio dei diritti, e non anche quello della legittimità della raccolta effettuata dalla agenzia investigativa incaricata, il reclamante aveva lamentato di aver appreso dell'esistenza e del contenuto della relazione investigativa solo in occasione della costituzione del titolare del trattamento nel giudizio di impugnazione del licenziamento proposto dal reclamante stesso davanti alla competente autorità giudiziaria, nonostante avesse presentato più volte istanza di accesso ai dati utilizzati per elevare la contestazione disciplinare cui aveva fatto seguito il licenziamento. L'Autorità ha preliminarmente ribadito alcuni punti fermi in materia di diritto di accesso, declinandoli in relazione ai fatti oggetto di reclamo.

In primo luogo, le richieste di accesso ai propri dati formulate dal reclamante sono qualificabili come esercizio del diritto di accesso garantito dall'art. 15 del RGPD anche se tale norma non è stata espressamente richiamata nelle istanze (conformemente a quanto sul punto indicato dal CEPD, *Guidelines 01/2022 on data subject rights - Right of access*, 28 marzo 2023, 3.1.1, n. 47). Inoltre, non è conforme a quanto stabilito dal medesimo art. 15 chiedere all'interessato l'indicazione dettagliata dei documenti cui si chiede di accedere, al fine di poter fornire riscontro all'istanza di accesso.

Peraltro, nel caso di specie, la richiesta del reclamante era stata tutt'altro che generica, riferendosi espressamente a tutti i dati utilizzati per effettuare la contestazione disciplinare. Anche su questo punto sono intervenute le richiamate *Guidelines 01/2022 on data subject rights - Right of access*, affermando che l'istanza di accesso ai dati personali ha, di regola, ad oggetto tutti i dati detenuti dal titolare del trattamento e che quest'ultimo può avere dubbi sul contenuto della richiesta solo se questa sia stata formulata in termini estremamente generici (si veda in particolare par. 2.3.1, n. 35). Il Regolamento, inoltre, non impone agli interessati alcun requisito in merito alla forma della richiesta di accesso ai dati personali (si vedano sempre le *Guidelines 01/2022 on data subject rights - Right of access*, par. 3.1.2, n. 52).

Ciò posto, il Garante ha stabilito che l'art. 15 del RGPD, nel definire l'oggetto del diritto di accesso, ricomprende anche le "categorie di dati personali" nonché, nel caso in cui i dati non siano raccolti presso l'interessato tutte "le informazioni disponibili sulla loro origine" (v. art. 15, par. 1, lett. b) e g), del RGPD).

Pertanto la società, in riscontro alla richiesta di accesso, tenuto conto dell'origine dei dati utilizzati per elevare la contestazione disciplinare, avrebbe dovuto fornire tutti i dati raccolti con la relazione investigativa, considerata anche la presenza, all'interno della stessa, di categorie di dati relative al reclamante (fotografie, una rilevazione GPS, descrizioni di luoghi, persone e situazioni) che non sono state trasferite nella contestazione disciplinare.

Infine, qualora il datore di lavoro avesse ritenuto che, nel caso specifico, ricorresse una delle concrete condizioni previste dall'art. 2-*undecies* del Codice, avrebbe dovuto comunicarlo all'interessato con motivato riscontro, come stabilito anche, in termini generali, dall'art. 12, par. 4, del RGPD. La condotta del titolare del trattamento è stata inoltre ritenuta non conforme al principio generale di correttezza del trattamento (art. 5, par. 1, lett. a), del RGPD).

13

Accesso a relazione
investigativa

13

Per le violazioni riscontrate alla società è stata applicata una sanzione amministrativa pecuniaria (provv. 6 luglio 2023, n. 290, doc. web n. 9927300).

Con un diverso provvedimento, l'Autorità ha accertato l'illiceità della condotta di una società che aveva omesso di fornire riscontro ad una dettagliata richiesta di accesso ai dati personali utilizzati per il licenziamento di una dipendente.

Solo dopo la presentazione del reclamo al Garante, nel corso del procedimento avviato sul caso e all'esito dell'accertamento ispettivo delegato al Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza a fronte della assenza di risposta alle richieste dell'Autorità, il titolare del trattamento aveva inviato alla reclamante un riscontro e aveva trasmesso la relazione dell'agenzia investigativa utilizzata per la contestazione disciplinare e il successivo licenziamento.

In particolare, è stata ritenuta in contrasto con gli artt. 15 e 12 del RGPD l'assenza di alcuna risposta alla richiesta di esercizio del diritto, allo scopo, secondo quanto dichiarato dal titolare, di evitare un pregiudizio per il diritto di difesa della società in caso di impugnazione del licenziamento dell'interessata. In base alle norme richiamate, infatti, il titolare del trattamento avrebbe dovuto in ogni caso fornire alla reclamante un riscontro indicando i motivi dell'inottemperanza e la possibilità di proporre reclamo al Garante o ricorso all'autorità giudiziaria ordinaria (art. 12, par. 4, del RGPD; art. 2-*undecies* del Codice). Con riguardo all'omessa risposta da parte del titolare del trattamento sia all'istanza di esercizio del diritto di accesso che alle richieste dell'Autorità, con il provvedimento è stato richiamato l'orientamento della Corte di cassazione secondo cui la responsabilità per la mancata lettura di una comunicazione/notifica ricevuta a mezzo PEC è da attribuire all'imprenditore, se conseguente a una sua carenza relativamente alla manutenzione e al controllo della casella di posta (v. Corte cass. n. 13917/2016).

Nel caso specifico, poi, è stata anche accertata la violazione delle regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, d.lgs. n. 101/2018, laddove tali regole stabiliscono che l'atto di incarico deve essere conferito per iscritto e menzionare in maniera specifica il diritto che si intende esercitare in sede giudiziaria, ovvero il procedimento penale al quale l'investigazione è collegata, nonché i principali elementi di fatto che giustificano l'investigazione e il termine ragionevole entro cui questa deve essere conclusa (art. 8, regole deontologiche cit.). La società aveva infatti conferito in forma orale a un'agenzia investigativa l'incarico di svolgere investigazioni difensive nei confronti della dipendente, violando dunque una delle condizioni di liceità del trattamento (v. art. 2-*quater*, comma 4, del Codice). Alla società è stata applicata una sanzione amministrativa pecuniaria (provv. 6 luglio 2023, n. 292, doc. web n. 9924466).

L'Autorità si è occupata di un reclamo concernente un generico riscontro fornito dal titolare del trattamento a un'istanza di esercizio del diritto di accesso ai dati personali del reclamante trattati nell'ambito di un rapporto di lavoro non più in essere e di cancellazione degli stessi.

L'Autorità ha ribadito che l'istanza di accesso ai dati personali può essere presentata anche in relazione a dati trattati in base ad un obbligo di legge oppure a dati posti già nella disponibilità dell'interessato o a questi già consegnati. Lo scopo del diritto di accesso è infatti quello di consentire all'interessato di verificare (anche a "intervalli ragionevoli" di tempo: v. cons. 63 del RGPD) che sia in corso o meno un determinato trattamento e valutarne la liceità e correttezza (tenuto anche conto che modalità e novero dei dati trattati possono cambiare nel tempo). L'art. 15 del RGPD non prevede alcuna limitazione in ordine alle informazioni riferite all'interessato che possono essere oggetto di accesso e lo stesso RGPD prevede espressamente la possibilità che l'interessato presenti più richieste di accesso (salva la possibilità per il titolare

Istanza di accesso e cancellazione di dati dopo la cessazione del rapporto di lavoro

del trattamento, in caso di richieste “eccessive, in particolare per il loro carattere ripetitivo”, di addebitare un contributo spese ragionevole; art. 12, par. 5, del RGPD).

Per quanto riguarda la richiesta di cancellazione dei dati trattati a seguito della cessazione del rapporto di lavoro con il reclamante, il Garante ha stabilito che la società avrebbe dovuto fornire comunque una risposta specifica, seppur precisando che alcuni dati personali riferiti al lavoratore devono essere conservati dal datore di lavoro in base a norme di settore. In conformità all’art. 12, par. 4, del RGPD, il titolare pertanto avrebbe dovuto informare l’interessato circa i motivi per i quali non dava corso all’istanza, o forniva un riscontro parziale, e i rimedi previsti dall’ordinamento avverso tale decisione.

Il titolare aveva fornito riscontro all’interessato nel corso del procedimento. Tuttavia il Garante ha ritenuto che la risposta all’istanza di accesso non fosse ancora idonea a soddisfare quanto previsto dalla disciplina in materia di protezione dei dati personali. Alla società è stato ingiunto di soddisfare la richiesta di esercizio del diritto di accesso da parte dell’interessato ai dati ancora detenuti ed è stata applicata una sanzione amministrativa pecuniaria (provv. 18 luglio 2023, n. 318, doc. web n. 9929053).

Con il provvedimento in esame, il Garante è tornato a pronunciarsi in materia di diritto di accesso ai dati trattati nell’ambito del rapporto di lavoro, in particolare ai dati relativi ai trattamenti effettuati dal datore di lavoro per calcolare i tempi della prestazione lavorativa e i rimborsi chilometrici.

In tale occasione è stato osservato come non possa considerarsi sufficiente, per conformarsi agli artt. 12 e 15 del RGPD, fornire un riscontro se quest’ultimo risulta avere un contenuto non adeguato. Nel caso si specie è stato accertato che il titolare del trattamento, pur avendo fornito un riscontro, non aveva fornito completa risposta alle analitiche e chiare istanze di esercizio dei diritti. La società, in particolare, si era limitata a indicare le modalità e le finalità del trattamento senza però comunicare gli specifici dati relativi ai reclamanti (trattati, tra l’altro, attraverso il terminale loro fornito nell’ambito della prestazione lavorativa) né le informazioni richieste dai reclamanti in proposito al predetto trattamento.

Considerato che la società, in qualità di titolare, aveva trattato, tra l’altro, dati relativi alla geolocalizzazione degli *smartphone* forniti ai reclamanti per lo svolgimento della prestazione lavorativa e, quindi, dati dei reclamanti (in particolare, quantomeno, la posizione geografica degli stessi nel momento della lettura dei contatori di acqua, gas e luce alla quale erano preposti), essa avrebbe dovuto fornire ai medesimi i dati relativi alle specifiche rilevazioni/coordinate geografiche effettuate con il GPS dello *smartphone* attivato dai lavoratori in prossimità del contatore per la lettura del medesimo.

Il Garante, a fronte della condotta non conforme alla disciplina di protezione dei dati, ha disposto una sanzione amministrativa pecuniaria e ha ingiunto alla società di soddisfare le richieste di accesso dei reclamanti, fornendo agli stessi i dati a loro relativi nonché le informazioni espressamente richieste nelle istanze al netto di quanto già limitatamente indicato (provv. 14 settembre 2023, n. 403, doc. web n. 9936174).

A seguito della presentazione di un reclamo, l’Autorità ha accertato la non conformità alla disciplina di protezione dei dati della condotta tenuta da una società nei confronti di istanze di accesso agli attestati di formazione formulate da un *ex* dipendente. In particolare, è stata accertata la violazione degli artt. 12 e 15 del RGPD per non avere il titolare del trattamento fornito idoneo riscontro a una prima istanza di accesso, non avendo chiarito, conformemente a quanto previsto dall’art. 12, par. 4, del RGPD, il motivo ostativo all’accesso agli attestati di formazione né indicato il diritto di proporre reclamo al Garante o ricorso giurisdizionale a fronte del diniego

13

**Diritto di accesso ai dati
di geolocalizzazione**

**Diritto di accesso agli
attestati di formazione
professionale**

13

**Omesso riscontro
all'istanza di esercizio
dei diritti**

manifestato. È stato accertato, inoltre, che neanche a seguito di una seconda istanza di accesso il titolare aveva fornito un idoneo riscontro all'interessato. Considerato inoltre che alla richiesta di informazioni presentata dall'Autorità la società non aveva fornito riscontro alcuno, tanto che è stato necessario chiedere l'intervento del Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza, è stata accertata anche la violazione dell'art. 157 del Codice.

A fronte delle violazioni riscontrate, il Garante ha disposto nei confronti del titolare del trattamento una sanzione amministrativa pecuniaria (provv. 12 ottobre 2023, n. 475, doc. web n. 9965598).

In un caso particolare, il titolare del trattamento aveva motivato il mancato riscontro a un'istanza di esercizio dei diritti proveniente da un proprio dipendente a causa dell'ampiezza e genericità delle informazioni richieste.

Nel caso specifico, il Garante ha rilevato che, a fronte della dichiarata difficoltà di evadere la richiesta di esercizio dei diritti nei termini previsti dalla normativa, la società non si era avvalsa della facoltà riconosciuta dal RGPD di rivolgere all'interessato le opportune specificazioni, né aveva informato l'istante dei motivi del ritardo, con ciò venendo meno al rispetto della disposizione di cui all'art. 12, par. 3, del RGPD (come ribadito anche nelle *Guidelines 01/2022 on data subject rights - Right of access*, 2.0., cit.). Per le violazioni riscontrate è stata disposta una sanzione amministrativa pecuniaria (provv. 16 novembre 2023, n. 530, doc. web n. 9960875, in senso analogo anche provv. 1° giugno 2023, n. 230, doc. web n. 9917820).

Tra le altre motivazioni addotte dai titolari del trattamento per giustificare il mancato riscontro alle istanze di esercizio dei diritti, ricorre spesso quella relativa alle difficoltà di tipo organizzativo e di coordinamento tra varie unità organizzative.

Pertanto, in un altro caso, il Garante ha precisato che tali argomentazioni non possono assurgere a valido motivo di esclusione della responsabilità, sulla base di una consolidata giurisprudenza che, in tema di violazioni amministrative, stabilisce che la buona fede esclude la responsabilità laddove “il trasgressore riesca a dimostrare di aver fatto tutto il possibile ai fini dell'osservanza della norma di legge” (tra tutte v. Cass. sez. II civ. n. 10841/2008).

In senso del tutto analogo, anche la disposizione contenuta nell'art. 24 del RGPD obbliga il titolare del trattamento a mettere “in atto misure tecniche e organizzative adeguate per garantire (...) che il trattamento è effettuato conformemente al Regolamento”. Per le violazioni riscontrate è stata disposta una sanzione amministrativa pecuniaria (provv. 9 marzo 2023, n. 67, doc. web n. 9877728).

13.3. *Trattamento di dati biometrici*

Il Garante, a seguito della presentazione di un reclamo, ha accertato che una società aveva installato un sistema di rilevazione delle presenze basato su tecnologie biometriche. In particolare, nel corso dell'istruttoria, è stato accertato che il sistema, basato sulla rilevazione delle impronte digitali, aveva coinvolto 13 dipendenti ed era stato implementato presso due sedi operative da circa 2 anni. Tale sistema era stato, nel corso del procedimento, rimosso e sostituito con un sistema di rilevazione basato su *badge*.

In linea con un orientamento ormai consolidato, il Garante ha ribadito la disciplina generale applicabile al trattamento di dati biometrici, da seguire sia in fase di *cd. enrolment*, consistente nell'acquisizione delle caratteristiche biometriche (nella specie impronte digitali) dell'interessato (v. punti 6.1 e 6.2 dell'all. A, provv. 12 novembre 2014, n. 513, doc. web n. 3556992), sia nella fase di riconoscimento biometrico, all'atto della rilevazione delle presenze (v. anche punto 6.3 dell'all. A al cit. provv.).

13

Il Garante ha ricordato, inoltre, che il trattamento di dati biometrici è consentito esclusivamente qualora ricorra una delle condizioni indicate dall'art. 9, par. 2, del RGPD e, con riguardo ai trattamenti effettuati in ambito lavorativo, solo quando il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, ove previsto dal diritto nazionale o unionale ovvero sulla base di un contratto collettivo, e in ogni caso in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. b), del RGPD; v. pure, art. 88, par. 1 e cons. 51-53 del RGPD).

Ai fini della valutazione del caso oggetto di reclamo, il Garante ha quindi tenuto conto della previsione normativa di cui all'art. 9, par. 2, lett. b), del RGPD, che stabilisce le condizioni in base alle quali il trattamento dei dati biometrici può essere lecitamente effettuato in ambito lavorativo, nonché di quanto previsto dall'art. 2-septies del Codice in base al quale tale trattamento deve avvenire "in conformità alle misure di garanzia disposte dal Garante" in relazione a ciascuna categoria di dati.

Pertanto, con riferimento al caso esaminato, il Garante ha accertato l'illiceità del trattamento effettuato, in quanto l'utilizzo del dato biometrico per finalità di ordinaria gestione del rapporto di lavoro (qual è l'attività di rilevazione delle presenze) non appare conforme ai principi di minimizzazione e proporzionalità del trattamento, nonché di liceità, correttezza e trasparenza (art. 5 del RGPD). Tra l'altro, l'Autorità ha ritenuto del tutto inidonea l'informativa predisposta dalla società, non avendo quest'ultima informato i dipendenti delle caratteristiche essenziali del dispositivo biometrico come richiesto dall'art. 13 del RGPD. Per le violazioni riscontrate è stata disposta una sanzione amministrativa pecuniaria (provv. 14 settembre 2023, n. 404, doc. web n. 9940565).

13.4. *Trattamento di dati sanitari*

A seguito della presentazione di un reclamo, è stato accertato che una società aveva tenuto una condotta non conforme alla disciplina di protezione dei dati personali durante la procedura di selezione del reclamante nell'ambito di tirocini formativi finalizzati all'assunzione ai sensi della l. n. 68/1999. In particolare la società aveva trattato in qualità di titolare del trattamento dati sensibili (oggi dati appartenenti a categorie particolari) del reclamante in assenza di idonea base giuridica. La società, infatti, dopo avere ricevuto il nominativo del reclamante dall'ufficio di collocamento competente e dopo avere invitato lo stesso a colloquio con la referente commerciale del gruppo societario di cui fa parte la società, aveva ritenuto fosse necessaria una "pre-analisi" della documentazione medica da parte del medico competente per valutare l'inserimento effettivo del reclamante. Pertanto aveva chiesto al reclamante di inviare la documentazione relativa al foglio visita/relazione conclusiva predisposta dalla commissione medica integrata e, ricevuta la comunicazione contenente il *link* dal quale poter scaricare i documenti medici, aveva provveduto a inoltrare al medico competente la predetta comunicazione. Con ciò aveva dimostrato di avere la materiale disponibilità dei documenti contenenti dati particolari del reclamante.

È stato rilevato, in proposito, che la violazione era avvenuta in una data antecedente alla piena efficacia del RGPD, ma che le norme interessate dalla violazione, vigenti all'epoca del fatto, erano identiche, quanto a contenuto, a quelle oggi previste dal RGPD. Pertanto, con riferimento alla condotta descritta è risultato accertato che la Società aveva violato gli artt. 11 e 26 del Codice, nella versione precedente alle modifiche apportate dal d.lgs. n. 101/2018, disposizioni che corrispondono all'art. 9 del RGPD il quale, a sua volta, costituisce espressione del principio di liceità del

13

trattamento (art. 5, par. 1, lett. a), del RGPD). L'illiceità del trattamento è stata rilevata anche in relazione a specifiche discipline di settore applicabili, in particolare il d.lgs. n. 81/2008 e l. n. 68/1999.

L'Autorità ha altresì accertato che il trattamento dei dati predetti da parte della società era stato effettuato senza fornire un'idonea informativa all'interessato, ai sensi dell'art. 13 del Codice, nella versione precedente alle modifiche apportate dal d.lgs. n. 101/2018, ora riprodotto dall'art. 13 del RGPD, – che costituisce diretta espressione del principio di trasparenza (v. art. 5, par. 1, lett. a), del RGPD); in particolare non erano stati comunicati chiaramente le finalità del trattamento né i soggetti destinatari dei dati raccolti.

Considerato che l'obbligo di informare un candidato all'assunzione ai sensi della l. n. 68/1999 è espressione del principio generale di correttezza, è risultato violato anche il principio di correttezza, previsto dall'art. 11, comma 1, lett. a), del Codice, nella versione precedente alle modifiche apportate con il d.lgs. n. 101/2018, oggi corrispondente all'art. 5, par. 1, lett. a), del RGPD.

Durante l'istruttoria, è stata accertata la contrarietà della condotta tenuta dalla società con riferimento alle istanze di esercizio del diritto di accesso (volte a conoscere il nominativo del medico competente e il motivo alla base del parere espresso da questi in merito alla idoneità) e quindi la violazione degli artt. 12 e 15 del RGPD, considerato che la condotta, cominciata prima della piena efficacia del Regolamento, è proseguita anche successivamente.

È risultato violato anche il principio di limitazione della finalità (fissato nell'art. 11, comma 1, lett. b), del Codice, nella versione antecedente alle modifiche apportate dal d.lgs. n. 101/2018, cui oggi corrisponde l'art. 5, par. 1, lett. b), del RGPD) poiché, dopo avere chiesto al reclamante la documentazione medica per inviarla al medico competente per la visita preassuntiva, la società aveva comunicato i predetti dati al medico competente per l'elaborazione di un parere preliminare.

A fronte delle violazioni riscontrate il Garante ha disposto una sanzione amministrativa pecuniaria (provv. 8 giugno 2023, n. 245, doc. web n. 9924438).

In sede istruttoria l'Autorità ha ritenuto di ammonire l'allora medico competente della società per avere trattato i dati sensibili del reclamante (tra gli altri, i dati sanitari contenuti nella relazione della commissione medica per l'accertamento dell'invalidità, anche nella versione priva di *omissis*) in qualità di titolare del trattamento senza fornire la necessaria informativa all'interessato.

In proposito è stato richiamato l'orientamento dell'Autorità in merito alla posizione di autonomo titolare del medico competente relativamente ai trattamenti volti a valutare l'idoneità alla mansione del lavoratore (si veda per es. provv. 27 aprile 2016, n. 194, doc. web n. 5149198; ma v. pure, con particolare riguardo alla tenuta delle cartelle sanitarie e di rischio da parte del medico competente e alla diversa attività di tenuta e aggiornamento dei fascicoli personali dei dipendenti da parte del datore di lavoro, le linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro, doc. web n. 1364939) (provv. 31 agosto 2023, n. 522, doc. web n. 9965614).

13.5. Videosorveglianza nei luoghi di lavoro del settore privato

Nell'anno di riferimento, a seguito della presentazione di una segnalazione da parte di un sindacato e della connessa attività di accertamento ispettivo *in loco*, il Garante ha adottato una sanzione amministrativa pecuniaria nei confronti di una società per l'accertata violazione degli artt. 5, par. 1, lett. a), 88 del RGPD e art. 114 del Codice.

In particolare, dall'istruttoria è emerso che la società aveva installato ed utilizzato sistemi di videosorveglianza presso una molteplicità di propri punti vendita, idonei a riprendere i lavoratori durante l'attività lavorativa, in assenza di accordo con le rappresentanze sindacali o di autorizzazione rilasciata dall'Ispettorato del lavoro ex art. 4 della l. n. 300/1970.

L'attivazione della procedura di garanzia di cui all'art. 4 citato, infatti, era avvenuta solo dopo un significativo periodo di tempo dalla installazione e attivazione dei sistemi di videosorveglianza. Conseguentemente, i trattamenti sono risultati illeciti, in alcuni casi, fino alla disattivazione delle telecamere a seguito dell'intervento dell'Ispettorato del lavoro e, per gli altri, fino alla stipulazione dell'accordo o al rilascio dell'autorizzazione. La predetta procedura di garanzia, come più volte sottolineato anche dalla giurisprudenza di legittimità, "tutela interessi di carattere collettivo e superindividuale", per cui la condotta del datore di lavoro che non la attivi lederà gli interessi collettivi a presidio dei quali tale procedura è posta (v., tra le altre, Cass., sez. III pen., 17 dicembre 2019, n. 50919). L'Autorità ha sottolineato, in particolare, che l'inderogabilità della citata procedura risponde anche alla situazione di sproporzione esistente tra la posizione datoriale e quella dei lavoratori.

Considerato che nel caso di specie i sistemi di videosorveglianza erano stati posizionati in modo da riprendere zone ove necessariamente transitavano i dipendenti per lo svolgimento dell'attività lavorativa, o anche per recarsi all'interno di aree per lo svolgimento dell'attività lavorativa, il Garante ha ricordato che anche le aree nelle quali transitano o sostano – talora continuativamente – i dipendenti (ad es. accessi alla struttura e ai garage, zone di carico/scarico merci, ingressi carrai e pedonali), qualora sottoposte a videosorveglianza, sono soggette alla piena applicazione della disciplina in materia di protezione dei dati personali (v., tra gli altri, provv.ti 16 settembre 2021, n. 331, doc. web n. 9719768; 30 luglio 2015, n. 455, doc. web n. 4261028; 4 luglio 2013, n. 334, doc. web n. 2577203; 18 aprile 2013, n. 200, doc. web n. 2483269; 9 febbraio 2012, n. 56, doc. web n. 188699; 17 novembre 2011, n. 434, doc. web n. 1859558; 26 febbraio 2009, doc. web n. 1601522). Ciò è peraltro conforme a quanto stabilito dalla giurisprudenza di legittimità (v. Cass. 6 marzo 1986, n. 1490; v. anche, con riferimento a strumento diverso dalla videosorveglianza, Cass. 13 marzo 2007, n. 15892).

È stato ricordato, inoltre, che i poteri che l'ordinamento riconosce al Garante ai sensi dell'art. 114 del Codice si aggiungono (e non sostituiscono né vengono meno rispetto) ai poteri propri dell'Ispettorato del lavoro. A seguito dell'accertamento ispettivo, è emerso che presso un punto vendita le immagini raccolte attraverso una telecamera del sistema di videosorveglianza erano state registrate e conservate per un tempo superiore al termine stabilito nell'accordo stipulato ai sensi dell'art. 4 della l. n. 300/1970. Peraltro, è risultato che presso un diverso punto vendita le registrazioni delle immagini con il sistema di videosorveglianza erano state effettuate in orario lavorativo anche se nelle relative autorizzazioni dell'Ispettorato del lavoro era stato precisato che le telecamere dovessero rimanere spente durante l'orario di apertura della sede operativa ai clienti.

Considerato che le illecità riscontrate erano cessate nel corso dell'istruttoria, nei confronti della società è stata adottata solo una sanzione amministrativa pecuniaria (provv. 2 marzo 2023, n. 58, doc. web n. 9880398).

A seguito della presentazione di due reclami nei confronti, tra l'altro, di una fondazione, con i quali era stata lamentata la violazione della disciplina di protezione dei dati rispettivamente con riferimento al diritto di accesso e al principio di liceità, l'Autorità ha ammonito la predetta fondazione quale titolare del trattamento per avere fornito un inidoneo riscontro (in quanto generico) all'istanza di accesso presentata dal reclamante in violazione degli artt. 12 e 15 del RGPD, nonché per

13

Diritto di accesso a un video e trasmissione dello stesso a un terzo

13

Utilizzo di
videosorveglianza
associata a rilevazione
biometrica e
geolocalizzazione

avere trasmesso a un soggetto terzo il video ritraente il reclamante, effettuato con il proprio sistema di videosorveglianza, in assenza di idonea condizione di liceità del trattamento, quindi, in violazione dell'art. 6 del RGPD (provv. 30 novembre 2023, n. 559, doc. web n. 9970864).

A seguito di un accertamento ispettivo effettuato dal Nucleo speciale tutela *privacy* e frodi tecnologiche della Guardia di finanza successivo a segnalazione, il Garante ha accertato l'illiceità dei trattamenti effettuati da una società tramite un sistema di videosorveglianza e un sistema di allarme, installati presso la sede legale, attivabili e disattivabili con le impronte digitali nonché un sistema di rilevazione della posizione geografica dei dipendenti funzionante tramite applicativo installato sui telefoni cellulari utilizzati dagli stessi.

Per quanto riguarda il sistema di allarme funzionante attraverso il trattamento di dati biometrici, è stato rilevato che la società aveva trattato, fino alla disinstallazione, dati biometrici (impronte digitali) anche di propri dipendenti in assenza di una idonea base giuridica, considerato che, come già chiarito dall'Autorità, c'è trattamento di dati biometrici sia nella fase di registrazione (cd. *enrolment*) sia nella fase di riconoscimento biometrico. In base alla disciplina di protezione dei dati personali, infatti, il trattamento di dati biometrici è consentito esclusivamente qualora ricorra una delle condizioni indicate dall'art. 9, par. 2, del RGPD e, con riguardo ai trattamenti effettuati in ambito lavorativo, solo quando il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, e ove previsto dal diritto nazionale o unionale ovvero sulla base di un contratto collettivo, e in ogni caso in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. b), del RGPD; v. pure, art. 88, par. 1 e cons. 51-53 del RGPD). La fattispecie oggetto di esame non rientrava nella presente ipotesi di trattamento di dati biometrici lecito.

Con riferimento al trattamento dei dati biometrici, è stata accertata la violazione dell'art. 13 del RGPD in quanto il trattamento era stato posto in essere senza fornire una idonea informativa agli interessati.

Con riguardo al sistema di localizzazione geografica, la condotta tenuta dalla società è stata ritenuta in contrasto con la disciplina di settore in materia di controlli a distanza (cfr. artt. 5, par. 1, lett. a), del RGPD in relazione agli artt. 114 del Codice e 4 l. 20 maggio 1970, n. 300, norma fatta salva dall'art. 88 del RGPD). La società aveva trattato i dati di geolocalizzazione del proprio personale tecnico senza avere attivato la procedura di garanzia prevista dall'art. 4, l. n. 300/1970, nonostante fosse risultata tracciata in modo continuativo la posizione dei lavoratori nello svolgimento dell'attività lavorativa nei periodi in cui l'applicativo installato sugli *smartphone* era risultato in uso. Oltre al dato relativo alla posizione geografica, la società aveva raccolto, tramite il sistema, anche il dato relativo all'ora e alla data della rilevazione della posizione, con riferimento a periodi molto risalenti nel tempo (2014).

È stato quindi riscontrato che il sistema utilizzato aveva violato il principio di minimizzazione dei dati, enunciato dall'art. 5, par. 1, lett. c), del RGPD, considerato che il sistema aveva raccolto non solo il dato relativo alla posizione geografica rilevato al momento della chiusura della chiamata del tecnico, ma anche la posizione geografica del lavoratore per tutto il tempo in cui l'applicativo era risultato attivo e il tecnico aveva acceduto allo stesso.

Inoltre, anche relativamente al trattamento di dati di geolocalizzazione, non era stata fornita un'adeguata informativa agli interessati, in violazione di quanto previsto dall'art. 13 del RGPD nonché dall'art. 5, par. 1, lett. a), del RGPD in quanto nell'ambito del rapporto di lavoro l'obbligo di informare il dipendente è altresì espressione del principio di correttezza.

Infine, in merito al trattamento dei dati effettuati tramite il sistema di videosorveglianza è stato accertato che dall'uso del predetto sistema poteva derivare un controllo a distanza dell'attività lavorativa: in particolare, il legale rappresentante della società, attraverso il proprio *smartphone*, poteva visionare, in diretta, quanto ripreso dalla telecamera nella postazione adibita a *reception*, quindi l'attività dei lavoratori che lavoravano e transitavano nell'area ripresa; il sistema inoltre poteva captare anche i suoni e poteva effettuare la registrazione delle immagini. Nonostante ciò, è stato riscontrato che il titolare non aveva attivato la procedura di garanzia prevista dall'art. 4 della l. n. 300/1970. Non è risultato inoltre che fosse stata fornita alcuna informativa in merito al trattamento dei dati tramite il sistema di videosorveglianza.

Il Garante ha quindi disposto il divieto del trattamento effettuato mediante il sistema di videosorveglianza, il divieto di monitoraggio continuo della posizione del lavoratore quanto al sistema di rilevamento della posizione geografica, nonché l'applicazione di una sanzione amministrativa pecuniaria (prov. 1° giugno 2023, n. 231, doc. web n. 9913830).

13

13.6. Pubblicazione di dati in internet

L'Autorità ha accertato la violazione della disciplina di protezione dei dati personali da parte di una società calcistica che, successivamente alla cessazione del rapporto di lavoro con il reclamante, aveva continuato a trattare, tramite conservazione con possibilità di consultazione, la scheda riferita allo stesso sul proprio sito web all'interno della "rosa" dei giocatori della squadra, contenente anche il dato relativo al peso corporeo (dato che nel caso di specie rientra tra i dati cd. comuni); il trattamento è risultato privo di base giuridica e, quindi, in violazione dell'art. 5, par. 1, lett. a), del RGPD (principio di liceità).

Inoltre il Garante ha ritenuto sussistente la violazione del principio di limitazione della conservazione (art. 5, par. 1, lett. e), del RGPD) considerato che la società aveva cancellato definitivamente la scheda *online* riferita al reclamante più di un anno dopo la cessazione del rapporto di lavoro e che in tale periodo di tempo la predetta scheda era rimasta consultabile. È stata, infine, stabilita la violazione dell'art. 12 del RGPD per non avere la società fornito idoneo riscontro al reclamante, a seguito della richiesta con cui questi lamentava la pubblicazione del dato relativo al peso corporeo chiedendone la cancellazione.

Per le violazioni poste in essere l'Autorità ha ammonito la società calcistica (prov. 27 aprile 2023, n. 180, doc. web n. 9910193).

13.7. Trattamento di dati mediante dispositivi tecnologici

L'Autorità ha adottato un documento di indirizzo, denominato "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", rivolto ai datori di lavoro pubblici e privati anche tenendo conto degli esiti di taluni specifici accertamenti effettuati.

È emerso, infatti, che alcuni programmi e servizi informatici di gestione della posta elettronica, commercializzati da fornitori, anche in modalità *cloud*, sono configurati in modo da raccogliere e conservare – per impostazione predefinita, in modo preventivo e generalizzato – i metadati relativi all'utilizzo degli *account* di posta elettronica dei dipendenti (ad es., giorno, ora, mittente, destinatario, oggetto e dimensione dell'*e-mail*). In alcuni casi, inoltre, i sistemi non consentono ai datori di lavoro di disabilitare la raccolta sistematica dei dati e ridurre il periodo di conservazione. Il documento di indirizzo – nel fornire ai titolari indicazioni utili a prevenire

13

trattamenti di dati in contrasto con la disciplina sulla protezione dei dati e le norme che tutelano la libertà e la dignità dei lavoratori – sollecita gli stessi a verificare che i programmi e i servizi informatici di gestione della posta elettronica in uso ai dipendenti (specialmente in caso di prodotti di mercato forniti in *cloud* o *as-a-service*) consentano di modificare le impostazioni di base, impedendo la raccolta dei metadati o limitando il loro periodo di conservazione a un massimo di 7 giorni (estensibili, in presenza di comprovate esigenze, di ulteriori 48 ore), periodo considerato congruo, sotto il profilo prettamente tecnico, per assicurare il regolare funzionamento della posta elettronica in uso al lavoratore. Nel documento si chiarisce, altresì, che ove i datori di lavoro, per esigenze organizzative e produttive o di tutela del patrimonio anche informativo del titolare (ad es. per specifiche esigenze di sicurezza dei sistemi), avessero necessità di trattare i metadati per un periodo di tempo più esteso, dovranno invece espletare le procedure di garanzia previste dallo Statuto dei lavoratori (accordo sindacale o autorizzazione dell'ispettorato del lavoro), poiché un periodo più lungo di conservazione dei metadati può comportare un indiretto controllo a distanza dell'attività del lavoratore (provv. 21 dicembre 2023, n. 642, doc. web n. 9978728).

Il Garante ha, inoltre, sanzionato due comuni per l'uso illecito delle registrazioni audio-video di una conversazione intercorsa presso un Comando di polizia locale. L'Autorità è intervenuta a seguito del reclamo di un dipendente di un comune, all'epoca vice commissario di polizia locale, che si era recato presso gli uffici del Comando di polizia locale di un altro comune e lì aveva avuto una conversazione con un agente su questioni lavorative e condizioni di lavoro. La comandante della polizia locale del comune presso cui lavorava il reclamante aveva chiesto e ottenuto dall'altro comune le registrazioni audio-video di tale conversazione, registrata dalla telecamera posta all'interno del Comando, facendo riferimento a una non meglio precisata indagine di polizia giudiziaria. Le registrazioni erano state usate per infliggere una sanzione al vice commissario, che si era poi dimesso.

L'Autorità, nel ribadire che il datore di lavoro può trattare i dati personali dei dipendenti solo se ciò è necessario per la gestione del rapporto di lavoro e per adempiere a specifici obblighi o compiti derivanti dalla disciplina di settore, ha ritenuto illeciti la trasmissione e l'uso delle registrazioni utilizzate per infliggere la sanzione disciplinare, perché privi di una idonea base giuridica. In particolare, l'Autorità ha rilevato la sproporzione dell'acquisizione dell'audio tramite dispositivi di videosorveglianza, con il rischio di carpire informazioni sulle opinioni, relazioni o vicende private dei lavoratori o su fatti comunque non rilevanti nell'ambito del rapporto di lavoro. Diverse le violazioni contestate, tra cui il mancato rispetto della disciplina di settore in materia di controlli a distanza dei lavoratori, la raccolta di dati non attinenti all'attività lavorativa, la mancanza di trasparenza nei confronti degli interessati, l'illecita comunicazione dei dati personali del reclamante da un comune all'altro, la mancata valutazione di impatto in relazione al sistema di videosorveglianza, la violazione del principio di limitazione della conservazione dei dati (provv.ti 16 novembre 2023, nn. 577 e 578, docc. web nn. 9963453 e 9963486).

13.8. *Trattamento di dati nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di illeciti (cd. whistleblowing)*

A seguito dell'entrata in vigore del d.lgs. 10 marzo 2023, n. 24 (attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali), il Garante ha reso parere favorevole sullo schema di linee guida elaborate dall'ANAC in materia, specificamente

13

relative alle procedure per la presentazione e gestione delle segnalazioni esterne, come previsto dall'art. 10, comma 1, del predetto d.lgs. n. 24/2023 (prov. 6 luglio 2023, n. 304, doc. web n. 9912239).

Le linee guida, poi adottate da ANAC in data 12 luglio 2023, sostituiscono le precedenti in merito alle quali l'Autorità si era espressa con provvedimento 4 dicembre 2019, n. 215, doc. web n. 9215763. La consultazione del Garante, fin dalla fase di elaborazione del documento, ha consentito di assicurare il necessario coordinamento tra la disciplina di settore e il quadro normativo in materia di protezione dei dati personali nell'ambito delle procedure di acquisizione e gestione delle segnalazioni di presunti illeciti, anche alla luce della particolare tutela accordata dalla disciplina di settore all'identità del segnalante e degli altri interessati e, in generale, degli specifici rischi per i diritti e le libertà degli interessati nel contesto lavorativo (art. 88 del RGPD).

Nello schema di linee guida sono stati inoltre forniti chiarimenti e principi di carattere generale che gli enti pubblici e privati potranno tenere in considerazione nell'ambito delle proprie scelte, anche sul piano organizzativo, finalizzate all'istituzione e alla gestione dei propri canali di segnalazione interni, anche in coerenza con il principio di responsabilizzazione e i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita. Lo schema di linee guida recepisce larga parte delle osservazioni e indicazioni del Garante, anche con riferimento ai profili relativi alla sicurezza del trattamento, caratterizzato da elevati rischi per i diritti e le libertà degli interessati, tra i quali si segnalano, in particolare:

- la necessità di individuare con precisione l'ambito oggettivo delle segnalazioni e di definire in maniera puntuale le ipotesi di esclusione dall'ambito di applicazione del d.lgs. n. 24/2023;

- la necessità di assicurare il coordinamento con le norme di settore, anche di derivazione europea, che regolano tempi e modi dei procedimenti di competenza delle autorità amministrative tenute a trattare la segnalazione esterna, trasmessa da ANAC, qualora la segnalazione verta su materie di competenza delle predette autorità;

- la necessità di fare ricorso a strumenti di crittografia nell'ambito dei canali interni e del canale esterno di segnalazione;

- la necessità di escludere il tracciamento dei canali di segnalazione nel caso in cui l'accesso ai canali interni e al canale esterno di segnalazione avvenga dalla rete dati interna del soggetto obbligato e sia mediato da dispositivi *firewall* o *proxy*, sia sulla piattaforma informatica che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni del segnalante;

- la necessità di garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione, fermo restando che, nel rispetto delle garanzie previste dalla disciplina di settore in materia di controlli a distanza (artt. 4, l. n. 300/1970, nonché 114 del Codice; v. anche art. 88 del RGPD), tale tracciamento può essere effettuato esclusivamente al fine di garantire la correttezza e la sicurezza del trattamento dei dati;

- la necessità che l'accesso da parte degli utenti autorizzati alla piattaforma informatica di ANAC, ai fini della gestione delle segnalazioni esterne, avvenga attraverso una procedura di autenticazione informatica a più fattori.

13.9. *La protezione di dati nell'ambito del rapporto di lavoro pubblico*

Nel corso del 2023, l'Autorità ha affrontato, sulla base di reclami, segnalazioni e richieste di parere (presentate anche da parte di RPD), numerosi temi relativi ai trattamenti di dati personali nel contesto lavorativo, effettuati da soggetti pubblici o da soggetti privati che svolgono compiti di interesse pubblico, con riguardo, in

13

particolare, ai trattamenti connessi all'impiego di strumenti tecnologici o volti ad assicurare la salute e la sicurezza sui luoghi di lavoro (anche nel contesto dell'emergenza epidemiologica da SARS-CoV-2), o comunque effettuati in occasione dell'assolvimento di obblighi derivanti da specifiche normative di settore, come la disciplina in materia di trasparenza dell'azione amministrativa e quella relativa alla tutela della riservatezza del dipendente che segnala illeciti (cd. *whistleblowing*) (cfr. 13.8).

13.9.1. Trattamento di dati per finalità di instaurazione e gestione del rapporto di lavoro

Anche con riguardo alle fasi antecedenti all'istaurazione del rapporto di lavoro (di regola nell'ambito di procedure concorsuali o selettive) e, più in generale, nell'ambito della gestione del rapporto stesso, il Garante, sulla base di istruttorie avviate a seguito di reclami presentati da dipendenti pubblici o da altri soggetti che prestano la propria attività lavorativa presso soggetti pubblici e enti che perseguono finalità di interesse pubblico, ha accertato l'illiceità di taluni trattamenti.

13.9.1.1. Trattamento di dati nell'ambito di procedure concorsuali

Alcuni reclami hanno riguardato il trattamento di dati nelle varie fasi di gestione delle procedure concorsuali e, in molti casi, la diffusione *online* di dati personali in occasione della pubblicazione di graduatorie e atti di procedure concorsuali, su cui tradizionalmente il Garante ha fornito specifiche indicazioni alle pubbliche amministrazioni in ordine alle cautele da adottare (v. le linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, adottate con provv. 2 marzo 2011, n. 88, doc. web n. 1793203, spec. II, par. 3.b, nonché le linee guida in materia di trattamento di dati personali, di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, adottate con provv. 14 giugno 2007, n. 161, doc. web n. 1417809).

In un caso, un consiglio nazionale di un ordine professionale aveva pubblicato sul proprio sito web istituzionale la graduatoria finale di una procedura concorsuale (in cui il reclamante figurava quale non vincitore), aveva poi adottato e pubblicato una deliberazione finalizzata all'adozione di un provvedimento di esclusione del reclamante in ragione della sussistenza di pregresse condanne penali (con oscuramento del nome e del cognome dello stesso e delle motivazioni sottese all'esclusione) e, infine, aveva pubblicato sul medesimo sito una versione rettificata delle predette graduatorie, priva di riferimenti al reclamante. Il Garante – nel rammentare che la disciplina di settore prevede che siano pubblicate le sole graduatorie definitive dei vincitori di concorso e non anche gli esiti delle prove intermedie o i dati personali dei concorrenti non vincitori o non ammessi (cfr. art. 15, comma 6-*bis*, d.P.R. n. 487/1994; art. 19, commi 1 e 2, d.lgs. n. 33/2013) – ha rilevato come, nel caso di specie, la pubblicazione della graduatoria intermedia, non prevista dalla legge, avesse, altresì, comportato la diffusione dell'informazione relativa all'esclusione del reclamante dalla procedura concorsuale in questione, per effetto del possibile raffronto tra le diverse versioni della graduatoria oggetto di pubblicazione, in violazione degli artt. 5, par. 1, lett. a), e 6 del RGPD, nonché 2-*ter* del Codice. A fronte di tali violazioni, il Garante ha comminato una sanzione amministrativa pecuniaria (provv. 23 marzo 2023, n. 83, doc. web n. 9888096).

In un altro caso, il Garante ha censurato l'intempestivo riscontro, da parte di un comune, all'istanza di esercizio del diritto di cancellazione dei dati, formulata da un interessato ai sensi dell'art. 17 del RGPD, con riguardo a dati relativi a condanne penali e reati acquisiti dal comune nel contesto di una procedura concorsuale a cui l'interessato aveva partecipato, e di una denuncia sporta dall'ente all'Autorità

giudiziaria penale nei confronti dello stesso. Il comune – che non aveva, peraltro, informato l'interessato, senza ritardo e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo o ricorso giurisdizionale – aveva, altresì, fornito allo stesso riscontri non pienamente conformi ai requisiti previsti dagli artt. 12, par. 3 e 4, e 17 del RGPD. Tenuto conto di tutte le specificità del caso – con particolare riguardo alla circostanza che la stessa soprintendenza archivistica e bibliotecaria territorialmente competente, nell'esprimere il proprio diniego all'autorizzazione allo scarto dei documenti amministrativi contenenti i dati personali del reclamante, si era riservata di chiedere un parere alla competente direzione generale del Ministero della cultura, stante la particolare delicatezza della questione – il Garante ha ritenuto sufficiente ammonire il titolare del trattamento (provv. 13 aprile 2023, n. 118, doc. web n. 9889553).

A seguito di un reclamo, il Garante ha poi avviato un'istruttoria nei confronti di un ateneo, che aveva pubblicato alcuni verbali, redatti nell'ambito di una procedura selettiva per un posto di ricercatore a tempo determinato, contenenti dati personali del reclamante e di altri otto partecipanti a detta procedura, ivi comprese le valutazioni e i giudizi espressi dalla commissione esaminatrice in relazione agli stessi. Ciò era avvenuto, tuttavia, in maniera non conforme alla disciplina di settore, che prevede la pubblicazione delle sole graduatorie definitive dei vincitori di concorso e non anche i verbali della procedura selettiva contenenti i dati personali dei candidati (v., in particolare, l'art. 7, d.P.R. n. 3/1957). Considerato che l'ateneo non aveva comprovato la sussistenza di un'idonea base giuridica che potesse giustificare la diffusione dei dati personali degli interessati, il Garante ha ritenuto che fossero soddisfatti i presupposti per l'adozione di un provvedimento di ammonimento (provv. 17 maggio 2023, n. 195, doc. web n. 9908484).

In un caso, nell'ambito dell'espletamento di una procedura concorsuale indetta dalla Banca d'Italia, è emerso che l'ufficio selezione e reclutamento aveva inviato agli indirizzi di posta elettronica di numerosi partecipanti al concorso un'*e-mail* con la quale si rammentava ai candidati in indirizzo la data e l'orario per lo svolgimento della prova preselettiva e il richiamo al rispetto delle misure di contenimento del contagio da Covid-19, fornendo altresì indicazioni di dettaglio per assicurare la correttezza e lo svolgimento in sicurezza della prova.

Il Garante ha al riguardo rilevato che l'invio del predetto messaggio di posta elettronica, seppure effettuato in conseguenza di un errore commesso da un dipendente, aveva determinato la messa a disposizione degli indirizzi di posta elettronica di ciascuno dei destinatari in favore degli altri che – anche tenuto conto della definizione di "terzo", contenuta nell'art. 4, par. 1, n. 10, del RGPD – non avevano titolo per conoscere i predetti recapiti. La trasmissione del messaggio con le modalità descritte aveva reso, altresì, vicendevolmente edotti tutti gli interessati, destinatari della predetta *e-mail*, della partecipazione al concorso, dando luogo a una comunicazione di dati personali in assenza di uno specifico presupposto giuridico. L'Autorità ha infatti ritenuto che non potesse configurarsi come valido, a tal fine, il consenso prestato al riguardo dal candidato all'atto della presentazione della domanda di partecipazione alla procedura selettiva in quanto, come da tempo affermato in numerosi provvedimenti, i trattamenti di dati legati allo svolgimento delle procedure concorsuali trovano la propria base giuridica nella specifica disciplina di settore che regola l'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei pubblici concorsi, e non già nel consenso degli interessati.

Tenuto conto delle circostanze del caso concreto, l'Autorità ha adottato un provvedimento di ammonimento nei confronti del titolare (provv. 23 febbraio 2023, n. 47, doc. web n. 9868646).

13

13

13.9.1.2. Trattamento di dati effettuato in occasione dell'accertamento del requisito vaccinale per i professionisti sanitari

In un caso, a seguito di sospensione dall'esercizio della professione per mancata sottoposizione alla vaccinazione contro SARS-Cov-2 da parte di un'azienda sanitaria, un dipendente aveva rappresentato di aver esercitato i diritti di cui agli artt. da 15 a 22 del RGPD nei confronti del datore di lavoro e di non avere ricevuto un idoneo riscontro. In particolare l'interessato, avendo la vicenda avuto un'ampia risonanza sulla stampa locale, aveva esercitato i menzionati diritti al fine di acquisire elementi circa la liceità e correttezza dei trattamenti dei propri dati personali effettuati dall'azienda stessa nell'ambito delle attività di accertamento del requisito vaccinale per gli esercenti le professioni sanitarie ai sensi dell'art. 4, d.l. n. 44/2021, senza tuttavia ricevere il dovuto riscontro.

Il Garante nel provvedimento in questione ha evidenziato che, sebbene l'azienda avesse dichiarato che i trattamenti di dati personali riferiti all'interessato erano stati posti in essere nel quadro delle disposizioni di settore – aspetti che non sono stati comunque oggetto di valutazione nel provvedimento – la stessa aveva dato seguito alla richiesta del reclamante ben oltre il previsto termine di un mese per un mero disguido organizzativo (provv. 14 settembre 2023, n. 419, doc. web n. 9941795).

In un altro caso un ordine provinciale dei medici chirurghi e degli odontoiatri, aveva, invece, inviato ad alcuni soggetti pubblici copia di una propria deliberazione, con la quale, ai sensi dell'art. 4, d.l. n. 44/2021, era stata disposta la sospensione del reclamante, professionista iscritto all'albo, in ragione del mancato possesso del requisito vaccinale SARS-Cov-2. Con un'ulteriore comunicazione, indirizzata al comune nel cui territorio il reclamante esercitava la propria attività professionale, il medesimo ordine aveva, inoltre, reso noto all'ente lo stato di positività al Covid-19 dell'interessato, al fine di dare impulso alla revoca dell'atto di sospensione dell'autorizzazione all'esercizio di attività sanitaria precedentemente adottato da tale comune. Il Garante, tenuto conto di tutte le specifiche circostanze emerse nel corso dell'istruttoria, ha ritenuto sufficiente ammonire il titolare del trattamento, per aver comunicato a terzi dati personali, di cui alcuni relativi allo stato di salute, in assenza di una base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del RGPD, nonché 2-ter e 2-sexies del Codice (provv. 17 maggio 2023, n. 194, doc. web n. 9910245).

13.9.1.3. Comunicazione di dati a soggetti terzi e circolazione di informazioni nei contesti lavorativi

In un caso oggetto di reclamo, un ateneo aveva comunicato dati personali del reclamante, anche relativi a reati, sia a un ispettorato territoriale del lavoro (in riscontro a un invito a comparire per un tentativo di conciliazione relativo al mancato versamento degli emolumenti asseritamente dovuti al reclamante per attività di docenza) sia all'Ispettorato per la funzione pubblica presso la Presidenza del Consiglio dei ministri (in riscontro a una richiesta dello stesso di effettuare verifiche interne sulla regolarità dell'azione amministrativa). In relazione a entrambe le comunicazioni, il Garante ha evidenziato che l'ateneo non aveva comprovato la sussistenza di un'idonea base giuridica che potesse giustificare le comunicazioni, non essendo necessario che gli enti destinatari delle due note venissero a conoscenza del procedimento penale a carico dell'interessato. Atteso che l'ateneo aveva invocato l'art. 2-octies, comma 3, lett. e), del Codice, il Garante ha ricordato che il trattamento di dati personali effettuato per finalità di tutela dei diritti deve riferirsi a contenziosi in atto o a situazioni precontenziose, e non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti. L'ateneo, al dichiarato fine di tutelare la propria reputazione, aveva, inoltre, inviato una lettera a tutti i rettori delle università italiane,

13

stigmatizzando talune condotte imputate al reclamante e dissociandosi dalle stesse, anche in questo caso senza aver, tuttavia, comprovato la sussistenza di un'idonea base giuridica. Accertata la violazione degli artt. 5, par. 1, lett. a), 6 e 10 del RGPD, nonché 2-ter e 2-octies del Codice, il Garante ha adottato un provvedimento sanzionatorio nei confronti dell'ateneo (27 aprile 2023, n. 167, doc. web n. 9897931).

In un altro caso, un comune, successivamente alla cessazione del servizio da parte della reclamante, aveva inviato con una medesima *e-mail*, indirizzata alla stessa e a due suoi *ex* colleghi, le schede di valutazione relative all'ultimo anno di servizio, unitamente alla graduatoria con il punteggio ottenuto, consentendo, in tal modo, a tutti i destinatari di tale *e-mail* di venire a conoscenza dei rispettivi dati personali, inclusi quelli contenuti nei documenti in questione. Tenuto conto che la comunicazione era stata effettuata in assenza di base giuridica, il Garante ha adottato un provvedimento sanzionatorio nei confronti dell'ente, per la violazione degli artt. 5, par. 1, lett. a) e 6 del RGPD, nonché 2-ter del Codice (provv. 1° giugno 2023, n. 223, doc. web n. 9916798).

13.9.1.4. Diffusione online di dati dei lavoratori

Continuano a essere numerosi i reclami nei confronti di amministrazioni, in merito alla pubblicazione sui siti web istituzionali, in alcuni casi nella sezione Amministrazione trasparente o in quella Albo pretorio, di atti e documenti contenenti dati personali di lavoratori (cfr. par. 4.4).

In due distinti casi, il Garante, nel dichiarare l'illiceità della diffusione *online* dei dati personali di dipendenti pubblici, si è soffermato sugli specifici requisiti di idoneità che devono essere soddisfatti dalla base giuridica che prevede una diffusione di dati personali, sia in termini di qualità della fonte, sia in termini di proporzionalità dell'intervento regolatorio rispetto alle finalità perseguite. L'Autorità ha evidenziato che, nel quadro di derivazione europea della disciplina di protezione dei dati, nella prospettiva della certezza del diritto, nonché del principio di non discriminazione, non sono consentiti livelli differenziati di tutela della protezione dei dati personali, né su base territoriale né a livello di singola amministrazione.

In particolare, in un primo caso, pronunciandosi sulla illiceità della pubblicazione, da parte di un'azienda sanitaria, di una deliberazione riguardante la presa d'atto della conclusione di un procedimento disciplinare nonché di ulteriore documentazione relativa a progressioni economiche di taluni dipendenti, ha evidenziato che, sul piano del trattamento dei dati personali, i contratti collettivi devono limitarsi a dettagliare in favore dei dipendenti interessati il quadro normativo già fissato a livello nazionale e non possono prevedere né giustificare in alcun modo l'introduzione di un trattamento non previsto dalle norme nazionali (provv. 13 aprile 2023, n. 125, doc. web n. 9907846).

In un secondo caso, nel sanzionare un comune per la pubblicazione sull'Albo pretorio *online*, in virtù di disposizioni contenute nel contratto collettivo decentrato integrativo territoriale, di una determina relativa all'attribuzione di compensi incentivanti la produttività individuale, con allegato l'elenco dei nominativi e i relativi compensi di circa 70 dipendenti, nonché dei nominativi e degli importi relativi alle progressioni economiche orizzontali di alcuni altri dipendenti, il Garante ha ribadito l'inidoneità dei contratti collettivi a innovare direttamente l'ordinamento giuridico sul piano del trattamento dei dati personali (provv. 6 luglio 2023, n. 287, doc. web n. 9920145).

Un ufficio scolastico regionale aveva pubblicato un decreto che disponeva la pubblicazione nella sezione Albo pretorio *online* della proposta di incarico e l'assegnazione della sede in favore dei docenti inclusi nelle graduatorie provinciali di supplenza per la scuola secondaria di I e II grado. Al predetto decreto risultavano allegate due ta-

13

belle che riportavano numerosi dati personali riferiti al reclamante e ad altri interessati (circa 300), tra cui informazioni relative alla fascia, riserva, nome, cognome, data di nascita, sede di assegnazione e in particolare l'indicazione (o meno) della condizione di precedenza, ai sensi della l. n. 104/1992. Il Garante in tale occasione, nel ribadire più radicalmente che non risulta sussistente alcuna idonea base giuridica che legittimi la pubblicazione *online* dei dati personali dei docenti assegnatari di specifiche sedi, ha osservato altresì che l'accorgimento, così come rappresentato dall'ufficio scolastico nel corso dell'istruttoria, di rimuovere dai predetti documenti oggetto di pubblicazione il riferimento alla l. n. 104/1992, mantenendo tuttavia il richiamo alla presenza di una condizione di precedenza, non poteva, comunque, ritenersi conforme alla normativa in materia di protezione dei dati anche in ragione del fatto che, come evidenziato dallo stesso ufficio scolastico, la condizione di precedenza sussisteva esclusivamente in caso di fruizione dei benefici *ex l. n. 104/1992*. È stata, pertanto, disposta la limitazione del trattamento in corso, vietando all'ufficio scolastico ogni ulteriore diffusione dei dati personali degli interessati (prov. 27 aprile 2023, n. 168, doc. web n. 9896845).

Considerato che la condotta dell'ufficio scolastico regionale aveva avuto luogo nel contesto della rapida evoluzione del quadro normativo di settore, che tuttavia non ha previsto alcun obbligo di pubblicazione di dati personali dei destinatari della proposta di incarico e della assegnazione della specifica sede di servizio, nell'ambito della procedura di conferimento delle supplenze al personale docente, il Garante ha coinvolto il Ministero dell'istruzione e del merito affinché, nell'ambito dei propri compiti di indirizzo e di coordinamento, sensibilizzasse le articolazioni territoriali coinvolte nei predetti procedimenti a operare nel rispetto del quadro normativo di settore e della disciplina di protezione dei dati. Il Ministero è poi intervenuto al riguardo in data 5 giugno 2023, fornendo specifiche indicazioni e chiarimenti agli uffici territoriali al fine di prevenire simili iniziative di diffusione illecita di dati personali.

Più in generale, molti casi affrontati nel corso del 2023 hanno riguardato la diffusione *online* di atti e documenti contenenti dati personali dei lavoratori. Il Garante, nel dichiarare l'illiceità del trattamento, in ragione dell'assenza di un'idonea base giuridica, ha adottato numerosi provvedimenti, di seguito riportati, concernenti la pubblicazione sul rispettivo sito web istituzionale di:

- un provvedimento di un ufficio scolastico regionale avente a oggetto il trasferimento del reclamante, contenente informazioni personali riferite allo stesso, nonché l'indicazione del motivo di "precedenza" attribuito all'interessato nelle operazioni di mobilità territoriale, individuato "nell'assistenza al genitore disabile", ai sensi della l. n. 104/1992 (prov. 11 gennaio 2023, n. 3, doc. web n. 9857610);
- decreti di un comune con cui era stata disposta la sostituzione *ad interim* di un dipendente in quanto "assente per malattia" (prov. 23 marzo 2023, n. 84, doc. web n. 9888113);
- una delibera di un comune in cui veniva dichiarata la nullità del licenziamento del reclamante, individuato attraverso le iniziali del cognome e del nome (prov. 13 aprile 2023, n. 124, doc. web n. 9890273);
- tre determinazioni di un comune aventi a oggetto la liquidazione del fondo incentivante con riferimento alla *performance* individuale del singolo dipendente, contenenti l'elenco degli interessati con l'indicazione del nome, cognome, categoria di appartenenza e somma erogata (prov. 14 settembre 2023, doc. web n. 9940457);
- numerosi dati personali, anche relativi alla salute, dei lavoratori di un'azienda che si occupa in particolare della produzione e trasformazione dell'acciaio, da parte di un ministero (prov. 28 settembre 2023, n. 420 doc. web n. 9944603);
- una bozza di documentazione contrattuale di una regione con alcune società concessionarie di servizio di pubblico trasporto e gli elenchi dei dipendenti delle

società coinvolte nell'operazione, comprensivi dei dati relativi al rapporto di lavoro, ai redditi percepiti, ai procedimenti giudiziari pendenti con i lavoratori e alle condizioni di salute di taluni interessati (provv. 26 ottobre 2023, n. 496, doc. web n. 9955372);

- un decreto di una regione contenente i riferimenti agli importi relativi a un'indennità per i lavoratori che avevano esercitato l'opzione in alternativa alla stabilizzazione (provv. 6 luglio 2023, n. 286, doc. web n. 9920116);

- una determinazione di un ente comunale contenente dati personali della reclamante e di un'altra dipendente e, segnatamente, il riferimento a un contenzioso davanti al giudice del lavoro per restituzione di somme indebitamente percepite (provv. 26 gennaio 2023, n. 28, doc. web n. 9865528);

- la scheda di insegnamento di una docenza a contratto da parte di un ateneo in cui erano riportati il nome e cognome del docente anche a seguito della conclusione del corso di insegnamento (provv. 13 aprile 2023, n. 119, doc. web n. 9889627).

13.9.2. Dati personali di lavoratori in banche dati pubbliche

Considerato che, a decorrere dall'anno 2023, tutte le amministrazioni pubbliche hanno l'obbligo di utilizzare il portale unico del reclutamento di cui all'art. 35-ter, d.lgs. n. 165/2001 per l'avvio e la gestione di tutte le procedure concorsuali e selettive finalizzate all'assunzione di personale a tempo determinato e indeterminato e sono esonerate dall'obbligo di pubblicazione nella Gazzetta ufficiale, il Garante ha reso in via d'urgenza il parere sullo schema di decreto del Ministro per la pubblica amministrazione, avente ad oggetto le caratteristiche e le modalità di funzionamento del predetto portale, sviluppato dal Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri e disponibile all'indirizzo www.inpa.gov.it.

Le interlocazioni con il Garante sono state finalizzate a far sì che i trattamenti ivi disciplinati – in ossequio ai principi generali del trattamento nonché a quelli di protezione dei dati fin dalla progettazione e per impostazione predefinita (artt. 5 e 25 del RGPD) e tenendo conto dei rischi elevati che caratterizzano il trattamento nello specifico contesto in esame – siano effettuati con modalità tali da assicurare il contestuale rispetto della normativa in materia di azione amministrativa e di reclutamento e selezione del personale nell'ambito del pubblico impiego nonché di quella concernente la protezione dati, anche nelle fasi antecedenti all'instaurazione del rapporto di lavoro (art. 88 del RGPD, art. 113 del Codice in relazione all'art. 8 della l. n. 300/1970, e all'art. 10, d.lgs. n. 276/2003).

Il Garante ha evidenziato in proposito che i trattamenti effettuati attraverso il portale presentano rischi elevati per i diritti e le libertà degli interessati, in quanto possono essere trattati anche dati appartenenti a categorie particolari o relativi a condanne penali e reati, e che i trattamenti sono effettuati su larga scala. In particolare le indicazioni fornite dal Garante sono state volte a assicurare:

- la puntuale individuazione del ruolo svolto rispettivamente dal Dipartimento funzione pubblica e dalle pubbliche amministrazioni in relazione alle distinte finalità perseguite nell'ambito del portale;

- le modalità per assicurare che siano trattati esclusivamente i dati personali degli interessati necessari al raggiungimento della specifica finalità di selezione, reclutamento e assunzione di personale;

- la puntuale individuazione delle tipologie di dati personali acquisiti presso gli interessati fin dalla fase di compilazione del *curriculum vitae* in occasione della registrazione al portale, nonché le misure volte ad assicurare il trattamento dei soli dati esatti e aggiornati e le misure per assicurare il coordinamento con la disciplina di settore in materia di documentazione amministrativa e di controlli sulla veridicità delle dichiarazioni rese dagli interessati;

13

13

- l'individuazione dei dati acquisiti nell'ambito delle procedure di autenticazione informatica con riguardo al personale autorizzato a operare sul portale per conto delle singole amministrazioni a tutela della sfera privata del lavoratore (artt. 88 del RGPD e 113 del Codice);

- la corretta individuazione dei tempi di conservazione delle diverse tipologie di dati personali trattati e le misure volte ad assicurare che le domande di partecipazione, compilate ma non presentate, siano visibili all'amministrazione banditrice soltanto per attività di supporto alla presentazione della domanda;

- l'adozione di specifici atti formali, volti ad accertare il malfunzionamento del portale, dandone comunicazione alle pubbliche amministrazioni e prevedendo avvisi informativi a beneficio degli utenti;

- le misure per assicurare il coordinamento con la disciplina di settore in materia di pubblicità dei provvedimenti finali e delle graduatorie di procedimenti relativi a concorsi, prove selettive e procedure di reclutamento del personale delle pubbliche amministrazioni.

Considerato che lo schema di decreto ha recepito tutte le osservazioni formulate nel corso delle interlocuzioni rese con carattere di urgenza, il Garante ha espresso parere favorevole (prov. 3 novembre 2023, n. 521, doc. web n. 9954845).

Analogamente il Garante si è espresso sullo schema di decreto del Ministro per la pubblica amministrazione, adottato di concerto con i Ministri dell'interno, della difesa, dell'economia e delle finanze e della giustizia, avente a oggetto l'utilizzo del medesimo portale da parte delle forze armate, delle forze di polizia e del Corpo nazionale dei vigili del fuoco. Le indicazioni del Garante hanno avuto il principale obiettivo di assicurare garanzie uniformi in merito al trattamento dei dati personali degli interessati per accedere in condizione di parità al pubblico impiego nonché rendere effettivo il coordinamento con la disciplina di settore in materia di reclutamento e selezione del personale presso le forze armate tenendo conto della specificità dei rispettivi ordinamenti (prov. 21 dicembre 2023, n. 605, doc. web n. 9976653).

Al fine di dare attuazione alle nuove misure di sostegno dell'ADI e del SFL, introdotte dal d.l. 4 maggio 2023, n. 48, il Ministero del lavoro e delle politiche sociali ha sottoposto alla consultazione dell'Autorità due schemi di decreto concernenti, rispettivamente, l'istituzione e il funzionamento del Sistema informativo per l'inclusione sociale e lavorativa (SIISL) e l'istituzione e la realizzazione del SFL su cui è stato reso parere favorevole (prov. 3 agosto 2023, n. 354, doc. web n. 9918937; cfr. par. 4.2). Lo schema di decreto ha recepito le indicazioni rese nel corso delle interlocuzioni aventi carattere di urgenza e riguardanti, tra gli altri profili, le specifiche garanzie da adottare con riguardo ai trattamenti di dati personali anche automatizzati effettuati a fini di profilazione nell'ambito delle attività di formazione, qualificazione e riqualificazione professionale, orientamento e accompagnamento al lavoro, tenendo conto di quanto previsto in casi analoghi (cfr. Programma di garanzia di occupabilità dei lavoratori (GOL), su cui il Garante si è pronunciato favorevolmente con prov. 20 ottobre 2022, n. 353, doc. web n. 9827428). Analoghe garanzie sono state richiamate nel successivo parere reso dal Garante sullo schema di decreto del Ministero del lavoro e delle politiche sociali relativo alla disciplina dell'ADI, nel percorso di attuazione del predetto d.l. n. 48/2023 (prov. 12 dicembre 2023, n. 597, doc. web n. 10000877).

Con riguardo alla tutela dei lavoratori del settore scolastico e dell'alta formazione il Garante ha espresso, in via d'urgenza, parere favorevole, sottoposto a condizione, ai sensi degli artt. 36, par. 4, e 58, par. 3, lett. b), del RGPD, nonché dell'art. 21, comma 4-*quinquies*, d.l. 22 giugno 2023, n. 75 sullo schema di decreto del Ministro dell'istruzione e del merito concernente "la disciplina sul trattamento dei dati personali effettuato dal Ministero dell'istruzione e del merito e dalle istituzioni scolastiche

ed educative statali nell'ambito della Piattaforma famiglie e studenti" (provv. 10 ottobre 2023, n. 468, doc. web n. 9953443, cfr. par. 4.3).

Da ultimo, con riferimento allo schema di decreto del Ministro dell'istruzione e del merito, avente ad oggetto criteri e modalità relativi alla sezione dell'Anagrafe nazionale dell'istruzione riguardante gli studenti iscritti ai percorsi degli ITS *Academy* e conseguenti adeguamenti nelle funzioni e nei compiti della banca dati nazionale per il monitoraggio quantitativo e qualitativo del Sistema terziario di istruzione tecnologica, ai sensi degli artt. 12, commi 1 e 2, e 14, comma 6, l. n. 99/2022, è stato fornito un parere sia con riguardo al trattamento dei dati personali dei docenti operanti presso i predetti istituti sia in merito al trattamento dei dati personali degli studenti frequentanti, in particolare nel quadro del monitoraggio degli esiti del percorso formativo in vista dell'inserimento lavorativo degli stessi (provv. 16 novembre 2023, n. 525, doc. web n. 9966592; cfr. par. 4.3).

13

14 Le attività economiche

14.1. *Trattamento di dati in ambito assicurativo*

In linea con gli andamenti degli anni passati, anche nel 2023 si è registrato un rilevante afflusso di istanze, in particolar modo segnalazioni e reclami, relative al settore assicurativo, per la maggior parte concernenti argomenti già esaminati e definiti in precedenza dal Garante e di cui si è dato conto nelle precedenti Relazioni (v. Relazione 2020, p. 179; Relazione 2021, p. 175; Relazione 2022, p. 142).

Molte delle richieste pervenute hanno riguardato il tema della conoscibilità, da parte di chiamati all'eredità e di eredi, dei dati identificativi dei beneficiari di polizze stipulate in vita da persone decedute.

Tenuto conto dei dubbi e delle incertezze riscontrate dai titolari del trattamento in sede applicativa, delle contrastanti posizioni assunte su questo tema dalla giurisprudenza di merito e del vigente quadro normativo in materia di protezione dei dati personali come interpretato dal CEPD mediante le linee guida relative al diritto di accesso dell'interessato ai propri dati personali (varate in via definitiva il 28 marzo 2023 a seguito di consultazione pubblica), il Garante ha ritenuto di dover fornire chiarimenti di carattere generale sull'interpretazione delle norme del RGPD (art. 15, e cons. 27, 63 e 64) e del Codice come modificato dal d.lgs. n. 101/2018 (art. 2-terdecies) applicabili alla fattispecie.

Il provvedimento ha preso le mosse dall'analisi dell'art. 15 del RGPD concernente il diritto degli interessati ad accedere alle informazioni (sufficienti, trasparenti e facilmente accessibili) sul trattamento dei dati personali che li riguardano e non, di massima, a quelle riferite a terzi, cioè a soggetti diversi dall'interessato.

Il Garante ha però evidenziato che, avvalendosi della facoltà prevista dal cons. 27 del RGPD, il legislatore nazionale, con l'art. 2-terdecies, comma 1, del Codice, ha disciplinato anche la possibilità di esercitare il diritto di accesso in relazione ai dati riguardanti le persone decedute da "chi ha un interesse proprio [...] o per ragioni familiari meritevoli di protezione".

Tenuto altresì conto che, proprio nell'ambito in esame, la giurisprudenza di legittimità ha affermato, in tempi recenti (con ordinanza 13 dicembre 2021, v. Cass. civ., sez. I, n. 39531), che "l'interesse alla riservatezza dei dati personali deve cedere a fronte della tutela di altri interessi giuridicamente rilevanti, tra i quali l'interesse, ove autentico e non surrettizio, all'esercizio del diritto di difesa in giudizio", il Garante ha ritenuto che, tra i dati ai quali è possibile accedere ai sensi del combinato disposto degli artt. 15 del RGPD e 2-terdecies del Codice, rientrano anche i dati personali dei beneficiari di polizze assicurative accese in vita da una persona deceduta, purché si sia in presenza di specifici presupposti e previa attenta valutazione comparativa tra gli interessi in gioco effettuata dall'impresa assicuratrice titolare del trattamento.

Pertanto, a fronte del dichiarato interesse del richiedente a conoscere anche i nominativi dei beneficiari delle polizze, il titolare deve verificare non solo che il soggetto che esercita il diritto di accesso ai dati del defunto sia portatore di una posizione di diritto soggettivo sostanziale in ambito successorio (corrispondente alla qualità di chiamato all'eredità o di erede), ma anche che l'interesse perseguito sia concreto, attuale (cioè realmente esistente al momento dell'accesso ai dati) e strumentale o prodromico alla difesa di un proprio diritto successorio in sede giudiziaria (provv. 26 ottobre 2023, n. 520, doc. web n. 9954881).

Trattamento dei dati
relativi a soggetti
deceduti

14.2. *Trattamento di dati in ambito bancario-finanziario e sistemi di informazioni creditizie*

14

Anche il 2023 è stato contraddistinto da un elevato numero di istanze (segnalazioni, reclami, quesiti e richieste di parere) riguardanti il trattamento di dati personali effettuato da istituti di credito, società finanziarie e sistemi di informazione creditizia gestiti da soggetti privati (cd. SIC), anche su profili già approfonditi in passato dal Garante mediante l'adozione di provvedimenti collegiali (in specie, provv. 25 ottobre 2007, n. 53, doc. web n. 1457247), dei quali si è dato diffusamente conto nelle precedenti Relazioni (v. Relazione 2020, p. 181; Relazione 2021, p. 175; Relazione 2022, p. 143).

Intenso è stato il flusso di richieste in materia di esercizio dei diritti degli interessati, con specifico riferimento al diritto di accesso ai dati personali.

In linea con il consolidato orientamento dell'Autorità in materia, è stato ribadito che il diritto di accesso ai dati personali, regolato dall'art. 15 del RGPD, è diverso dal diritto di accedere ai documenti bancari disciplinato dall'art. 119, d.lgs. n. 385/1993 – t.u. delle leggi in materia bancaria e creditizia.

Le istanze di accesso ai dati personali, pertanto, oltre a doversi conformare alla disciplina in materia di protezione dei dati (artt. 12 e ss. del RGPD), non devono mirare ad ottenere (in visione o in copia) documenti bancari e non consentono di ricevere dati riferiti a soggetti diversi dall'interessato o dal *de cuius* (qualora l'istanza sia rivolta al titolare ai sensi dell'art. 2-terdecies del Codice).

Con provvedimento 26 ottobre 2023, n. 501 (doc. web n. 9965201), il Garante ha ravvisato la violazione dell'art. 12, par. 3, del RGPD nei confronti di una società che offre *online* servizi bancari e di pagamento, per omesso tempestivo riscontro all'istanza presentata dal reclamante ai sensi degli artt. 15 e ss. del RGPD. In particolare, l'interessato, non essendo andato a buon fine il processo di registrazione alla piattaforma della società per l'attivazione di servizi relativi a carte di credito ricaricabili, aveva avanzato una richiesta di esercizio dei diritti e di contestuale cancellazione dei dati riferiti a lui e ai propri figli. La società, tuttavia, nonostante avesse assicurato una risposta nei termini previsti dal RGPD, non aveva più inviato alcun riscontro in merito, se non a seguito dell'invito ad aderire formulato dall'Autorità, limitandosi, in tale occasione, a far presente che il ritardo era stato determinato da un errore (senza fornire ulteriori precisazioni).

Nel corso dell'attività istruttoria, la società, nel precisare che il motivo del ritardo era stato causato da “un mero errore accidentale imputabile ad un difetto procedurale-organizzativo”, aveva rappresentato di essersi dotata, a seguito di quanto avvenuto, di specifiche misure volte ad assicurare il rispetto dei termini e di avere provveduto, in particolare, ad automatizzare il calcolo delle tempistiche di evasione delle richieste, dapprima gestito manualmente, così da evitare il ripetersi di errori umani legati alla determinazione del termine ultimo da rispettare per fornire agli interessati il riscontro nei termini previsti.

Il Garante, pur avendo ravvisato la violazione dell'art. 12, par. 3, del RGPD, ha ritenuto, in ragione delle misure già implementate dalla società, che non vi fossero i presupposti per l'applicazione delle misure correttive e di qualificare il caso come violazione minore, ai sensi dell'art. 83 e del cons. 148 del RGPD, adottando nei confronti della società la misura dell'ammonizione, ai sensi dell'art. 58, par. 2, lett. b), del RGPD.

Similmente, con provvedimento 23 marzo 2023, n. 90 (doc. web n. 9888188), l'Autorità ha ritenuto fondate le doglianze del reclamante nei confronti di una banca che aveva omesso di fornire riscontro all'istanza di accesso ai dati personali della madre defunta avanzata ai sensi degli artt. 15 del RGPD e 2-terdecies del Codice.

Esercizio dei diritti
degli interessati

14

Nel caso di specie, a seguito dell'intervento dell'Autorità, il titolare del trattamento aveva comunicato all'interessato le informazioni richieste, rappresentando come l'omesso riscontro fosse stato determinato da un disguido operativo di una struttura della banca che, a fronte della richiesta di accesso, anziché inoltrare l'istanza alla competente funzione *privacy*, l'aveva assegnata alla struttura preposta alle pratiche successive (ove era già aperta una pratica riferita al medesimo *de cuius*). La banca aveva altresì aggiunto che il ritardo nel riscontro aveva avuto origine dal fatto che l'istanza di accesso, formulata ai sensi della normativa in materia di protezione dei dati personali ma in modo estremamente generico, era stata inviata ad una casella PEC diversa rispetto a quella specificamente e propriamente dedicata all'esercizio dei diritti.

Al riguardo, l'Autorità ha osservato che le motivazioni addotte dall'istituto di credito a giustificazione della propria condotta omissiva non potevano essere prese in considerazione, poiché anche le *Guidelines 01/2022 on data subject rights - Right of access - Version 2.0* chiariscono che non grava sugli interessati l'onere di specificare la base giuridica della richiesta, tanto che – qualora il titolare del trattamento abbia dei dubbi in merito al diritto che l'interessato intende esercitare – deve chiedere all'interessato stesso di specificarne l'oggetto (v. *Guidelines 01/2022* cit., punto 47 e punto 48).

Inoltre, in merito all'avvenuto invio dell'istanza a una casella PEC diversa da quella specificamente dedicata all'esercizio dei diritti, le sopra citate *Guidelines 01/2022* hanno precisato che sugli interessati non grava l'obbligo di adottare un determinato formato per presentare le istanze di esercizio del diritto di accesso (v. *Guidelines 01/2022* cit., punto 52). Nel caso di specie l'Autorità, considerata la particolarità della vicenda e valutate positivamente le misure organizzative apprestate dal titolare al fine di evitare il ripetersi di episodi simili nonché l'assenza di precedenti violazioni per la medesima fattispecie, ha ritenuto di definire il caso mediante adozione, ai sensi dell'art. 58, par. 2, lett. b), del RGPD, della misura dell'ammonizione.

Diversamente, seppure rispetto ad una fattispecie analoga, il Garante, con provvedimento 14 settembre 2023, n. 402 (doc. web n. 9941780) ha applicato una sanzione amministrativa pecuniaria nei confronti di un altro istituto di credito che aveva omesso di fornire riscontro a un genitore che, nell'esercizio della sua potestà genitoriale, aveva chiesto di accedere ai dati riferiti al figlio minore. Anche in questo caso, la banca aveva rappresentato di essere venuta a conoscenza dell'istanza di accesso solo al momento dell'apertura del procedimento istruttorio da parte dell'Autorità a causa di "un errore operativo intervenuto nel processo di gestione" dell'istanza medesima; in particolare, l'istanza di accesso era stata inviata a una casella PEC generale anziché a quella propriamente dedicata all'esercizio dei diritti in materia di protezione dei dati personali. Nel caso esaminato, l'Autorità, ai fini della determinazione della sanzione e del suo ammontare, ha tenuto conto del fatto che il titolare fosse già stato destinatario di precedenti provvedimenti pertinenti di cui all'art. 58 del RGPD.

Sempre in materia di esercizio dei diritti, con provvedimento 17 maggio 2023, n. 200 (doc. web n. 9902499), l'Autorità ha accolto il reclamo presentato nei confronti di un istituto di credito che non aveva fornito all'interessata un tempestivo e idoneo riscontro alla richiesta di accesso e di cancellazione delle informazioni pregiudizievoli contenute nei sistemi di informazioni creditizie e riferite ad un prestito che le era stato accordato dall'istituto medesimo; più specificamente l'istituto in questione, a fronte delle istanze avanzate ai sensi degli artt. 15 e 17 del RGPD, dapprima aveva omesso di fornire riscontro nei termini di legge e poi, tardivamente, ovvero decorsi i trenta giorni dalle istanze, anziché comunicare all'interessata i dati richiesti, si era limitato a informarla che, stante l'avvenuta cessione del credito, i dati medesimi potevano essere reperiti presso la società cessionaria quale nuovo ed effettivo titolare del trattamento, e pertanto unico soggetto in grado di fornire informazioni aggiornate. Peraltro, nel corso del procedimento istruttorio, l'istituto di credito aveva rappresentato che, pur volendo ritenere lo stesso quale effettivo destinatario delle istanze di

14

esercizio dei diritti (in luogo del cessionario), il mancato e insufficiente riscontro non sarebbe stato a lui ascrivibile bensì alla società designata quale responsabile del trattamento per la gestione e lo smistamento dei reclami e delle richieste della clientela.

Purtuttavia l'istituto di credito, non appena ricevuto l'invito ad aderire formulato dall'Autorità, aveva comunicato all'interessata i dati richiesti, precisando altresì che le informazioni pregiudizievoli segnalate nei SIC non risultavano più visibili, in quanto decorsi i termini di conservazione previsti dall'art. 7 del codice di condotta adottato dal Garante il 12 settembre 2019 (n. 163, doc. web n. 9141941). Pertanto, all'esito dell'istruttoria, l'Autorità, nel ritenere accertata la violazione dell'art. 12, par. 3 e 4 del RGPD da parte dell'istituto di credito, ha formulato alcune osservazioni in ordine alle argomentazioni addotte dalla parte. In relazione alla "carenza di legittimazione passiva", ha rammentato che l'art. 15 del RGPD riconosce all'interessato "il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano" e, di conseguenza, in caso affermativo, il diritto "di ottenere l'accesso ai dati" stessi e alle ulteriori informazioni, anche al fine di verificare la correttezza e la completezza dei dati oggetto di trattamento (anche laddove si tratti di sola conservazione dei dati – cfr. art. 4, par. 2, del RGPD).

In merito all'asserita responsabilità del soggetto nominato responsabile del trattamento ai sensi dell'art. 28 del RGPD, l'Autorità ha sottolineato come gravi specificamente sul titolare del trattamento l'obbligo di dare seguito alle istanze degli interessati relative all'esercizio dei diritti (art. 12, par. 1 e 2, del RGPD), mentre è compito del responsabile cui sia stata esternalizzata la gestione pratica delle singole richieste prestare assistenza al titolare tenendo conto della natura del trattamento, al fine di soddisfare l'obbligo del titolare del trattamento di soddisfare le richieste medesime (art. 28, par. 3, lett. e), del RGPD). La natura di tale assistenza deve, quindi, essere valutata alla luce delle caratteristiche del trattamento e le sue specifiche devono essere previste puntualmente nel contratto che, ai sensi del citato art. 28, par. 3, "vincola il responsabile del trattamento al titolare [...]"

Ancora in relazione a un reclamo in materia di esercizio dei diritti, l'Autorità ha esaminato il tema del necessario coordinamento tra i principi propri della normativa sulla protezione dei dati personali e la complessa e articolata legislazione in materia di antiriciclaggio (prov. 16 novembre 2023, n. 531 doc. web n. 9967641).

Nel caso di specie il reclamante – cui l'istituto di credito aveva comunicato il preavviso di recesso unilaterale dal contratto perché da "controlli di *routine* espletati sulla clientela" era emerso che il suo nominativo appariva in siti web pubblicamente accessibili relativamente a indagini penali condotte a suo carico dall'Autorità giudiziaria – si era rivolto all'istituto medesimo per conoscere quale fonte fosse stata utilizzata per acquisire le predette informazioni (asseritamente riferite alla sua persona), chiedendo altresì la limitazione del trattamento ai sensi dell'art. 18 del RGPD e l'opposizione all'ulteriore trattamento per finalità di *marketing*. Benché la banca, nei giorni successivi la ricezione delle istanze di accesso e di limitazione, avesse chiarito che, a seguito di "un'ulteriore analisi", era stato rilevato che le informazioni acquisite non erano esatte e che si era trattato di un fraintendimento – con conseguente annullamento della pratica di recesso – fornendo, altresì, all'interessato l'URL della fonte web da cui le informazioni erano state raccolte, il Garante, pur prendendo atto che le istanze citate erano state soddisfatte nei termini previsti dall'art. 12, par. 3, del RGPD, ha ritenuto che il trattamento di dati personali dell'interessato posto in essere dall'istituto di credito fosse in contrasto con i principi generali di minimizzazione e di esattezza dei dati, di cui all'art. 5, par. 1, lett. c) e d) e par. 2 del RGPD.

L'Autorità infatti, nel ricostruire il quadro normativo eurounitario in materia di prevenzione e contrasto al riciclaggio – articolatosi, allo stato, in cinque direttive – ha evidenziato l'impegno profuso dalla stessa, nell'arco di un ventennio – soprattutto

14

in sede di parere sui decreti di recepimento delle predette direttive nell'ordinamento nazionale – al fine di contemperare i principi fondamentali in materia di protezione dei dati personali con le esigenze di una normativa estremamente articolata, oggetto di continui interventi modificativi, applicativi e interpretativi, che impone, a un ampio novero di soggetti, l'obbligo di porre in essere complesse operazioni finalizzate a contrastare il fenomeno del riciclaggio.

In particolare l'Autorità ha evidenziato come lo stesso CEPD (e, prima ancora, il Gruppo Art. 29) abbia, in più occasioni, rilevato l'importanza di trovare un "giusto equilibrio" tra l'interesse a prevenire il riciclaggio di denaro, da un lato, e gli interessi sottesi ai diritti fondamentali alla protezione dei dati e alla vita privata, dall'altro (cfr. lettera alla Commissione europea del 19 maggio 2021).

Alla luce di un siffatto quadro giuridico, estremamente complesso e in via di continua elaborazione, il Garante, nel caso esaminato, ha accertato che la banca, nell'espletamento delle procedure di adeguata verifica della clientela a cui è tenuta, ai sensi della cd. normativa antiriciclaggio di cui al d.lgs. n. 231/2007 (come modificato dal d.lgs. n. 90/2017, dal d.lgs. n. 125/2019 e, da ultimo, dall'art. 12-bis, l. n. 136/2023 di conversione del d.l. n. 104/2023), che si sostanziano in numerose e specifiche attività, tra cui il monitoraggio e il controllo continuativo dei rapporti contrattuali in essere secondo i criteri stabiliti dalla Banca d'Italia nel provvedimento del 30 luglio 2019, attraverso la consultazione delle cd. fonti aperte (ovvero fonti pubblicamente e generalmente accessibili da chiunque) aveva raccolto, da un articolo di stampa, informazioni concernenti una persona coinvolta in una indagine penale associandole erroneamente al proprio cliente, solo sulla base del nominativo (nome e cognome), dell'età e dell'area geografica di operatività; in questo modo, sulla base di tale impropria associazione, aveva ritenuto che il profilo di rischio del cliente, alla luce della normativa antiriciclaggio, richiedesse l'adozione di misure di riduzione – consistite nella comunicazione dell'avviso di recesso – determinando, in tal modo, un illecito trattamento dei dati personali del reclamante, in quanto basato su dati inesatti e non pertinenti.

L'illiceità scaturisce dal fatto che erano state utilizzate informazioni rinvenute presso un'unica fonte (un solo articolo di stampa), risalente a due anni prima, in assenza di alcuna ulteriore necessaria verifica, da parte del titolare del trattamento, in ordine alla loro esattezza e pertinenza rispetto a uno specifico cliente identificato (art. 5, par. 1, lett. c) e d), del RGPD). E' infatti preciso dovere del titolare del trattamento assicurare che, a fronte di un dato "sospetto" astrattamente riferibile a un cliente identificato, sia sempre definita un'idonea procedura che preveda, oltre alla consultazione di più fonti - di cui sia sempre assicurato l'aggiornamento (cfr. art. 17, comma 3, d.lgs. n. 231/2007 come integrato dalla l. n. 136/2023) – anche un'attenta verifica circa la certa riferibilità dell'informazione all'interessato, in assenza della quale il trattamento di quei dati deve ritenersi precluso. Di conseguenza, l'utilizzo di dati provenienti da fonti aperte nel contesto di un trattamento di dati necessario per adempiere a un obbligo legale cui è soggetto il titolare del trattamento in materia di antiriciclaggio non è conforme alla disciplina di protezione dati se non sussistono le condizioni per attribuire l'informazione in modo certo, al di là di ogni ragionevole dubbio, a uno specifico interessato.

Al riguardo devono richiamarsi le recenti linee guida del Comitato consultivo della Convenzione 108 sul trattamento dei dati personali per finalità di lotta al riciclaggio e contrasto al finanziamento del terrorismo (adottate il 16 giugno 2023) che, appunto, raccomandano l'attuazione, da parte dei soggetti obbligati, di procedure idonee a garantire il rispetto del principio di accuratezza cui all'art. 5, par. 1, lett. d), del RGPD in qualsiasi trattamento dei dati connesso alle operazioni di adeguata verifica della clientela, in modo da evitare rischi ed effetti dannosi sui diritti del cliente/interessato che potrebbero derivare dal trattamento di dati non aggiornati (cfr. par. 3.5 - raccomandazione).

Le medesime linee guida aggiungono, altresì, che nel caso in cui le informazioni siano state raccolte ed elaborate da una terza parte (sulla quale il titolare del trattamento fa affidamento), l'obbligo di provvedere all'aggiornamento dei dati e delle informazioni relative all'adeguata verifica della clientela incombe comunque sul titolare (par. 3.5 - contestualizzazione AML/CFT 37).

Si segnala infine che, nel caso di specie, l'Autorità ha ritenuto di poter considerare come minore la violazione accertata, con conseguente ammonimento nei confronti del titolare, ai sensi degli artt. 143 del Codice e 58, par. 2, lett. b), del RGPD; al riguardo, è stato tenuto conto, da un lato, del comportamento della banca che, oltre ad avere prontamente provveduto a interrompere la correlazione dei dati del cliente con le informazioni riguardanti un terzo, aveva immediatamente comunicato all'interessato l'origine dell'informazione medesima; dall'altro, della complessità della normativa antiriciclaggio alla luce dell'articolato quadro giuridico di riferimento.

È stato altresì affrontato il tema della limitazione ai diritti degli interessati, di cui agli artt. da 15 a 22 del RGPD, con specifico riferimento agli interessi tutelati dalle disposizioni in materia di riciclaggio (d.lgs. n. 231/2007, attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo). In particolare, sono pervenuti al Garante due reclami, da parte dello stesso interessato, che evidenziavano il non completo riscontro alle istanze di esercizio dei diritti dallo stesso avanzate a due diversi istituti di credito, e che, all'esito dell'attività istruttoria, sono stati definiti dal Garante con distinti provvedimenti di ammonimento per la violazione degli artt. 5, par. 1, lett. a) e c) e 15 del RGPD.

È emerso infatti che il rifiuto da parte di entrambi gli istituti di credito a fornire all'interessato tutte le informazioni in loro possesso allo stesso riferite trovava il presupposto sia nell'art. 2-undecies del Codice, che consente l'applicazione del principio di limitazione qualora dall'esercizio di tali diritti possa derivare un pregiudizio "agli interessi tutelati in base alle disposizioni in materia di riciclaggio", sia nella normativa in materia di antiriciclaggio che prevede "il divieto ai soggetti tenuti alla segnalazione di un'operazione sospetta e a chiunque ne sia comunque a conoscenza, di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo" (d.lgs. n. 231/2007, art. 39). Gli istituti di credito, quindi, poiché si trattava di informazioni oggetto di valutazione nell'ambito della normativa in materia di antiriciclaggio, hanno ritenuto che la comunicazione all'interessato di tali informazioni, delle quali erano venuti a conoscenza da organi di stampa e accedendo a banche dati pubbliche, avrebbe potuto comportare una violazione delle citate disposizioni.

Il Garante, all'esito dell'attività istruttoria, ha ritenuto che, nei casi in esame, non ricorressero gli estremi per l'applicazione della misura prevista dall'art. 2-undecies recante la limitazione al diritto di accesso, dal momento che, trattandosi di informazioni accessibili a chiunque - in quanto provenienti da banche dati pubbliche - e note all'interessato, la loro comunicazione non avrebbe comportato un pregiudizio effettivo e concreto all'interesse generale tutelato dalle disposizioni in materia di riciclaggio tale da giustificare la limitazione dei diritti dell'interessato. In particolare, il Garante ha precisato che non tutte le informazioni raccolte per finalità antiriciclaggio devono, necessariamente, essere oggetto di limitazione in termini di esercizio dei diritti degli interessati, essendo piuttosto necessario che il titolare del trattamento effettui una valutazione circa la natura delle informazioni e le conseguenze della loro comunicazione. Tale valutazione non può prescindere dal considerare se la limitazione costituisca una misura necessaria e proporzionata in relazione agli interessi che si intendono salvaguardare.

14

14

Furti di identità e frodi informatiche

Trattamento dei dati nei sistemi di informazione creditizia (SIC)

In tal senso si è espresso anche il CEPD nelle linee guida 10/2020 sulle restrizioni ai sensi dell'art 23 del RGPD adottate il 13 ottobre 2021. Le stesse linee guida riportano, tra i casi nei quali tale limitazione può trovare applicazione, quello di salvaguardare “la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, compresa la tutela e la prevenzione di minacce alla sicurezza pubblica”. In particolare, nel caso dell'antiriciclaggio, la limitazione ai diritti potrebbe essere necessaria laddove fornire informazioni a interessati sottoposti ad indagine potrebbe compromettere il successo dell'indagine stessa.

Le informazioni omesse, tuttavia, dovrebbero essere fornite non appena la loro comunicazione non comporti più un pregiudizio all'indagine in corso. L'applicazione della limitazione, quindi, deve rispondere ai principi di necessità e proporzionalità, in ragione dei quali il diritto dell'interessato a ricevere le informazioni che lo riguardano non può essere eliminato, ma eventualmente differito a un momento successivo.

Per tale motivo il legislatore nazionale, nel disporre in merito alle limitazioni dei diritti dell'interessato, ha previsto, secondo un criterio di gradualità, la possibilità di ritardare, limitare e, in ultima istanza, escludere l'esercizio dei diritti degli interessati. È inoltre stabilito che il titolare è tenuto a informare l'interessato della facoltà, allo stesso riconosciuta, di esercitare i diritti anche tramite il Garante, con le modalità di cui all'art. 160 del Codice, affinché siano effettuati gli opportuni accertamenti, all'esito dei quali “il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale” (art. 2-terdecies del Codice).

In entrambi i provvedimenti adottati, l'Autorità ha ritenuto di applicare la misura dell'ammonimento, tenuto conto della complessità del quadro giuridico di riferimento, del profilo di novità rappresentato dalla vicenda, nonché dell'assenza di precedenti pronunce da parte dell'Autorità in merito a questo specifico tema (provvti 13 aprile 2023, n.128, doc. web n. 9888438 e n.129, doc. web n. 9888457).

Nel corso dell'anno sono cresciute le richieste rivolte al Garante rispetto a fattispecie riconducibili a furto d'identità e a frodi informatiche.

Nei casi esaminati, si è rammentato che, preso atto dell'aumento di frodi informatiche sempre più sofisticate e complesse sul piano tecnologico, il Garante ha già da tempo reso disponibile, sul proprio sito, una scheda informativa per sensibilizzare l'utenza affinché adotti accorgimenti e cautele per evitare di rimanere vittima di comportamenti fraudolenti e illeciti penali (v. doc. web n. 5779928).

Si è pure ribadito che indicazioni sui comportamenti da assumere o evitare per non incorrere in questa tipologia di frodi sono sempre presenti sui siti istituzionali di ogni banca e intermediario finanziario che consenta alla clientela di operare a distanza e che, agli strumenti e alle iniziative già adottate in materia di sicurezza da ABI, istituzioni e singole banche, si affianca anche un *Vademecum* (del 2022 e sottoposto a periodici aggiornamenti) che l'ABI stessa e la Polizia di Stato hanno realizzato congiuntamente ed è consultabile sui rispettivi siti istituzionali.

Considerato, peraltro, che tutti gli interessati avevano denunciato gli eventi occorsi nelle sedi preposte all'accertamento delle fattispecie di reato rinvenibili nelle condotte oggetto di successive istanze all'Autorità, ci si è riservati – anche alla luce dell'art. 167, comma 4, del Codice – di assumere eventuali determinazioni all'esito sulla base delle risultanze degli accertamenti già attivati in sede giudiziaria.

Molteplici sono stati i reclami e le segnalazioni in materia di trattamenti di dati personali censiti nei sistemi di informazioni creditizie gestiti da soggetti privati (cd. SIC).

Alcune richieste hanno riguardato il tema del preavviso da rendere all'interessato, al verificarsi di ritardi nel pagamento degli importi pattuiti e prima dell'inserimento dei dati nei SIC; altre i tempi di conservazione dei dati nei SIC (diversi a seconda che il rapporto censito sia stato stipulato o meno e, in caso positivo che abbia o meno un andamento regolare).

In tutti i casi esaminati sono state richiamate, in particolare, le norme contenute nel codice di condotta – strumento di autoregolamentazione ad adesione volontaria in grado di concorrere, nel settore che rileva, alla corretta applicazione della normativa in materia di protezione dei dati personali (art. 40) – approvato dal Garante dapprima il 12 settembre 2019 e, in via definitiva, con provvedimento 6 ottobre 2022, n. 324 (doc. web n. 9818201) con il quale è stato anche accreditato il relativo organismo di monitoraggio.

Nella quasi totalità delle fattispecie esaminate, in relazione alle istanze pervenute all’Autorità non sono risultate comprovate violazioni della normativa in materia di protezione dei dati personali.

Nel corso del 2023 è proseguita la partecipazione del Garante, quale membro permanente, all’attività del Comitato di coordinamento FINTECH istituito presso il MEF (d.m. n. 100/2021, attuativo della delega prevista dal d.l. n. 34/2019), con lo scopo di esaminare e autorizzare la sperimentazione in un ambiente controllato (*sandbox*) di progetti relativi a prodotti e servizi tecnologicamente innovativi nel settore bancario, finanziario e assicurativo, presentati da intermediari vigilati e operatori del settore FINTECH.

La sperimentazione avviene per un periodo di tempo limitato (18 mesi) e durante tale fase gli operatori FINTECH possono beneficiare di un regime semplificato transitorio, in costante dialogo con le autorità di vigilanza (Banca d’Italia, CONSOB, IVASS), anche attraverso la deroga di atti di carattere generale nonché delle norme o dei regolamenti adottati dalle autorità di vigilanza, specificamente indicati dall’art. 10 del d.m. n. 100/2021.

Nel corso dell’anno si sono svolte le sperimentazioni relative ai progetti presentati e ammessi con la prima finestra temporale aperta dal 15 novembre 2021 al 15 gennaio 2022 ed è stata avviata la seconda fase di sperimentazione con una finestra temporale aperta dal 3 novembre al 5 dicembre 2023.

Il Garante ha partecipato, insieme ad altre amministrazioni, alle riunioni periodiche del Comitato, nel corso delle quali le autorità di vigilanza (Banca d’Italia, CONSOB, IVASS) hanno fornito un aggiornamento sullo stato delle istruttorie relative alle richieste pervenute e delle sperimentazioni dei progetti ammessi. In relazione a taluni progetti, la Banca d’Italia ha chiesto un confronto informale con l’Autorità, che si è svolto anche attraverso incontri con le singole società coinvolte. Vi sono stati, inoltre, incontri con singole società che, tramite l’autorità di vigilanza competente, hanno richiesto un confronto con il Garante in merito a eventuali profili di criticità nel trattamento dei dati personali emersi dai progetti presentati.

Nell’ambito del Gruppo di lavoro “Rete dei RPD nel settore bancario” il primo obiettivo è stato quello di fornire una “fotografia” delle caratteristiche che connotano il ruolo e l’attività del RPD in tale contesto, attraverso un questionario condiviso tra ABI e l’Autorità. Il rapporto illustrativo delle principali evidenze del questionario è frutto del contributo di circa 90 associati ABI, tra gruppi bancari e banche individuali, e può quindi considerarsi ben rappresentativo del comparto.

Il questionario e la lettera di accompagnamento sono stati inviati dalle associazioni di categoria ai RPD delle banche associate in data 10 febbraio 2023 con l’invito a compilare il questionario entro il 15 marzo 2023. Il questionario è stato formulato attraverso 46 domande suddivise in 5 macro sezioni: designazione, requisiti ed esperienza del RPD; compiti e risorse del RPD; ruolo e posizione del RPD; descrizione del titolare del trattamento, risorse e formazione del RPD; note, osservazioni e suggerimenti. La somministrazione del questionario e l’analisi delle risposte formulate dalle banche sono state effettuate da ABI e FEDERCASSE. Al questionario hanno partecipato ottantasette (87) rispondenti, tra banche individuali e capogruppo di gruppi bancari. Con riferimento alle principali evidenze del questionario relativamente alle modalità di designazione del RPD, di svolgimento dell’attività e

14

Comitato FINTECH**Rete dei RPD in ambito bancario**

14

inquadramento aziendale è emerso che, nella quasi totalità dei casi, il titolare del trattamento ha formalizzato la nomina del RPD mediante un apposito atto di designazione, principalmente tramite la sottoscrizione di appositi accordi di servizio. Nelle banche di maggiori dimensioni e in quelle intermedie il responsabile per la protezione dei dati è prevalentemente un dipendente del titolare del trattamento. Invece, nelle banche di minori dimensioni, nella maggior parte dei casi il RPD è un soggetto esterno alla banca. In tutti e tre i casi è emerso che, in linea generale, il RPD non svolge attività a titolo esclusivo per il titolare.

Un altro aspetto significativo riguarda il fatto che lo stesso RPD spesso svolge la sua funzione nei confronti di più entità giuridiche (molte volte appartenenti allo stesso gruppo e operanti anche in settori di attività esterni a quello bancario). Ciò impone una riflessione in termini di sufficienti risorse allocate ai RPD (anche in termini di staff e di tempo) nonché di situazioni di potenziale conflitto d'interesse.

La descrizione dei compiti fornita dal titolare corrisponde sostanzialmente a quelli effettivamente svolti dal RPD. Questi, inoltre, in linea generale, ha accesso e riceve informazioni necessarie per svolgere i suoi compiti. Inoltre, nelle banche di minori e intermedie dimensioni, generalmente esistono procedure per tracciare le consultazioni e i pareri emessi dal RPD, ma nella maggior parte dei casi non sono stati approntati processi interni per documentare le decisioni assunte dal titolare in cui si disattendono le indicazioni del RPD.

Nella maggior parte dei casi il RPD partecipa a iniziative formative almeno una o due volte l'anno, generalmente attraverso la frequentazione di corsi e convegni. L'utilizzo di certificazioni in materia di sicurezza e *data protection* (UNI 11697:2017), abbastanza diffuso nel settore, obbliga, inoltre, a una formazione continua del RPD. Il 28 novembre 2023 si è svolta una riunione con ABI e alcuni RPD della "Rete" per commentare il rapporto illustrativo, e in tale occasione è stato proposto alla Rete – come obiettivo da perseguire nel 2024 – di lavorare congiuntamente alla definizione di informative (ai sensi degli artt. 13 e 14 del RGPD) omogenee e semplificate mediante l'utilizzo di icone standardizzate per il settore. Il rapporto illustrativo dei risultati dei questionari è disponibile sul sito istituzionale del Garante.

Si è tenuto il 23 giugno 2023 in collaborazione con Lepida S.c.p.A. l'evento "RPD al centro!". Gli RPD del settore pubblico e privato sono stati protagonisti di una giornata di confronto con il Garante. A cinque anni dall'applicazione del RGPD, l'Autorità ha incontrato nuovamente a Bologna gli RPD per fare un bilancio dell'esperienza maturata e per individuare le aree di intervento finalizzate a rafforzare il ruolo di tale figura nel prossimo futuro. I partecipanti in presenza sono stati circa 800 e l'evento è stato registrato e messo a disposizione degli utenti sul sito istituzionale del Garante e di Lepida. Le tematiche affrontate hanno riguardato: designazione, requisiti, esperienza, formazione e aggiornamento del RPD rischi connessi alla posizione del RPD (indipendenza e conflitto di interessi); valore preventivo dell'attività del RPD (contributo del RPD nelle situazioni complesse e rapporto con l'Autorità) (cfr. par. 23.1).

**Organizzazione
dell'evento "RPD al
centro!"**

14.3. Imprese

In materia di esercizio dei diritti degli interessati, il Garante si è pronunciato nei confronti di una società di noleggio a lungo termine in relazione all'inesatto riscontro ad un'istanza di diritto di accesso, applicando una sanzione pecuniaria di 40 mila euro (prov. 17 maggio 2023, n. 199, doc. web n. 9899914).

La violazione ha riguardato, in particolare, gli artt. 12 e 15 del RGPD a fronte del mancato rilascio, da parte del titolare, di informazioni personali dell'istante – acquirente previo accesso ai SIC – utilizzate per giungere ad una valutazione di inaffidabilità

Esercizio dei diritti

dello stesso ostativa all'accoglimento della richiesta di finanziamento per un noleggìo a lungo termine.

L'Autorità, nel rammentare che il titolare è tenuto a fornire l'accesso ai dati personali dell'interessato in forma completa e aggiornata, ha precisato che i titolari, in sede di riscontro *ex art.* 12 del RGPD, non possono limitarsi alla mera menzione del ricorso a valutazioni sul merito creditizio – come era avvenuto nel caso oggetto di contestazione – né limitarsi ad invitare l'interessato a rivolgersi al gestore del SIC al fine di reperirle, dovendo invece fornire, anche in ragione del ruolo di partecipanti ai SIC, in adempimento all'*art.* 15 del RGPD, tutte le informazioni ivi acquisite ed effettivamente trattate.

Il provvedimento ha costituito l'occasione per ribadire l'importanza dell'istituto del diritto d'accesso ai propri dati in relazione alle attività delle società private funzionali alla verifica dell'affidabilità della clientela, in ragione della natura particolarmente delicata delle informazioni trattate (afferenti al merito creditizio degli interessati) nonché delle possibili conseguenze pregiudizievoli sui diritti e sulle libertà dell'individuo derivanti da un inesatto riscontro da parte del titolare alle istanze di accesso *ex art.* 15 del RGPD (prima tra tutte, l'impossibilità di verificare l'esattezza delle informazioni trattate per decretare il diniego del finanziamento richiesto e, quindi, di valutare l'eventuale esercizio del diritto di rettifica/cancellazione delle stesse).

Con riferimento ai trattamenti aventi a oggetto categorie particolari di dati personali (*art.* 9 del RGPD), il Garante ha adottato un provvedimento correttivo e sanzionatorio nei confronti del gestore di una piattaforma di *dating online* volta a consentire agli utenti registrati la ricerca di potenziali *partner* sul territorio nazionale (prov. 7 dicembre 2023, n. 599, doc. web n. 9978568).

La decisione, assunta a seguito di una complessa attività istruttoria che ha richiesto anche un accertamento ispettivo *in loco*, ha rilevato l'illiceità dei trattamenti dei dati personali (tra cui anche quelli relativi alle preferenze e agli orientamenti sessuali) di circa 1 milione di utenti iscritti al sito d'incontri in violazione degli *artt.* 5, par. 1, lett. a), e) ed f) e *parr.* 2; 9, 13, 24, 32, 30, 35 e 37 del RGPD. Nella specie, è stato accertato che la società aveva trattato le informazioni personali degli utenti raccolte in sede di registrazione dei relativi *account* all'area privata del sito, nonché caricate successivamente da questi ultimi (quali, per es., quelle contenute in foto personali degli stessi), in assenza dei necessari presupposti di legittimità del trattamento e a fronte di un'informativa inidonea. È altresì emerso che il predetto titolare non disponeva di una specifica *privacy policy* inerente alle tempistiche di conservazione dei dati personali trattati, limitandosi a procedere in maniera disarticolata alla cancellazione degli *account* non più attivi e delle informazioni ivi contenute, così come delle richieste di iscrizione non andate a buon fine. Parimenti, con riferimento agli obblighi di cui all'*art.* 33 del RGPD, è stata constatata l'assenza di misure tecnico-organizzative idonee a garantire l'integrità e la riservatezza delle informazioni personali trattate, soprattutto alla luce della loro delicatezza e dei connessi significativi rischi per i diritti e le libertà degli interessati coinvolti.

La società, infine, pur essendovi tenuta, non aveva redatto il registro delle attività di trattamento, non aveva nominato il RPD, né aveva predisposto la valutazione d'impatto richiesta dall'*art.* 37 del RGPD.

In ragione delle numerose violazioni riscontrate, il Garante ha comminato una sanzione pecuniaria di 200.000 euro e ha ingiunto una serie di misure correttive volte a conformare il trattamento oggetto di contestazione al RGPD. In tale ottica è stato prescritto alla società, in particolare, di individuare adeguate tempistiche di conservazione delle informazioni personali trattate, provvedendo a cancellare i profili degli utenti la cui conservazione risulti eccedente; di redigere la valutazione

14

Dating online

14

Settore alberghiero

App per il rimborso dei costi autostradali

d'impatto in materia di protezione dei dati personali; di adottare specifiche misure tecniche volte a rafforzare la sicurezza dei trattamenti posti in essere nell'ambito della piattaforma di *dating* (tra cui, per es., sistemi di *Identity and Access Management*; misure di cifratura o di pseudonimizzazione dei dati sensibili; *file di log* dotati di marche temporali e controlli di integrità degli stessi).

Nel corso del 2023 si è conclusa l'attività di indagine nei confronti di una società facente parte di un gruppo multinazionale operante nel settore alberghiero. Dalle verifiche condotte sono state accertate violazioni che hanno portato all'applicazione di una sanzione pecuniaria di duecentomila euro (provv. 1° giugno 2023, n. 229, doc. web n. 9980043).

Le violazioni riscontrate hanno nello specifico riguardato la registrazione nel sistema di prenotazione alberghiero dei dati personali afferenti alle allergie e/o intolleranze alimentari degli ospiti (acquisiti in sede di *check-in* e a seguito di specifiche richieste da parte dei medesimi) nonché i contratti stipulati dalla società con i soggetti che trattano i dati personali acquisiti tramite gli impianti di videosorveglianza installati presso le strutture alberghiere.

In merito al primo profilo, l'Autorità ha ribadito l'obbligo in capo alla società, quale titolare del trattamento, di informare adeguatamente la clientela in occasione della raccolta dei predetti dati, ai sensi dell'art. 13 del RGPD, affinché gli interessati siano messi nella condizione di prestare il proprio consenso in maniera consapevole rispetto a tale specifica finalità.

Inoltre – tenuto conto della natura delle informazioni in questione, particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, in quanto riconducibili ai dati relativi alla salute – è stato ribadito che il consenso può considerarsi validamente prestato soltanto ove lo stesso sia non soltanto specifico ed informato, ma anche fornito dagli interessati in forma esplicita, come stabilito dall'art. 9, par. 2, lett. a), del RGPD (v. sul punto cons. 51 del RGPD e par. 4 delle linee guida 5/2020, cit.). Trattasi di misure che, come constatato in sede di accertamenti, e in particolare all'esito dell'esame della modulistica predisposta dalla società ivi acquisita, non erano state invece adottate da quest'ultima, in violazione delle disposizioni di cui agli artt. 5, par. 1, lett. a), 9 e 13 del RGPD.

Inoltre, rispetto all'ulteriore profilo relativo agli impianti di videosorveglianza ubicati presso le strutture alberghiere, è stato rilevato che la società si avvaleva di servizi di progettazione, installazione e manutenzione offerti da soggetti terzi, in qualità di fornitori. Tenuto conto che l'erogazione di tali servizi poteva comportare trattamenti di dati personali degli ospiti dell'hotel da parte dei soggetti incaricati (anche solo in ragione degli accessi alle immagini registrate dalle telecamere in occasione dello svolgimento dell'attività di manutenzione), ne è seguita l'ulteriore violazione dell'art. 28 del RGPD. In sede di verifiche, è stato infatti accertato che la società non aveva disciplinato il rapporto instaurato con i fornitori deputati alla manutenzione dei predetti impianti, che avrebbe invece dovuto avere luogo mediante la predisposizione di un contratto (o di altro atto giuridico) recante la designazione a responsabile del trattamento e le relative istruzioni, in conformità alla sopra citata disposizione.

L'Autorità si è pronunciata nei confronti di una società concessionaria della rete autostradale a seguito di un'istanza presentata da un'associazione di consumatori, con la quale è stata segnalata una *app* volta a consentire il rimborso totale o parziale del costo del biglietto autostradale per ritardi dovuti a cantieri per lavori (provv. 22 giugno 2023, n. 264, doc. web n. 9909702).

Il Garante ha dichiarato l'illiceità del trattamento dei dati personali di circa 100.000 utenti, effettuato per il tramite della menzionata *app* e ai fini dell'erogazione del predetto servizio, in ragione della riscontrata violazione degli artt. 5, par. 1, lett.

a); 13 e 28 del RGPD, e ha applicato la sanzione pecuniaria di 1 milione di euro.

Nel corso dell'istruttoria, a seguito della valutazione delle circostanze concrete relative al caso di specie, è stato constatato che, diversamente da quanto indicato nella documentazione contrattuale acquisita agli atti e riportato nell'informativa resa agli utenti ai sensi dell'art. 13 del RGPD, la società rivestiva il ruolo di titolare del trattamento e non quello di responsabile; quest'ultimo ruolo era invece ricoperto da altra società incaricata di provvedere allo sviluppo e alla gestione dell'*app* in questione. Era stata infatti la società concessionaria ad aver definito le finalità e i mezzi del trattamento, stabilendo il meccanismo di rimborso del costo del pedaggio, le condizioni e i requisiti della richiesta dello stesso da parte degli utenti, e la tipologia del ritardo correlato alla presenza dei cantieri. Di contro, lo sviluppatore aveva agito a fronte dell'incarico espressamente conferitogli e sulla base della procedura e dei criteri individuati dalla società concessionaria. L'errata qualificazione dei ruoli *privacy* rivestiti dalle due società ha avuto immediate ripercussioni anche sulla conformità al RGPD dell'informativa, che non indicava correttamente l'effettiva identità del titolare e le finalità del relativo trattamento, né recava le ulteriori informazioni volte ad assicurare, nel rispetto dei principi generali di cui all'art. 5 del RGPD, un trattamento corretto e trasparente dei dati personali degli utenti.

Da ultimo, nel rilevare che i rapporti tra le due società avrebbero dovuto essere regolati, ai sensi dell'art. 28 del RGPD, sulla base di un contratto o altro atto giuridico, è stata rilevata anche l'ulteriore violazione consistente nella mancata designazione del soggetto responsabile del trattamento.

Di significativa rilevanza è stata infine la richiesta – qualificata come consultazione preventiva ai sensi dell'art. 36 del RGPD – con cui una società ha rappresentato l'intenzione di voler procedere, in proprio e nell'interesse di altre società del gruppo, al trattamento dei dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza delle proprie controparti contrattuali, anche potenziali, al fine di preservare la propria attività dai rischi di infiltrazioni criminali.

In particolare, al fine di stabilire relazioni economiche con *partner* "affidabili", le società del gruppo intendevano richiedere a questi ultimi, all'atto della loro iscrizione al portale di *procurement*, un'autodichiarazione relativa all'assenza, in capo ai relativi "soggetti rilevanti", di procedimenti giudiziari *ex d.lgs. nn. 231/2001 e 159/2011*, per poi verificarne l'eventuale veridicità attraverso informazioni autonomamente acquisite presso "fonti aperte".

Considerata la delicatezza dei trattamenti prospettati, la società aveva provveduto a effettuare una valutazione di impatto ai sensi dell'art. 35 del RGPD, individuando tuttavia, anche a seguito del parere negativo reso al riguardo dal proprio RPD, un elevato rischio "residuo" per i diritti e le libertà degli interessati, in ragione dell'assenza nell'ordinamento di un'ideale base giuridica per il trattamento dei suddetti dati.

Con nota 5 luglio 2023, l'Ufficio, premessa l'inidoneità della richiesta formulata dalla società (risultata carente sul piano delle informazioni di dettaglio e fondata, più che sull'indicazione dei rischi "residui" non attenuabili dal titolare del trattamento, sull'assenza stessa di un'ideale base giuridica per il trattamento medesimo), ha comunque provveduto a fornire prime indicazioni a quest'ultima, richiamando dapprima i presupposti normativi per il trattamento dei dati relativi a condanne penali, a reati o a connesse misure di sicurezza (art. 10 del RGPD, art. 2-*octies* del Codice; art. 22, comma 12, d.lgs. n. 101/2018) ed evidenziando, successivamente, la necessità di un'ideale base giuridica (di natura legislativa o, nei casi previsti dalla legge, regolamentare) quale condizione di legittimità dei trattamenti stessi.

Nel caso di specie, l'inesistenza – evidenziata dallo stesso RPD della società – di adeguate disposizioni legislative o regolamentari che disciplinassero i trattamenti in esame e che prevedessero, altresì, misure appropriate a tutela dei diritti e delle libertà

14

Consultazione
preventiva

14

degli interessati non ha consentito, nelle more dell'adozione del decreto ministeriale di cui al citato art. 2-*octies* del Codice, di individuare idonei presupposti per il lecito trattamento dei dati sopra indicati; si è, tuttavia, ricordato che il trattamento dei dati relativi a condanne penali, a reati o a connesse misure di sicurezza è comunque consentito, sulla scorta del già menzionato art. 22, comma 12, d.lgs. n. 101/2018, e sino alla data di entrata in vigore del predetto decreto ministeriale, se effettuato in attuazione dei protocolli di intesa previsti da tale disposizione. Le società del gruppo sono state pertanto invitate ad attendere la conclusione del (già avviato) procedimento di adesione ai suddetti protocolli ai fini dell'eventuale trattamento dei dati in esame.

14.4. *Concessionari di pubblici servizi*

In relazione ai trattamenti effettuati da concessionari di pubblici servizi, il 2023 è stato caratterizzato da un'intensa attività di vigilanza e di controllo volta a verificare il corretto adempimento della normativa di protezione dei dati personali da parte dei fornitori operanti nel mercato libero dell'energia elettrica e del gas, anche in considerazione delle rilevanti implicazioni – in termini di allargamento della platea di interessati coinvolti – derivanti dall'imminente completamento del processo di liberalizzazione del mercato energetico.

L'attenzione dell'Autorità si è appuntata sulle diverse segnalazioni pervenute da interessati coinvolti nella prima fase del processo di liberalizzazione suddetto, consistita nella migrazione al Servizio a tutele graduali dei contratti di fornitura erogati a favore delle microimprese che al 1° aprile non erano ancora passate al mercato libero. Sul punto, il Garante ha chiarito che tale Servizio, sulla base della disciplina vigente in materia (art. 1, comma 60 della legge annuale per il mercato e la concorrenza n. 124/2017), opera di *default* nei confronti dei predetti clienti e determina un passaggio automatico degli stessi a fornitori specificamente individuati per territorio sulla base di procedure di aggiudicazione pubblica. Pertanto, alla luce delle summenzionate disposizioni di settore, il trattamento dei dati personali dei clienti forzatamente migrati al succitato nuovo fornitore del Servizio a tutele graduali è lecito in quanto effettuato nell'ambito della cornice normativa sopra richiamata (v. art. 6, comma 1, lett. c), del RGPD).

Contratti non richiesti

Anche alla luce del contesto sopra delineato, sono state avviate diverse attività d'indagine, in alcuni casi comprendenti accertamenti ispettivi, dirette, nello specifico, a individuare pratiche illecite da parte dei predetti fornitori, volte all'acquisizione di contratti non richiesti nel settore energetico mediante il trattamento di dati personali inesatti e non aggiornati dei potenziali clienti.

Si tratta di un fenomeno, oramai largamente diffuso e in continua evoluzione, generalmente frutto di attività fraudolente poste in essere da agenti che disattendono le mansioni loro attribuite contrattualmente nonché le istruzioni fornite dai titolari del trattamento ai sensi dell'art. 28 del RGPD, approfittando, nella maggior parte dei casi, dell'inadeguatezza, in termini di *accountability*, delle misure tecniche e organizzative adottate dai fornitori di energia per conformare i trattamenti di dati personali dei clienti al RGPD (artt. 5, par. 2 e 24).

Sul punto, l'Autorità si è, *in primis*, pronunciata, con provvedimento 28 settembre 2023, n. 427 (doc. web n. 9940988), nei confronti di un fornitore operante su scala nazionale. In tale sede, è stata accertata l'illiceità dei trattamenti da quest'ultimo posti in essere nei confronti di circa 5.100 clienti interessati in violazione degli artt. 5, par. 1, lett. a) e d) e par. 2 e 24 del RGPD.

È in particolare emerso che le misure tecniche e organizzative adottate dal titolare, nell'ambito dei processi di contrattualizzazione della clientela dallo stesso

implementati per il tramite del canale agenzia porta a porta, non erano adeguate alla natura, al contesto, alle finalità e ai rischi del trattamento, configurando innanzitutto la violazione del principio di responsabilizzazione che impone al titolare di attuare un sistema organizzativo e gestionale contraddistinto da misure effettive ed efficaci di protezione dei dati, nonché comprovabili. L'art. 24 del RGPD, inoltre, impone al titolare di configurare *ab origine* il trattamento mediante l'adozione di tutte le garanzie necessarie a tutelare con efficacia i diritti degli interessati, richiedendo un'attenta analisi dei rischi per i diritti e le libertà di questi ultimi.

Il Garante, dopo aver accertato l'inadeguatezza degli strumenti di *accountability* adottati dalla società, ha applicato una sanzione pecuniaria di 10 milioni di euro e imposto alla stessa l'adozione di una serie di misure tecniche e organizzative atte a garantire l'esattezza dei dati personali dei potenziali clienti che, in quanto riportate all'elevata diffusione negli ultimi anni del fenomeno delle attivazioni non richieste nel mercato libero dell'energia, devono essere idonee a rafforzare le attività di vigilanza delle società fornitrici sull'operato delle agenzie esterne incaricate della contrattualizzazione dei clienti. Le misure in questione includono, in particolare, l'introduzione di sistemi di *alert* in grado di rilevare eventuali comportamenti scorretti e/o fraudolenti da parte degli agenti nell'acquisizione dei dati di potenziali clienti; l'implementazione di meccanismi di accertamento dell'effettiva ricezione delle comunicazioni trasmesse al cliente in fase di contrattualizzazione; l'adozione di regole procedurali volte a rafforzare le attività di *audit* nei confronti dell'operato delle agenzie selezionate per svolgere le attività di contrattualizzazione in modalità porta a porta.

Si segnala da ultimo che, con riferimento ai dati dei clienti rispetto ai quali era stata accertata l'attivazione di contratti non richiesti mediante trattamento illecito delle informazioni personali loro riferite, l'Autorità ha altresì rilevato l'assenza di un sistema idoneo a prevedere, a seguito di un reclamo per attivazione non richiesta (e nelle more della definizione dello stesso), forme di segregazione di ogni ulteriore e diversa attività di trattamento dei dati dei clienti, al fine di sospendere in via precauzionale eventuali trattamenti illeciti dei predetti dati (ad es. per finalità di *marketing* o di profilazione).

A tal fine, è stata pertanto prescritta, con la medesima decisione, l'implementazione, da parte del titolare, di una procedura che preveda la tempestiva limitazione di ogni ulteriore attività di trattamento dei dati personali inerenti a contratti/proposte contrattuali rispetto alle quali sia stato presentato un reclamo per attivazione non richiesta, sulla base di meccanismi di oscuramento dei dati e di segregazione logica e fisica degli stessi volti a garantire la separazione delle relative operazioni di trattamento rispetto a quelle poste in essere nell'ambito delle attività di ordinaria gestione della clientela.

Sempre nel contesto dei contratti non richiesti, una decisione di analogo tenore è stata adottata il 12 ottobre 2023 (prov. n. 476, doc. web n. 9965217) nei confronti di un fornitore di energia di più limitate dimensioni; anche in questa ipotesi, era stata accertata la mancata adozione di adeguate misure tecnico-organizzative volte a garantire la legittimità dei trattamenti dei dati della clientela in fase di contrattualizzazione della stessa. Carezza quest'ultima che ha determinato il caricamento nei sistemi della società di circa 196 proposte contrattuali non richieste, corrispondenti – per il periodo di riferimento considerato dall'attività istruttoria – al 22% del totale di proposte contrattuali complessivamente acquisite dal fornitore per il tramite della propria rete di vendita porta a porta.

È stata pertanto rilevata l'illiceità del trattamento effettuato dalla società per la violazione degli artt. 5, par. 1, lett. a) e d) e par. 2 e 24 del RGPD e sono state prescritte diverse misure di natura correttiva volte ad imporre al titolare la predisposizione di

14

14

un sistema di controlli preventivi finalizzati a intercettare tempestivamente eventuali comportamenti scorretti e/o fraudolenti dei propri responsabili *ex art. 28 del RGPD* (nella specie, agenti porta a porta), già in una fase antecedente alla proposizione del reclamo da parte dei clienti. Contestualmente è stata applicata una sanzione pecuniaria di duecentomila euro.

14.5. Procedure IMI relative a trattamento di dati in ambito economico-produttivo

La partecipazione al sistema IMI previsto dal reg. (UE) 1024/2012, per la gestione dei meccanismi di cooperazione e coerenza di cui al Capo VII del RGPD, costituisce ormai un impegno rilevante per tutte le autorità di protezione dei dati del SEE (Spazio economico europeo).

Per quanto riguarda l'ambito economico, si sottolinea che le procedure IMI riguardano casistiche eterogenee riferite ad una variegata pluralità di titolari e responsabili del trattamento, considerata la granularità del settore di riferimento.

Si conferma nel 2023 la prevalenza delle procedure IMI volte all'identificazione dell'autorità capofila (ai sensi dell'art. 56, par. 1, del RGPD) e delle autorità interessate (ai sensi dell'art. 4 n. 22 del RGPD) in presenza di trattamenti transfrontalieri, che rappresentano circa il 80% delle procedure trattate.

Nel 2023 l'Autorità si è dichiarata "interessata" in 78 casi (32%) assumendo invece la posizione di autorità capofila in un numero limitato di casi riguardanti società con stabilimento unico o principale in Italia.

Per quanto concerne i reclami presentati al Garante nel 2023 ai sensi degli artt. 143 e ss. del Codice nei confronti di società con sede in altro Stato membro, per i quali si è reso necessario avviare le procedure di cooperazione applicabili provvedendo a trasmettere la relativa documentazione alla competente autorità capofila, si segnalano: un reclamo con il quale è stato lamentato che nel creare un *account* su un *app leader* a livello mondiale per la salute e il *fitness* l'interessato è stato costretto ad acconsentire al trasferimento dei propri dati verso gli Stati Uniti e altri Paesi con leggi diverse sulla protezione dei dati, esprimendo un consenso che non soddisferebbe i requisiti del RGPD; un altro reclamo in cui è stato lamentato che nel corso della procedura di recupero della *password* su un sito di una società italiana il *browser* del PC del reclamante avrebbe incorporato il sistema di verifica reCAPTCHA comportando un trasferimento automatico dei dati dell'interessato verso gli Stati Uniti, senza che egli avesse manifestato alcun consenso in merito; infine, un reclamo che ha avuto a oggetto la richiesta a una banca con sede nel Lussemburgo di accedere ai dati ostativi all'emissione di una carta di credito e contestualmente ottenere la cancellazione dei dati.

Rimane sostanzialmente stabile, rispetto al 2022, il numero delle procedure IMI di consultazione informale previste dall'art. 60, par. 1, del RGPD. A questo proposito si rileva come le autorità di protezione dei dati abbiano ormai compreso l'importanza, più volte ribadita dal CEPD, e in particolare nelle linee guida 2/2022 sull'applicazione dell'art. 60 del RGPD, di ricorrere a tale procedura volta a consentire lo scambio, fra l'autorità di controllo capofila e le autorità interessate, di informazioni, valutazioni e documenti relativi alla controversia prima della fase decisoria vera e propria.

Sono invece lievemente aumentate, rispetto al 2022, le procedure di cooperazione giunte alla fase decisoria nel settore privato. Rispetto ai progetti di decisione caricati sulla piattaforma IMI dalle competenti autorità capofila si è ritenuto, complessivamente, di condividerli limitandosi, ove opportuno, a sollevare solo commenti o richieste di chiarimenti. Si segnala, inoltre, un caso in cui l'interessata aveva lamentato

una possibile violazione del diritto di accesso a seguito di un presunto *data breach*; il Garante (autorità che ha ricevuto il reclamo), dopo aver condiviso la linea decisa dall'autorità capofila di archiviare il caso non essendo stata rilevata la violazione dell'art. 15, ha adottato, *ex art.* 60.8 del RGPD, il provvedimento finale di rigetto (provv. 23 marzo 2023, n. 92, doc. web n. 9885177).

Riguardo ai casi in cui l'Autorità si è dichiarata capofila in relazione a casi aventi rilevanza transfrontaliera trasmessi da altre autorità europee di protezione dati, sono state avviate istruttorie (con relativi scambi di informazioni con le altre autorità interessate) relativamente a una serie di reclami o segnalazioni nei confronti di società con sede principale in Italia (a titolo esemplificativo, piattaforme di comparazione prezzi, *e-commerce*, noleggio di auto), nei quali gli interessati hanno lamentato principalmente il mancato esercizio dei diritti di accesso o cancellazione o la possibile violazione di dati personali.

In un caso avente a oggetto il reclamo proposto da un cittadino austriaco nei confronti di una piccola società con sede in Italia operante nel settore editoriale e di sviluppo di siti web, volto a ottenere la cancellazione dei dati dell'interessato, il Garante ha proposto, attraverso la procedura IMI di consultazione informale *ex art.* 60, di definire amichevolmente la controversia, senza l'adozione di misure correttive/sanzionatorie. Nel caso concreto, infatti, si è ritenuto che ricorressero i presupposti per un *amicable settlement* previsti dalle linee guida del CEPD 6/2022 sull'attuazione pratica delle composizioni amichevoli, e in particolare: esercizio di un diritto (cancellazione) e corrispondente obbligo adempiuto da parte del titolare, anche grazie all'intervento dell'Autorità; numero limitato di interessati coinvolti e di dati trattati; natura non sistematica della violazione ed effetti lievi della stessa; soddisfacimento dell'interessato (che non ha sollevato ulteriori rilievi). Il Garante, in qualità di autorità capofila, ha, quindi, condiviso il proprio progetto di decisione con le altre autorità interessate che non hanno sollevato obiezioni pertinenti e motivate ai sensi dell'art. 60, par. 4; è stata successivamente adottata la decisione finale con definizione amichevole della controversia e chiusura del procedimento ai sensi dell'art. 60, par. 7.

Per quanto riguarda l'assistenza reciproca fra le autorità di controllo *ex art.* 61 del RGPD, sempre con riferimento all'ambito economico, si conferma l'utilizzo della relativa procedura IMI allo scopo di ottenere informazioni sulle normative nazionali in tema di protezione dei dati o su questioni relative all'applicazione di particolari disposizioni del RGPD. In particolare, è stata fornita risposta ad alcune richieste di assistenza reciproca in tema di: *data retention* dei dati relativi agli acquisti nell'ambito di programmi di fidelizzazione; registrazione delle telefonate dei clienti; registrazione dei dati dei dipendenti; sistema di pagamento *Google Pay*; modalità di autenticazione nei sistemi di pagamento *online*; normativa antiriciclaggio; recupero crediti; installazione di impianti di videosorveglianza nei condomini; riprese video attraverso l'uso di *dashcam*.

Infine, in data 4 luglio 2023, è stata presentata dalla Commissione europea la proposta di regolamento recante norme procedurali aggiuntive nel contesto del meccanismo dello sportello unico in relazione al quale il CEPD ed il GEPD hanno adottato un parere congiunto il 20 settembre 2023 (cfr. cap. 21). In merito, occorre evidenziare che il nuovo quadro regolatorio, una volta concluso l'*iter* di approvazione, non solo comporterà la necessità di adattare la piattaforma IMI ai requisiti previsti dalle nuove norme procedurali ma avrà anche un immediato impatto sulle disposizioni procedurali nazionali applicabili nella trattazione dei casi aventi rilevanza transfrontaliera.

14

15 Altri trattamenti in ambito privato

15.1. *Trattamento di dati personali nell'ambito del condominio*

Anche nel 2023 si è registrato un significativo afflusso di istanze relative all'ambito condominiale, in prevalenza relative ad argomenti già esaminati e definiti in passato e precipuamente alla questione relativa alla circolazione dei dati tra i partecipanti alla compagine condominiale.

In merito alla possibilità di comunicare ad altri condòmini, da parte degli amministratori di condominio, i dati personali dei singoli partecipanti alla compagine condominiale, l'Ufficio, richiamando il provvedimento generale del Garante del 18 maggio 2006 (doc. web n. 1297626) (per i profili compatibili con il novellato quadro di riferimento), ha chiarito nuovamente che possono formare oggetto di lecito trattamento da parte del condominio (con l'ausilio, di regola, dell'amministratore nell'eventuale veste di responsabile del trattamento) i soli dati pertinenti e non eccedenti la finalità di amministrazione e gestione del condominio; in particolare, è stato ribadito (cfr. *ex multis*, nota 20 ottobre 2023) che non sono di regola conoscibili dai partecipanti alla compagine condominiale, se non in presenza di un idoneo presupposto di liceità, i dati – quali le utenze telefoniche e/o gli indirizzi *e-mail* (v., in proposito, *Vademecum* “Il Condominio e la *privacy*” del 10 ottobre 2013, doc. web n. 2680240) – che, pur potendo agevolare (specie in casi di necessità e urgenza) i contatti tra gli interessati e/o lo svolgimento delle incombenze gravanti sull'amministratore, non sono tuttavia funzionali alla determinazione dei diritti o degli oneri relativi al bene comune.

Nella stessa prospettiva, sono state fornite indicazioni in merito alla pubblicazione di documenti contenenti dati personali (nota 20 luglio 2023). Muovendo dal consolidato principio secondo cui non possono essere di regola diffusi – integrando, quindi, “un trattamento illecito (anche in violazione del principio di proporzionalità)” – i dati personali contenuti in avvisi, comunicati o altri documenti affissi in spazi accessibili al pubblico, “potendo tali informazioni venire a conoscenza di una serie indeterminata di soggetti, nell'intervallo di tempo in cui l'avviso risulta visibile”, il Garante ha ribadito che è necessario prestare la massima cautela alla pubblicazione di documenti in spazi condominiali pubblicamente accessibili, dovendosi in proposito adottare, “se del caso anche a cura dell'amministratore del condominio, idonee misure di sicurezza” atte a evitare l'indebita conoscibilità di dati relativi agli interessati (ad esempio, pubblicando solo avvisi di carattere generale, ovvero privi di dati personali riferiti a singoli soggetti identificati o identificabili).

Altra questione rilevante, già trattata in passato dall'Autorità (cfr. Relazione 2015, p. 130, e 2022, p. 155), ha riguardato la possibilità di accedere ai dati del registro dell'anagrafe condominiale.

L'Ufficio, nel richiamare ancora una volta due pronunce di merito in materia di accessibilità da parte dei singoli condòmini al registro dell'anagrafe condominiale (Trib. Palermo n. 2514/2021; Trib. Brescia n. 2177/2018), ha ribadito che “la conoscibilità delle informazioni concernenti i partecipanti alla compagine condominiale deve restare impregiudicata qualora ciò sia conforme alla disciplina civilistica o comunque sia prevista in base ad altre norme presenti nell'ordinamento, purché sussistano i relativi presupposti fissati dalla legge”, ferma restando l'accessibilità del registro in questione nei termini indicati dalla medesima disciplina civilistica

(art. 1129, comma 2, c.c.) (nota 14 luglio 2023). L'Autorità ha altresì ricordato che le informazioni personali riferibili a ciascun condòmino possono essere trattate per la finalità di gestione ed amministrazione del condominio e che possono essere trattati anche dati personali di natura sensibile o dati giudiziari in misura strettamente funzionale al perseguimento delle medesime finalità. In particolare le informazioni relative ai singoli condòmini possono essere comunicate a terzi solo con il consenso espresso degli interessati, ovvero in presenza di altro presupposto di liceità individuato nell'art. 6 del RGPD e comunque nel rispetto dei principi generali di cui all'art. 5 del RGPD.

All'esito della trattazione di un reclamo con cui veniva lamentata l'affissione presso gli androni delle sette scale di un supercondominio di un atto di diffida, indirizzato ai reclamanti e contenente anche taluni dati personali degli interessati, il Garante ha ricordato che le bacheche condominiali sono utilizzabili per avvisi di carattere generale e non per comunicazioni che comportano l'uso dei dati personali riferibili a singoli condòmini. Per comunicazioni individualizzate è, invece, necessario fare ricorso a modalità alternative che scongiurino il rischio che soggetti terzi vengano a conoscenza delle informazioni relative ai singoli condòmini o affittuari (nota 9 novembre 2023).

Nel definire un reclamo con il quale è stato lamentato l'invio di comunicazioni di posta elettronica con l'indirizzo *e-mail* degli interessati in chiaro, l'Autorità ha richiamato l'amministratore *pro tempore* del condominio a una scrupolosa osservanza della disciplina in materia di protezione dati, con invito ad astenersi dal porre in essere ulteriori operazioni di trattamento di dati non conformi a questi ultimi. Pur essendo il contenuto delle *e-mail* oggetto di contestazione afferente a temi concernenti la gestione e l'amministrazione del condominio, l'utilizzo "cumulativo" e "in chiaro" degli indirizzi di posta elettronica degli interessati senza la previa adozione di idonei accorgimenti atti a impedire la reciproca conoscibilità dei dati da parte dei destinatari del messaggio – quali, ad es., la funzione ccn (copia conoscenza nascosta) – non risulta conforme ai principi in materia di protezione dati (nota 24 novembre 2023).

Si segnala infine il provvedimento 23 marzo 2023, n. 91 (doc. web n. 9885127) adottato a seguito di un reclamo concernente la contestata comunicazione di alcune informazioni sullo stato di salute dei reclamanti da parte dell'amministratore del condominio. Quest'ultimo, infatti, avendo appreso che i due reclamanti avevano contratto il *virus* da Covid-19, aveva inviato una *e-mail* a tutti i condòmini informandoli di tale particolare circostanza.

L'Autorità ha quindi accertato in capo all'amministratore del condominio la violazione dell'art. 9, parr. 1 e 2 del RGPD, avendo trattato i predetti in assenza di qualsiasi presupposto di legittimità. In particolare, l'Autorità ha chiarito che la deroga al trattamento di categorie particolari di dati personali (quali quelli oggetto del trattamento *de quo*) ricorre solo nei casi tassativamente previsti dall'art. 9, par. 2, del RGPD e non era stata intaccata dalla normativa d'urgenza conseguente all'emergenza epidemiologica da Covid-19, cosicché è rimasto immutato il divieto, da parte di qualsiasi soggetto pubblico o privato, di diffondere, attraverso siti web o altri canali, e di comunicare (come nel caso di specie) i nominativi dei casi accertati di Covid-19 o dei soggetti sottoposti alla misura dell'isolamento per finalità di contenimento della diffusione dell'epidemia.

L'Autorità ha deciso su un reclamo presentato da un interessato che aveva lamentato l'installazione di alcune telecamere nel proprio condominio senza che fosse stata adottata una delibera assembleare.

Al riguardo va tenuto conto che, in conformità all'art. 1122-ter c.c. (introdotto dalla legge di riforma del condominio con la l. 11 dicembre 2012, n. 220), in combinato disposto con l'art. 1130, comma 1, punto 1, c.c., l'installazione di impianti di videosorveglianza in ambito condominiale è subordinata ad una decisione assunta

15

Videosorveglianza nel
condominio

15

dai condòmini con delibera assembleare, da eseguire a cura dell'amministratore in virtù del mandato ricevuto.

Nel corso dell'istruttoria, svolta con l'intervento del Nucleo tutela *privacy* della Guardia di finanza, è stata acquisita documentazione idonea a comprovare che, effettivamente, l'installazione delle menzionate telecamere era stata disposta direttamente dall'amministratore, in assenza di una delibera condominiale e che l'amministratore si era limitato a comunicare l'intenzione di installare un sistema di videosorveglianza idoneo alla tutela dello spazio condominiale esterno, invitando i condòmini a produrre preventivi in occasione di una successiva assemblea.

L'Autorità ha avuto modo di chiarire che la delibera condominiale rappresenta il presupposto necessario per la liceità del trattamento realizzato mediante l'installazione di videocamere in spazi condominiali. Infatti, mediante tale atto, i condòmini concorrono a definire le caratteristiche principali del trattamento, andando a individuare le modalità e le finalità del trattamento stesso, i tempi di conservazione delle immagini riprese, l'individuazione dei soggetti autorizzati a visionare le immagini. Nel caso in esame, era risultato inoltre che l'amministratore del condominio, oltre all'installazione delle telecamere, aveva deciso anche il loro angolo visuale e si era dotato di un'applicazione per visionare le immagini direttamente sul proprio *smartphone*, previo inserimento di credenziali di autenticazione a lui solo conosciute. Tali circostanze, esaminate nel loro complesso, hanno permesso di individuare l'amministratore (e non il condominio) come titolare del trattamento.

Ne è derivato che il trattamento dei dati personali in questione era stato effettuato dall'amministratore in assenza di un idoneo presupposto di liceità, ai sensi dell'art. 6 del RGPD. Il Garante ha quindi dichiarato illecito il trattamento perché effettuato in violazione dei principi generali di liceità, correttezza e trasparenza (art. 5, par. 1, lett. a), del RGPD nei confronti di tutti gli interessati (condòmini e non) nonché in assenza di un idoneo presupposto di legittimità ai sensi dell'art. 6 del RGPD (provv. 26 ottobre 2023, n. 502, doc. web n. 9960920).

Sempre in riferimento al trattamento dei dati effettuato dalle compagini condominiali mediante sistemi di videosorveglianza per il controllo delle aree comuni, sono state fornite indicazioni in relazione al profilo della legittimazione del titolare del trattamento a comunicare a soggetti terzi le immagini registrate, specificando che tale comunicazione può essere lecitamente effettuata solo in presenza di adeguati presupposti e sulla base di un'adeguata base giuridica.

Occorre, in particolare, verificare se il trattamento sia effettuato solo per finalità di tutela delle cose comuni o anche per finalità di tutela dei beni dei terzi. In questo secondo caso la (eventuale) comunicazione dei dati del terzo ripreso dalle telecamere potrebbe essere ammissibile e la base giuridica potrebbe essere individuata nel perseguimento di un legittimo interesse anche di terzi, a condizione però che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (art. 6, par. 1, lett. f)). Resta fermo, tuttavia, che l'eventuale comunicazione di dati nei termini sopra definiti resta una mera facoltà del titolare e non configura un diritto dell'interessato (nota 28 settembre 2023).

15.2. *Trattamento di dati da parte di associazioni e fondazioni*

In materia di trattamenti di dati personali effettuati da associazioni e partiti politici, numerosi reclami hanno riguardato il mancato riscontro da parte dei titolari del trattamento alle istanze presentate dagli interessati ai sensi degli artt. 15 e ss. del RGPD.

All'esito di un'istruttoria avviata a seguito di un reclamo, il Garante ha adottato un provvedimento di ammonimento nei confronti di un'associazione che aveva dichiarato

all'interessato, in risposta alla sua specifica richiesta, di aver provveduto alla cancellazione dei suoi dati personali, ma gli aveva poi inviato un'ulteriore *e-mail* relativa alla comunicazione del rinnovo automatico della sua iscrizione all'associazione.

Alla luce delle circostanze che avevano determinato il ritardo nel riscontro all'interessato e delle azioni intraprese dal titolare del trattamento, il Garante ha ritenuto di qualificare il caso come violazione minore, ai sensi dell'art. 83, par. 2 e del cons. 148 del RGPD (prov. 31 agosto 2023, n. 365, doc. web n. 9936247).

L'Autorità si è altresì pronunciata sul trattamento di alcuni dati personali del reclamante, raccolti da un comitato locale in occasione della sottoscrizione di una petizione diretta al sindaco del suo comune di residenza e al presidente della provincia e successivamente diffusi attraverso un *post* pubblicato sulla pagina Facebook di una lista civica collegata al sindaco; nel *post* era stato riportato il nominativo e il ruolo politico del reclamante quale firmatario della citata petizione al fine di screditarlo rispetto alla problematica della chiusura/apertura delle scuole durante il periodo pandemico e all'assunzione – nell'arco di pochi giorni – di posizioni diametralmente opposte.

All'esito dell'attività istruttoria, nel corso della quale la lista civica ha dichiarato di avere rimosso il *post* oggetto di reclamo, l'Autorità, pur prendendo atto della notorietà politica dell'interessato e della sua partecipazione al dibattito politico oggetto della petizione, ha riconosciuto l'illiceità del trattamento effettuato dalla predetta lista civica nei cui confronti ha adottato un provvedimento di ammonimento.

L'Autorità ha ritenuto che, nel caso di specie, rilevassero non tanto i principi concernenti i trattamenti effettuati per finalità giornalistiche e altre manifestazioni del pensiero, come richiamati dal titolare del trattamento nella sua articolata memoria difensiva (artt. 136 e ss. del Codice), bensì il fatto che la lista civica, data la "contiguità politica" con il sindaco e con gli esponenti di maggioranza in consiglio comunale, avesse trattato i dati personali dell'interessato – acquisiti dai predetti soggetti per lo svolgimento delle funzioni istituzionali – per una finalità propria e in assenza di idonei presupposti di liceità, nonché in violazione del principio generale di liceità, correttezza e trasparenza di cui all'art. 5, par. 1 lett. a), del RGPD (prov. 13 aprile 2023, n. 131, doc. web n. 9892911).

In un altro caso l'Autorità si è espressa su un reclamo concernente la divulgazione di un comunicato stampa relativo alla cancellazione dei reclamanti dall'elenco degli iscritti a un partito politico, in assenza del loro consenso, ritenendo prevalente la tutela del legittimo interesse del menzionato partito sottesa alla suddetta comunicazione rispetto ai contrapposti interessi degli interessati, in ragione dello specifico contesto di riferimento.

Ha infatti osservato che il trattamento dei dati degli interessati a opera del partito era stato posto in essere in base agli atti statutari dell'organizzazione e che la scelta di comunicare pubblicamente le determinazioni assunte rispondeva alla necessità di dare una corretta informazione ai propri elettori e simpatizzanti nel contesto delle scelte che questi erano chiamati a effettuare in occasione delle allora imminenti consultazioni elettorali amministrative. Tale circostanza, corroborata dalla presentazione e dalla candidatura dei reclamanti in liste elettorali concorrenti non sostenute dal partito in questione, in un contesto locale di limitate dimensioni, avrebbe, verosimilmente, potuto indurre l'elettorato del partito a sostenere erroneamente candidati non più riconducibili politicamente a quest'ultimo.

È stato altresì evidenziato che l'appartenenza politica dei reclamanti poteva intendersi già nota presso l'opinione pubblica locale per effetto della loro militanza e delle cariche ricoperte da diversi interessati al momento della "sospensione", ricorrendo quindi la condizione prevista dall'art. 9, par. 1, lett. e), del RGPD. Pertanto, la diffusione del comunicato in questione è risultata funzionale alla trasparenza e alla

15

15

corretta informazione della comunità locale chiamata a rinnovare i rappresentanti dell'amministrazione comunale, risultando, altresì, evidenti la preminenza della tutela dei terzi elettori e il legittimo interesse degli stessi a esercitare il voto consapevolmente e a esprimere la propria preferenza politica (nota 7 giugno 2023).

A seguito di una istanza formulata da un'associazione sindacale, nonché da alcuni singoli aderenti alla stessa, l'Autorità è intervenuta sul trattamento di dati posto in essere mediante comunicazioni effettuate via *e-mail* in ambito associativo.

Più nel dettaglio, i reclamanti – per lo più iscritti all'associazione sindacale che aveva presentato la segnalazione, ma anche soggetti che rivestivano in seno alla stessa diversi incarichi – avevano lamentato l'illecito utilizzo, da parte di un'organizzazione sindacale diversa da quella di appartenenza, dei loro indirizzi di posta elettronica. La suddetta organizzazione aveva ripetutamente inviato a tali recapiti personali diverse comunicazioni che recavano messaggi di vario tenore, in larga parte di carattere informativo in ordine ad iniziative assunte dalla stessa nell'ambito dello svolgimento della propria attività sindacale, coinvolgendo un cospicuo numero (circa 150) di soggetti terzi i cui indirizzi erano contenuti nelle *mailing list*.

All'esito dell'attività istruttoria – nel corso della quale l'associazione non ha fornito indicazioni in ordine ai presupposti di legittimità e alle finalità del trattamento oggetto di contestazione, né chiarimenti su come siano stati reperiti i recapiti degli interessati – è stato rilevato che l'associazione in questione aveva posto in essere un illecito trattamento dei dati personali degli istanti.

In particolare, partendo dal presupposto che il dato consistente in un indirizzo *e-mail* ha natura personale (cfr. art. 4, n. 1, del RGPD; v. anche WP 136 - parere 4/2007 sul concetto di dato personale del Gruppo *ex Art.* 29 del 20 giugno 2007), l'Autorità ha in primo luogo constatato che la trasmissione delle comunicazioni oggetto di contestazione agli indirizzi di posta elettronica dei sopra citati destinatari aveva avuto luogo in assenza del previo consenso di quest'ultimi (o comunque in mancanza di altra idonea base giuridica prevista dall'art. 6, par. 1, del RGPD).

Inoltre è stato accertato che tale trasmissione aveva avuto luogo mediante un unico invio rivolto a un numero plurimo e indifferenziato di interessati i cui dati personali – nella fattispecie, gli indirizzi *e-mail* – risultavano visibili in chiaro. Tutto ciò aveva invero comportato la reciproca ed illecita comunicazione degli indirizzi di posta elettronica di tutti i destinatari coinvolti nelle *e-mail* oggetto di contestazione, tra i quali erano ricompresi gli istanti. Tale trasmissione avrebbe potuto avere luogo in forma individualizzata, consentendo così di prevenire una indebita comunicazione di dati personali a soggetti diversi dal singolo destinatario (v., in tal senso, provv. ti 30 novembre 2005, doc. web n. 1213644; 26 novembre 2006, doc. web n. 1364099 e 18 maggio 2006, doc. web n. 1297626), o comunque avrebbe potuto essere effettuata mediante l'adozione da parte dell'associazione di opportuni accorgimenti atti a impedire la conoscibilità dei dati dei vari destinatari dei messaggi, ad es. utilizzando la funzione cd. copia conoscenza nascosta (v. provv. 4 luglio 2013, doc. web n. 2542348 e provv. 9 gennaio 2020, doc. web n. 9261234).

L'Autorità ha pertanto provveduto, sulla base dei criteri indicati dall'art. 83 del RGPD, a sanzionare l'associazione in questione per violazione delle disposizioni contenute nell'art. 5, par. 1, lett. a) e f), del RGPD, nonché nell'art. 6, par. 1, lett. a), del RGPD (provv. 13 aprile 2023, n. 130, doc. web n. 9892716).

Nel 2023 sono pervenute alcune istanze in materia di cd. "sbattezzo". In particolare, sono stati segnalati alcuni mancati riscontri, da parte di talune parrocchie, alle richieste di rettifica/cancellazione avanzate dagli interessati in merito ai dati personali contenuti nel registro dei battezzati e di annotazione della loro volontà di non appartenere più alla Chiesa cattolica apostolica romana.

Nel rappresentare che il tema della cancellazione dei dati personali in ambito

confessionale aveva già formato oggetto di disamina da parte del Garante (cfr. in particolare provv. 13 settembre 1999, doc. web n. 1090502, confermato da Trib. Padova, sez. I civ. 26 maggio 2000, n. 3531/99), si è altresì ribadito, in termini generali, che “il battesimo non è solo un atto di carattere confessionale, ma anche un atto giuridico costitutivo che segna l’ingresso di una persona nella Chiesa cattolica” e che pertanto non può essere chiesta la cancellazione di un’informazione ineliminabile “se non a costo di modificare la stessa rappresentazione della propria realtà”.

Fermo restando quanto sopra, il Garante è comunque intervenuto nei casi in cui le richieste di rettifica/annotazione erano rimaste inevase, contattando le parrocchie di riferimento e invitandole, tanto alla luce dell’art. 16 del RGPD che degli artt. 3, par. 1, lett. d) e 7, par. 2, del decreto generale approvato dalla CEI in data 24 maggio 2018 (il quale stabilisce il diritto di chiedere la correzione dei dati personali qualora errati o non aggiornati, con obbligo per il titolare di adottare “tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati”) di fornire adeguato riscontro agli interessati (nota 17 febbraio 2023).

Di particolare interesse è stato anche il riscontro fornito a un segnalante in merito al trattamento dei propri dati personali effettuato dalla Congregazione Cristiana dei Testimoni di Geova.

L’istante aveva lamentato che, in occasione di un’adunanza pubblica, i cd. anziani avrebbero divulgato informazioni relative alla sua fuoriuscita dalla Congregazione, subendone per l’effetto le conseguenze sul piano dei rapporti con gli altri aderenti (cd. ostracismo). Richiamando il proprio provvedimento del 25 febbraio 2021 (doc. web n. 9574136), il Garante ha chiarito che la Congregazione Cristiana dei Testimoni di Geova è una confessione religiosa riconosciuta quale ente morale con personalità giuridica e, come tale, legittimata a trattare i dati personali degli aderenti in conformità alla propria organizzazione interna e ai principi di culto cui la stessa si ispira. In tale quadro, i dati personali degli aderenti possono essere lecitamente trattati dalla Congregazione per lo svolgimento delle molteplici attività connesse al culto e all’assistenza spirituale dei fedeli, ivi compreso il trattamento dei medesimi dati per “il migliore conseguimento dei propri fini di religione e di culto” (art. 3 dello statuto della Congregazione; v. pure l’“Informativa globale dei testimoni di Geova in materia di trattamento dei dati personali” e l’“Informativa al trattamento dei dati personali – Italia”, disponibili sul sito della Congregazione).

Muovendo da tali premesse, l’Autorità, nel ricordare le condizioni di liceità dei trattamenti svolti dalla Congregazione (artt. 6, par. 1, lett. f) e 9, par. 2, lett. d), del RGPD), ha quindi ritenuto che i trattamenti effettuati dalle relative articolazioni territoriali e dagli organi religiosi e ministri di culto della stessa in conformità alle proprie prassi interne – che possono ricomprendere, tra l’altro, anche i cd. annunci pubblici – e nel rispetto dei precetti e dei principi dalla stessa divulgati, non fossero in contrasto con la disciplina in materia di protezione dei dati personali, sia perché le correlate operazioni di trattamento si sarebbero svolte nel rispetto delle attività di fede professate dall’organizzazione, secondo le disposizioni dottrinali e catechistiche proprie dello stesso ordine confessionale, sia perché non vi era prova che le informazioni trattate dalla Congregazione fossero circolate al di fuori della comunità.

È stata infine rappresentata (anche alla luce di quanto stabilito da Trib. Roma 23 maggio 2021, RGN 76320/2016, in merito al riconoscimento del diritto della confessione religiosa di informare la propria comunità sulla cessazione dello stato di appartenenza di un suo (ex) membro), l’assenza di idonei presupposti per ulteriori iniziative da parte dell’Ufficio nonché la facoltà per l’interessato di far valere in altra sede competente eventuali e ulteriori profili controversi (artt. 57 del RGPD e 154 del Codice) (nota 31 marzo 2023).

15

15

**Videosorveglianza in
ambito commerciale o
professionale**

15.3. Videosorveglianza nel settore privato

Nel 2023 i trattamenti di dati effettuati tramite sistemi di videosorveglianza da parte di soggetti privati sono stati oggetto di un significativo numero di reclami e segnalazioni.

Sono state numerose le violazioni in tale ambito commesse da esercizi commerciali, in particolare di medie-piccole dimensioni, segnalate da clienti e dalla polizia locale intervenuta per controlli di competenza.

Le violazioni più frequentemente rilevate hanno riguardato: telecamere esterne con un angolo ripresa troppo ampio, esteso a luoghi pubblici o ad aree riferibili ad altri soggetti privati, comunque ben oltre l'area di pertinenza immediatamente prospiciente l'esercizio commerciale; telecamere che inquadrano gli spazi interni del negozio, installate a tutela del patrimonio, ma senza richiedere la preventiva autorizzazione all'Ispettorato territoriale del lavoro o provvedere con gli adempimenti alternativi previsti dallo Statuto dei lavoratori; mancata apposizione di idonei cartelli informativi che segnalano la presenza delle telecamere.

Si tratta di adempimenti che potrebbero essere assolti dal titolare dell'esercizio commerciale con uno sforzo (anche economico) minimo, ma che sono spesso sottovalutati e, in caso di violazione, possono condurre a sanzioni sia di tipo amministrativo che di tipo penale.

Si menzionano di seguito alcuni dei numerosi provvedimenti sanzionatori adottati, in continuità con gli orientamenti già consolidati negli anni precedenti, nei confronti di alcune imprese individuali e di alcune società che avevano effettuato trattamenti di dati personali per mezzo di impianti di videosorveglianza in violazione.

Con il provvedimento 8 giugno 2023, n. 244 (doc. web n. 9917900) l'Autorità ha sanzionato una società per aver installato un impianto di videosorveglianza non adeguatamente segnalato mediante l'apposizione di appositi cartelli recanti l'informativa di cui all'art. 13 del RGPD. Inoltre, dall'accertamento ispettivo è risultato che presso i locali della società erano presenti "sei telecamere di cui due all'interno del capannone e quattro poste a sorveglianza delle aeree esterne" in grado di riprendere l'attività lavorativa dei dipendenti senza che fossero state attivate le procedure previste dall'art. 4 della l. n. 300/1970 e che alcune telecamere erano in grado di riprendere anche la strada pubblica. Il Garante ha pertanto adottato un'ordinanza-ingiunzione ordinando alla società di pagare una somma di denaro a titolo di sanzione amministrativa pecuniaria e ha prescritto alla società di conformare il trattamento alle disposizioni in materia di protezione dei dati personali oggetto di violazione.

Con provvedimento 6 luglio 2023, n. 293 (doc. web n. 9920881), il Garante ha sanzionato una società la quale, sulla base dell'accertamento effettuato dalla Guardia di finanza, aveva installato un impianto di videosorveglianza presso la propria sede, idoneo a riprendere la strada pubblica, in assenza di apposti i cartelli recanti l'informativa di cui all'art. 13 del RGPD e senza aver adottato le misure di garanzia di cui al menzionato art. 4 della l. n. 300/1970, richiamato dall'art. 114 del Codice, in relazione al personale dipendente. Avendo la società cooperato con l'Autorità nel corso del procedimento, modificando l'angolo di ripresa delle telecamere, predisponendo idonei cartelli informativi e conformandosi alle procedure di garanzia previste dalla l. n. 300/1970, la stessa è stata sanzionata a pagare una somma di denaro a titolo di sanzione amministrativa pecuniaria senza la previsione di alcuna prescrizione a suo carico.

L'Autorità si è occupata anche delle implicazioni di un progetto, avviato da una società di telecomunicazioni, per l'utilizzo di droni al fine di mappare e individuare aree del territorio nazionale idonee all'installazione di antenne per la telefonia 5G. Nel caso specifico, segnalato da alcuni cittadini, non sono emerse violazioni in

materia di protezione dati. A ogni modo, il Garante ha invitato la società ad adottare tutte le misure tecniche e organizzative necessarie per far sì che il proprio personale, nonché i fornitori e sub-fornitori esterni incaricati di valutare siti idonei all'uso, operino correttamente nel trattare dati personali accidentalmente acquisiti tramite l'uso di droni, anche se non memorizzati, impartendo opportune istruzioni, anche per iscritto, a tutti i soggetti coinvolti e provvedendo, ove necessario, a integrare al riguardo i contratti sottoscritti con le società *partner* e con i fornitori.

La società nei termini previsti si è impegnata a effettuare le riprese in orari poco frequentati e solo dopo aver accertato che le aree oggetto di verifica non siano frequentate da individui che potrebbero, anche solo in via incidentale, essere oggetto di video-riprese; i droni, inoltre, effettueranno le riprese solo a un'altezza minima di ventiquattro metri e solo parallelamente al suolo. La società, infine, si è impegnata a pubblicare una dettagliata informativa sul trattamento dei dati personali sul proprio sito web e a procedere a un'ulteriore verifica in *back office* delle immagini che dovessero ritrarre soggetti, direttamente o indirettamente, identificabili. L'Autorità ha definito l'istruttoria con nota 7 agosto 2023 prendendo favorevolmente atto delle misure poste in essere, adottate e comunicate entro i termini richiesti.

In materia di sistemi di videosorveglianza installati in ambito privato, meritano particolare attenzione alcuni provvedimenti adottati nei confronti di persone fisiche.

Sebbene, infatti, in via generale, la disposizione di cui all'art. 2, par. 2, del RGPD escluda dall'ambito di applicazione della disciplina in materia di protezione dei dati personali il trattamento effettuato da una "persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico", nei casi in argomento l'Autorità non solo ha invece ritenuto applicabile la disciplina generale, ma ha anche rilevato la mancanza di idonei presupposti di legittimità alla base dei relativi trattamenti posti in essere.

Non è infatti possibile invocare l'esclusione prevista dall'art. 2, par. 2, del RGPD, ove l'ambito di comunicazione dei dati ecceda la sfera familiare del titolare, oppure le immagini siano oggetto di comunicazioni a terzi o di diffusione, oppure qualora il trattamento si estenda oltre gli ambiti di stretta pertinenza riprendendo immagini in aree comuni (anche di tipo condominiale quali scale, androni, parcheggi), luoghi aperti al pubblico (vie o piazze), o aree di pertinenza di terzi (giardini, terrazzi, porte o finestre di pertinenza di terzi).

Soltanto in presenza di situazioni di rischio effettivo il titolare del trattamento può, sulla base di un legittimo interesse, estendere la ripresa delle videocamere anche ad aree che esulano dalla propria esclusiva pertinenza. In tali casi il titolare del trattamento è tenuto al rispetto delle disposizioni in materia di protezione dati personali, anche alla luce delle linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate dal CEPD e del provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680).

Il Garante ha in particolare adottato il provvedimento 27 aprile 2023, n. 173 (doc. web n. 9896468), con cui ha accertato l'illiceità del trattamento effettuato da una persona fisica che aveva installato telecamere a tutela della proprietà privata che, tuttavia, erano orientate in modo tale da riprendere anche spazi pubblici e proprietà di terzi. Considerato che, nel corso dell'istruttoria, il titolare del trattamento non aveva dimostrato la sussistenza di un legittimo interesse riferito a una situazione di rischio effettivo che avrebbe giustificato tale trattamento, ne è derivata l'applicazione di una sanzione amministrativa pecuniaria, oltre all'indicazione di un congruo periodo di tempo entro cui conformare il trattamento ai principi generali.

Una motivazione simile a quella sinteticamente sopra riportata è contenuta nel provvedimento di ammonimento adottato dal Garante nei confronti di un'azienda agricola il cui sistema di videosorveglianza, installato anche a protezione

15

Provvedimenti nei
confronti di persone
fisiche

15

dell'abitazione privata del titolare del trattamento, è risultato potenzialmente idoneo a riprendere anche le aree di proprietà e di pertinenza dei reclamanti (prov. 2 marzo 2023, n. 59, doc. web n. 9872567). In considerazione dell'attività posta in essere dal titolare del trattamento nel corso del procedimento, il caso è stato qualificato come "violazione minore", ai sensi dell'art. 83, par. 2 e del cons. 148 del RGPD.

Con provvedimento 18 luglio 2023, n. 319 (doc. web n. 9935503), adottato a conclusione di un procedimento avviato a seguito di reclamo, l'Autorità ha rilevato un trattamento illecito di dati personali effettuato attraverso un sistema di riprese video idoneo a riprendere la pubblica via in assenza di presupposti di liceità del trattamento e, pertanto, ha ritenuto necessario ingiungere al titolare del trattamento l'adozione delle misure necessarie a circoscrivere la ripresa alle sole aree di stretta pertinenza, nonché il pagamento della somma di euro 400,00 a titolo di sanzione amministrativa pecuniaria.

Similmente, in un caso segnalato dalla polizia municipale del Comune di Arezzo, il Garante ha adottato un provvedimento di ammonimento nei confronti di un soggetto privato che sulla parte esterna dell'immobile aveva installato due telecamere idonee a riprendere la pubblica via. Le telecamere erano state installate per controllare l'autovettura parcheggiata nel posto auto assegnato al titolare del trattamento, ma di fatto riprendevano anche la strada pubblica adiacente e parte di aree di sosta pubbliche. A seguito dell'adozione di maschere di oscuramento la ripresa è stata circoscritta all'area di parcheggio dell'autovettura (prov. 28 settembre 2023, n. 429, doc. web n. 9947775).

Infine l'Autorità ha rilevato che sul muro esterno di proprietà di un soggetto privato era stata installata una telecamera idonea a riprendere l'area pubblica antistante dove si trovano un parco giochi e una piazza. Tale telecamera, oltre a riprendere le immagini, consentiva anche di registrare audio nelle immediatezze e di intervenire parlando attraverso il microfono.

Anche in questo caso l'istruttoria ha evidenziato che la ripresa delle aree ultronee rispetto a quelle di pertinenza era avvenuta in assenza di idonei presupposti di liceità, considerato che il titolare del trattamento non aveva dimostrato la sussistenza di un legittimo interesse riferito a una situazione di rischio effettivo che avrebbe giustificato tale trattamento. Le stesse conclusioni hanno riguardato la captazione di conversazioni avvenute in spazi pubblici attraverso dispositivi audio.

Avendo provveduto a sostituire la telecamera precedentemente installata con una fissa e puntata solo verso l'ingresso dell'abitazione, l'Autorità ha ammonito il titolare del trattamento per la violazione dell'art. 5, par. 1, lett. a) e c) e dell'art. 6, par. 1, del RGPD (prov. 12 ottobre 2023, n. 477, doc. web n. 9949494).

16 Intelligenza artificiale e diritto alla protezione dei dati personali

La locuzione “intelligenza artificiale” (di seguito IA) è ormai entrata nell’uso comune e le sue molteplici applicazioni continuano a formare oggetto di ampio dibattito con l’intento di individuare un punto di equilibrio tra innovazione e regolazione (nelle varie forme in cui può essere declinata), affinché le potenzialità dei più recenti avanzamenti tecnologici possano trovare spazio senza pregiudicare non solo i diritti e le libertà fondamentali dei singoli, ma anche interessi di natura sovraindividuale, quale quello di preservare la democraticità degli ordinamenti. È in particolare nella dimensione sovranazionale che la ricerca di questo punto di equilibrio, lungo tutto il 2023, ha avuto luogo; sono infatti proseguiti i lavori volti ad individuare un quadro regolatorio (sufficientemente) condiviso (come già evidenziato nella precedente Relazione 2022, p. 159) sia presso l’Unione europea, con riguardo al regolamento sull’IA, sia in seno al Consiglio d’Europa, con riguardo alla *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. Senza potersi soffermare in un’analisi di dettaglio del contenuto di tali strumenti, alcune sintetiche considerazioni possono comunque qui svolgersi.

Rilevanza prioritaria per gli Stati membri dell’UE riveste il quadro regolatorio volto a disciplinare le applicazioni sociali dell’IA e le condizioni che andranno a regolare l’introduzione sul mercato europeo dei sistemi di IA: a questo proposito, a seguito della proposta di regolamento presentata dalla Commissione europea il 21 aprile 2021 – sulla quale si era incentrato il parere congiunto, reso il 18 giugno 2021 dal CEPD e dal GEPD (profili ai quali si è fatto cenno nella Relazione 2021, p. 194) –, la posizione comune del Consiglio dell’UE si è formata il 6 dicembre 2022 (in <https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/it/pdf>) e la posizione negoziale del Parlamento europeo è stata raggiunta il 14 giugno 2023 (cfr. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.html). A seguito dell’accordo politico intervenuto nell’ambito del cd. trilogio interistituzionale nel dicembre 2023, il *Provisional Agreement* sul regolamento è stato raggiunto il 2 febbraio 2024 con conseguente approvazione del testo da parte del Parlamento europeo il 13 marzo 2024; il procedimento legislativo si potrà concludere, secondo la procedura ordinaria, con la formale approvazione da parte del Consiglio dell’UE, in conformità a quanto previsto dall’art. 194 TFUE. Il regolamento sull’IA, che fa espressamente salve le discipline di protezione dei dati personali (cfr. art. 2, par. 7), troverà comunque applicazione graduale a partire dalla sua entrata in vigore.

Volendo fare un rapido cenno ai contenuti – con l’occhio rivolto in particolare agli aspetti di diretto rilievo per la protezione del diritto alla vita privata e ai dati personali –, può dirsi che il regolamento identifica alcune applicazioni vietate dei sistemi IA e stabilisce per le restanti obblighe differenziate sulla base dei possibili rischi e del livello d’impatto sui diritti e le libertà fondamentali (cd. *risk based approach*).

Quanto alle pratiche di IA vietate, le stesse sono indicate nell’art. 5, disposizione che richiederà per più di una fattispecie una valutazione attenta (non scevra da qualche sforzo interpretativo) in vista della loro puntuale identificazione: solo in primissima approssimazione (e in via esemplificativa), può dirsi che formano oggetto di divieto sistemi di IA che utilizzano tecniche subliminali o manipolative ovvero che sfruttano le vulnerabilità di singoli e gruppi. Vietati sono altresì, alle condizioni indicate, i sistemi di credito sociale come pure taluni sistemi di IA di cd. polizia

[Verso il regolamento UE sull’IA](#)

16

predittiva (se fondati in via esclusiva sulla profilazione o sulla valutazione delle caratteristiche di una persona); i sistemi di riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione; ancora, i sistemi di categorizzazione biometrica basati su caratteristiche sensibili e l'estrapolazione indiscriminata di immagini facciali da internet o dalle registrazioni dei sistemi di videosorveglianza a circuito chiuso per creare banche dati di riconoscimento facciale.

Tuttavia, sistemi di IA che consentono l'identificazione da remoto "in tempo reale" per finalità di *law enforcement* – valutati criticamente nel parere del CEPD/GEPD n. 5/2021 (v. Relazione 2021, p. 223) – potranno essere utilizzati in presenza delle condizioni indicate dal regolamento (all'art. 5, lett. h) di quest'ultimo), nel rispetto delle misure di tutela e delle condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che tale uso autorizza, nonché previa valutazione d'impatto sui diritti fondamentali da parte dell'autorità che intende impiegarli. L'utilizzo di tali sistemi è inoltre di regola subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente e soggetto a notificazione alla pertinente autorità di vigilanza del mercato e all'autorità di protezione dei dati personali.

In relazione alla realizzazione e all'uso dei sistemi di IA ad alto rischio – quali, in via esemplificativa, quelli correlati all'istruzione e alla formazione professionale, all'occupazione, alla prestazione di servizi pubblici e privati di base, all'impiego di alcuni sistemi di contrasto, come pure di sistemi realizzati per la gestione delle frontiere, per finalità di giustizia e nell'ambito dei processi democratici (come nel caso di sistemi di IA usati per influenzare le elezioni) – sono previsti obblighi penetranti e, tra questi, quelli di valutare preventivamente e mitigare i rischi (art. 9); di adottare pratiche di *governance* per i set di dati di addestramento, convalida e prova (artt. 10-11); di predisporre e conservare la pertinente documentazione tecnica (art. 11); di conservare la registrazione automatica degli eventi (*log*) per l'intera durata del loro ciclo di vita (art. 12); di assolvere obblighi di trasparenza, sì da consentire "ai *deployer* di interpretare l'*output* del sistema e utilizzarlo adeguatamente", anche mediante specifiche istruzioni d'uso (art. 13); di assicurare l'efficace supervisione umana durante il periodo in cui sono in uso, al fine di prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile (art. 14); di accuratezza, robustezza e cibersicurezza (art. 15).

Obblighi specifici sono altresì declinati in capo ai vari soggetti che realizzano, utilizzano o comunque contribuiscono alla commercializzazione di servizi di IA ad alto rischio (fornitori, rappresentanti autorizzati, importatori, distributori e *deployer* dei sistemi di IA ad alto rischio).

Ai singoli è attribuito il diritto di presentare reclami relativi ai sistemi di IA (impregiudicate altre forme di tutela, e tra queste quelle previste dalle discipline di protezione dei dati personali) e di ricevere spiegazioni in merito alle decisioni basate su sistemi di IA ad alto rischio che incidono sui loro diritti.

Il regolamento disciplina altresì i sistemi di IA per finalità generali (non menzionati nell'originaria proposta della Commissione), anche prevedendo specifici requisiti di trasparenza (artt. 50 e 51 ss.). In relazione ai modelli più potenti, che potrebbero comportare rischi sistemici, si prevedono obblighi ulteriori, ad esempio quello di effettuare valutazioni dei modelli, di valutare e mitigare i rischi sistemici nonché di riferire in merito agli incidenti. Le immagini e i contenuti audio o video artificiali o manipolati (i cd. *deepfake*) dovranno essere chiaramente etichettati come tali (art. 50, par. 4).

Gli Stati membri dovranno istituire e rendere accessibili a livello nazionale spazi di sperimentazione normativa (cd. *sandbox*) e meccanismi di prova in condizioni reali,

in modo favorire lo sviluppo di sistemi di IA innovativi in vista della loro immissione sul mercato (artt. 57 ss.); in questo ambito potranno essere chiamate a operare anche le autorità di protezione dei dati personali (cfr. art. 57, par. 10).

A tale riguardo, il regolamento sull'IA fa espressamente salva la disciplina in materia di protezione dei dati personali (e, quindi, le attribuzioni proprie delle autorità indipendenti istituite in base al RGPD e alla disciplina nazionale di recepimento della direttiva 2016/680: nel caso italiano, il Garante). Tanto premesso, deve tuttavia rilevarsi che, a tutta prima, appare articolata, e in misura non trascurabile rimessa all'intervento dei legislatori nazionali, che sono chiamati a individuare le autorità nazionali competenti – una (o più) autorità nazionale di notifica e una (o più) autorità nazionale di sorveglianza del mercato –, la cornice istituzionale che, a livello nazionale, dovrà assicurare la vigilanza sul corretto funzionamento dei diversi sistemi di IA e l'armonico coordinamento tra le varie autorità che (anche a titolo diverso) potranno essere chiamate a svolgere una complessiva attività di *oversight* sul funzionamento dei sistemi di IA. Al riguardo, in più occasioni e in linea con quanto già rappresentato durante l'audizione informale tenutasi il 9 marzo 2022 avanti alle Commissioni IX e X riunite della Camera dei deputati a margine della proposta di regolamento (UE) sull'intelligenza artificiale (doc. web n. 9751565), il Garante (non diversamente dai pareri espressi in passato da CEPD e GEPD) aveva ribadito le ragioni a favore di una posizione di preminenza dell'Autorità, ovvero la stretta connessione tra la materia del trattamento dei dati personali e il funzionamento dei sistemi di IA, non di rado ad alto rischio, incentrati sull'utilizzo (in fase di progettazione o di esecuzione) di tali dati nonché la piena indipendenza che dovrebbe caratterizzare l'operato dei soggetti tenuti a svolgere l'azione di *enforcement* sui sistemi di IA in base alla previsione contenuta nell'art. 70, par. 1. Infatti, nella prospettiva condivisa dalle autorità di protezione dei dati europee, i trattamenti di dati personali effettuati mediante l'IA (o che contribuiscono al cd. allenamento di quest'ultima) si collocano naturalmente nell'alveo oggetto della protezione approntata dalle discipline di *data protection*, tra le quali il controllo ad opera delle autorità di protezione dei dati, in linea con la previsione contenuta nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea.

Sempre nella cornice sovranazionale, merita sottolineare i lavori del Comitato sull'intelligenza artificiale (*Committee on Artificial Intelligence - CAI*), cui ha contribuito, d'intesa con il Ministero degli esteri ed in stretto coordinamento con la Rappresentanza permanente d'Italia presso il Consiglio d'Europa, anche un rappresentante dell'Autorità. Iniziata a Roma il 4 aprile 2022, con l'*Inaugural Meeting* organizzato dal Consiglio d'Europa e dalla Presidenza italiana del Comitato dei ministri del Consiglio d'Europa, la negoziazione della Convenzione ha richiesto un impegno superiore a quello preventivato, come reso evidente dal più ampio numero di incontri tenutisi rispetto a quelli originariamente pianificati al fine di raccogliere un più largo consenso tra i partecipanti (cfr., nel dettaglio, parte IV, tab. 22); per ulteriori informazioni, v. anche <https://www.coe.int/en/web/artificial-intelligence/cai>). Come è noto, all'elaborazione della Convenzione quadro hanno partecipato non solo le Parti contraenti, ma anche, in qualità di osservatori, rappresentanti della società civile e numerosi altri Stati nelle cui giurisdizioni spesso operano i principali attori quanto allo sviluppo di sistemi di IA: tra gli altri, il Canada, il Giappone, Israele e gli USA. Il testo elaborato dal Comitato verrà sottoposto all'adozione da parte del Comitato dei ministri del Consiglio d'Europa per essere quindi aperto alla fase di ratifica, anche da parte di Stati diversi dalle Parti contraenti (analogamente a quanto già accaduto in passato con la Convenzione 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale o con la Convenzione sulla criminalità informatica 185/2001).

16

CAI

G7 DPA Roundtable

Considerata, come già accennato, l'ormai indiscussa rilevanza transnazionale del tema, profili dell'IA formano costantemente oggetto di trattazione in diversi *fora* di approfondimento e discussione: così nel corso della terza *Roundtable* of G7 *Data protection and Privacy Authorities* tenutasi il 20 e 21 giugno 2023 a Tokyo, anche i temi dell'IA hanno formato oggetto di trattazione tra quelli connessi alle tecnologie emergenti e il Garante, rappresentato dalla Vice Presidente Ginevra Cerrina Feroni, ha contribuito alla redazione dello *Statement on Generative AI* del 21 giugno 2023 (v. pure par. 21.4).

Proprio i temi dell'IA (peraltro presenti nell'*Action Plan*: cfr. https://www.ppc.go.jp/files/pdf/G7Roundtable_202306_actionplan.pdf) torneranno ad essere dibattuti in occasione della quarta *Roundtable* of G7 *Data protection and Privacy Authorities* che, con l'organizzazione del Garante, si terrà in Italia dal 9 all'11 ottobre 2024 (cfr. doc. web n. 9956837).

GPA AIWG

Sempre sul piano della collaborazione internazionale, gli effetti dell'IA sul diritto alla protezione dei dati e sui diritti fondamentali hanno continuato a formare oggetto di confronto e successiva elaborazione, anche con il contributo fattivo dell'Autorità, in seno alla *Global Privacy Assembly* (GPA): tale attività, a seguito dei lavori condotti in particolare nell'ambito del GPA *Working Group on Ethics and Data protection in AI* (AIWG), ha portato all'adozione, in occasione della 45ª riunione della GPA (Hamilton, Bermuda, 15-20 ottobre 2023), della *Resolution on AI and Employment* e, riprendendo il tema già trattato nell'ambito della menzionata *G7 DPA Roundtable*, della *Resolution on Generative AI Systems* (in <https://globalprivacyassembly.org/document-archive/adopted-resolutions/>).

ECHW

L'esperienza applicativa italiana relativa al RGPD rispetto ai primi casi di interazione con l'IA ha altresì formato oggetto di trattazione nell'ambito dello *European Case Handling Workshop* (ECHW) 2023 (Berna, 8-9 novembre 2023), con specifico riferimento al tema "*Personal data and face detection*" che ha tratto spunto da un provvedimento adottato dal Garante il 13 aprile 2023, n. 122 (doc. web n. 9896412 sul quale v. *amplius* par. 4.12).

Incontri sull'IA

Il dinamismo che caratterizza gli sviluppi tecnologici come pure istituzionali correlati all'IA è stato oggetto di una pluralità di incontri (v. anche par. 23.4): si può così ricordare la partecipazione attiva di un rappresentante dell'Ufficio, unitamente a rappresentanti di altre autorità di protezione dei dati europee, all'evento intitolato "*Towards the Artificial Intelligence Act*", organizzato dall'on. Brando Bonifei presso il Parlamento europeo (7 marzo 2023) e incentrato sulla proposta di regolamento IA, come pure al *panel* dedicato al tema "*AI Beyond Privacy: Solving the Governance Dilemma*" nell'ambito del 12° *IAPP Europe Data protection Congress* 2023 (Bruxelles, 15 novembre 2023), unitamente a un rappresentante dell'Autorità di controllo francese e all'on. Dragoș Tudorache, nonché alla Conferenza internazionale "*Next Democratic Frontiers for Facial Recognition Technology*" (Università degli Studi di Firenze, 29 settembre 2023) e al seminario "*Improving GDPR compliance at work: the path ahead*" organizzato dal Friedrich-Ebert-Stiftung's *Competence Centre on the Future of Work* (Bruxelles, 19 novembre 2023).

CEN/CENELEC

Nell'ambito delle interazioni con i diversi attori che si occupano delle tematiche legate all'IA, meritano di essere menzionati alcuni tavoli di lavoro presso il CEN/CENELEC JTC 21, in particolare dedicati ai profili della individuazione e gestione dei rischi connessi all'IA (*AI risk catalogue and risk management*) nonché al tema della cd. *data quality*. L'operato degli enti di standardizzazione assumerà crescente rilevanza con l'adozione del regolamento sull'IA.

**Attività
provvedimentale**

L'azione (e l'attenzione) dell'Autorità non si è limitata al piano sovranazionale. Anche dall'attività provvedimentale del Garante è invero possibile inferire un crescente ricorso all'utilizzo di tecniche di IA, anzitutto nel contesto della ricerca

medico-scientifica (v. in proposito i provv.ti 28 settembre 2023, n. 465, doc. web n. 9948285 e 12 ottobre 2023, n. 472, doc. web n. 9953841), e, più in generale, nella realizzazione di servizi sanitari nazionali, tema rispetto al quale il Garante ha fornito indicazioni di carattere generale in ordine alle condizioni di liceità dei trattamenti così effettuati con il “Decalogo” pubblicato il 10 ottobre 2023 (doc. web n. 9938038; in merito v. *amplius* par. 5.2). Come già evidenziato nella precedente Relazione (cfr. p. 161) con riferimento all’attività di contrasto rispetto a fenomeni evasivi/elusivi in ambito fiscale, il ricorso a sistemi di IA in chiave di supporto allo svolgimento di attività di controllo è stato altresì prefigurato, con la previsione in via legislativa di un quadro di garanzia, dallo schema di decreto legislativo recante semplificazione dei controlli sulle attività economiche in attuazione della delega al governo di cui all’art. 27, comma 1, l. n. 118/2022, in merito al quale il Garante ha reso il proprio parere con provv. 31 agosto 2023, n. 387 (doc. web n. 9929069, sul quale v. par. 3.1.2).

Merita altresì menzionare il provvedimento 2 febbraio 2023, n. 39 (doc. web n. 9852214), con il quale si è disposta la limitazione provvisoria con riguardo al trattamento di dati riferiti a persone residenti sul territorio nazionale adottato dal Garante nei confronti di una società stabilita negli Stati Uniti che gestisce un *chatbot*, dotato di una interfaccia scritta e vocale, il quale, avvalendosi di un sistema di IA, genera un “amico virtuale”. Tale provvedimento è stato adottato sull’assunto che l’applicazione presenterebbe rischi concreti in particolare per i minori d’età (ad es. in relazione alla formulazione di risposte inidonee al grado di sviluppo dei minori o in presenza di soggetti emotivamente fragili), peraltro incrementato in ragione della ritenuta assenza di meccanismi atti a verificarne l’età, oltre che per alcune carenze riscontrate dall’Autorità con riguardo alla *privacy policy* (in merito v. *amplius* par. 12.7).

È proseguita, entro la cornice di riferimento dell’accordo quadro di durata triennale formalizzato il 17 gennaio 2022, la preziosa collaborazione con il Consorzio interuniversitario nazionale per l’informatica - CINI (al quale si è fatto cenno già nella Relazione 2021, p. 195). In questo spirito, il Presidente del CINI è intervenuto, con un *opening speech*, ai lavori dell’*International Working Group on Data protection in Technology* (cd. Gruppo di Berlino), tenutosi a Roma dal 6 al 7 giugno 2023 (in merito al quale v. la sintesi riportata in doc. web n. 9902660). La cooperazione con il CINI si è concretizzata in molteplici interlocuzioni intervenute nel corso dell’anno con il “Lab Nazionale IA”, al fine di agevolare la reciproca comprensione delle interrelazioni tra le tematiche dell’IA e le discipline di protezione dei dati personali. Parimenti, è continuata la collaborazione con il Lab Nazionale “Informatica e scuola”, in particolare in relazione all’iniziativa “Programma il futuro”; in questo ambito, nel 2023 ha infatti avuto luogo un secondo ciclo di *webinar* curati da personale dell’Autorità e dedicati a profili di interesse dei minori rispetto alle nuove tecnologie; tutti i *webinar* (registrati ed arricchiti da materiali di primo riferimento) sono accessibili all’indirizzo <https://programmailfuturo.it/notizie/webinar>. Infine, grazie al coordinamento offerto dal Lab Nazionale “Informatica e società” e alla partecipazione di docenti e ricercatori di talune delle Università afferenti al CINI, è stato realizzato presso l’Autorità un ciclo di seminari interni su vari profili connessi allo sviluppo delle ICT.

È altresì proseguita la cooperazione nell’ambito del progetto di ricerca denominato *Legality Attentive Data Scientist* (LeADS), finanziato dall’UE nell’ambito del programma Horizon 2020 – *Research and Innovation Framework* e coordinato dal prof. Giovanni Comandé (Scuola superiore Sant’Anna di Pisa), alle cui attività l’Autorità ha partecipato in qualità di *partner*. A tale iniziativa, mirante a formare esperti in *data science* e diritto hanno partecipato l’Università

16

CINI

LeADS

16

del Lussemburgo unitamente alla Paul Sabatier Tolosa III, alla *Vrije Universiteit* di Bruxelles, all'Università del Pireo, all'Università Jagellonica e al Consiglio nazionale delle ricerche, nonché alcune imprese. All'interno di questa cornice l'Autorità ha ospitato presso la propria sede nel corso dell'anno quattro dottorande di ricerca afferenti al Consorzio universitario.

17 Violazioni dei dati personali

Dal 1° gennaio al 31 dicembre 2023 sono state notificate all’Autorità 2.037 violazioni dei dati personali ai sensi dell’art. 33 del RGPD o dell’art. 26 del d.lgs. n. 51/2018 (cfr. sez. IV, tab. 9) da parte di soggetti pubblici (37% dei casi) e privati (63% dei casi). Gran parte delle violazioni dei dati personali è stata notificata per fasi (circa il 64% dei casi) con l’invio, in un primo momento, di una notifica preliminare e, successivamente, di una o più notifiche integrative (cfr. sez. IV, tab. 10).

In particolare, nel settore pubblico, le violazioni dei dati personali hanno riguardato soprattutto comuni, istituti scolastici e strutture sanitarie; nel settore privato, sono stati coinvolte grandi società del settore delle telecomunicazioni, energetico, bancario e dei servizi, ma anche piccole e medie imprese e professionisti.

La maggior parte delle violazioni dei dati personali notificate ha riguardato la perdita di riservatezza o di disponibilità (anche solo temporanea) dei dati personali (circa 88% dei casi; cfr. sez. IV, tab. 11). I fenomeni più frequentemente riscontrati sono stati la diffusione di *malware* di tipo *ransomware*, con compromissione della disponibilità e, in molti casi, della riservatezza dei dati all’interno di sistemi *server* o di postazioni di lavoro di organizzazioni pubbliche e private; l’accesso non autorizzato o illecito ai dati personali trattati all’interno di sistemi informativi; la compromissione di credenziali di autenticazione informatica; la divulgazione accidentale di dati personali a causa di erronea configurazione o utilizzo di piattaforme informatiche o di sistemi *software* di gestione della posta elettronica.

L’attività istruttoria svolta a seguito della notifica delle violazioni dei dati personali ha avuto un duplice obiettivo: quello di esaminare l’adeguatezza delle misure adottate dal titolare del trattamento (o che lo stesso intendeva adottare) per porre rimedio alla violazione dei dati personali o per attenuarne i possibili effetti negativi nei confronti degli interessati, nonché quello di valutare la necessità di comunicare la violazione agli interessati coinvolti, fornendo loro indicazioni specifiche sulle misure da adottare per proteggersi da eventuali conseguenze pregiudizievoli. Laddove non compiutamente rappresentati dal titolare del trattamento, sono stati acquisiti elementi necessari alla valutazione del rischio derivante dalla violazione oggetto di notifica o dell’adeguatezza delle misure in essere al momento della violazione e di quelle adottate per porvi rimedio, sia attraverso acquisizione documentale, sia attraverso specifiche attività ispettive presso i titolari o i responsabili del trattamento.

Con riferimento ad alcune violazioni dei dati personali rispetto alle quali i titolari del trattamento avevano ritenuto di non dover informare gli interessati coinvolti, l’Autorità, dopo aver valutato la probabilità che le violazioni presentassero un rischio elevato, ha ingiunto ai titolari di provvedervi senza ritardo ai sensi dell’art. 58, par. 2, lett. e), del RGPD (cfr. provv.ti 13 aprile 2023, n. 117, doc. web n. 9903696; 8 giugno 2023, n. 255, doc. web n. 9896217; 3 agosto 2023, n. 351, doc. web n. 9941763).

Nei casi in cui è emersa un’inadeguatezza delle misure di sicurezza adottate o il mancato rispetto degli obblighi in materia di violazione dei dati personali da parte del titolare o del responsabile, sono stati adottati provvedimenti correttivi, anche di tipo sanzionatorio.

Per maggiori informazioni in merito, si fa rinvio ai paragrafi 5.4.1. e 5.4.2. della presente Relazione.

18 Il trasferimento dei dati personali all'estero

Nel corso del 2023 si è conclusa l'attività di collaborazione del Garante nell'ambito della *Task Force* 101 (cd. TF 101) la quale, come già rappresentato nella Relazione 2022 (p. 164), è stata specificamente incaricata dal Comitato europeo per la protezione dei dati personali di coordinare l'esame di 101 reclami aventi ad oggetto la liceità dei trasferimenti dei dati personali verso gli USA, posti in essere da alcuni gestori di siti web, mediante l'utilizzo di Facebook Pixel.

All'esito dell'attività di coordinamento e di scambio di informazioni tra le varie autorità di controllo nazionali partecipanti alla TF 101, sono stati acquisiti gli elementi in merito alle caratteristiche dei servizi resi da Meta Platforms, utili alla definizione delle istruttorie nazionali, tenuto conto anche dell'imminente adozione dell'accordo UE-USA denominato *Data Privacy Framework* (cfr. 21.1).

È inoltre proseguita l'attività di valutazione delle istanze pervenute al Garante in ordine all'approvazione di norme vincolanti di impresa (BCR) ai sensi dell'art. 47 del RGPD.

In particolare, l'8 giugno 2023, l'Autorità ha approvato (prov. n. 243, doc. web n. 9921218), le BCR predisposte da un gruppo multinazionale d'impresa, *leader* nel settore delle infrastrutture digitali (cfr. Relazione 2022, p. 165).

Tali norme vincolanti d'impresa concernono i trasferimenti intragruppo, come specificatamente individuati nell'appendice allegata al provvedimento del Garante, posti in essere dalle società del gruppo in qualità di titolari.

Al riguardo, merita evidenziare che si tratta della prima procedura europea di cooperazione volta all'approvazione delle BCR condotta dal Garante in qualità di Autorità capofila (cd. BCR *lead*).

Tale procedura prevede l'attivazione del cd meccanismo di coerenza, nell'ambito del quale è stato acquisito il 17 maggio 2023, ai sensi dell'art. 64, par. 1, lett. f), del RGPD, il parere favorevole del CEPD (v. *Opinion* 9/2023 del 17 maggio 2023).

A conclusione della stessa, il Garante ha quindi approvato, ai sensi degli artt. 57, par. 1, lett. s), e 58, par. 3, lett. j), del RGPD, le norme vincolanti d'impresa per i titolari del trattamento predisposte dal sopra menzionato gruppo, in quanto garanzie adeguate ex artt. 46, parr. 1 e 2, lett. b) e 47, parr. 1 e 2 del RGPD per il trasferimento intragruppo di dati personali verso Paesi terzi, posto in essere dalle società appartenenti a tale gruppo.

BCR

19 L'attività ispettiva

19.1. L'attività ispettiva fra programmazione e contingenze

Dopo le inevitabili difficoltà e i vincoli che avevano caratterizzato il lungo periodo dello stato di emergenza determinato dalla pandemia da Covid-19, l'anno 2023, nel segnare un generalizzato ritorno alla normalità, ha consentito anche un più regolare svolgimento dell'attività ispettiva.

Ne sono testimonianza i dati statistici che condensano l'impegno di questi mesi: in totale, nel corso del 2023, sono stati svolti 144 interventi ispettivi *in loco* di cui 51 svolti direttamente da personale in servizio presso l'Ufficio del Garante e i rimanenti 93 delegati al Nucleo speciale *privacy* e frodi tecnologiche della Guardia di finanza.

A questi valori numerici, comunque significativi, considerate anche le limitate risorse umane disponibili, si devono aggiungere le 49 ispezioni da remoto (cd. ispezioni *online*) finalizzate alla verifica dell'osservanza del provvedimento contenente le linee guida del Garante in materia di *cookie* e altri strumenti di tracciamento del 10 giugno 2021, n. 231 (doc. web n. 9677876) (v. *infra*).

Tutte le attività ispettive svolte, sia quelle scaturenti da autonome iniziative dell'Ufficio, sia quelle connesse alla definizione di istruttorie in corso (anche svolte in via d'urgenza) si sono ovviamente inserite nel solco delle due delibere approvate dal Collegio (provv.ti 26 gennaio 2023, n. 23, doc. web n. 9862660 e 3 agosto 2023, n. 339, doc. web n. 9920683) con le quali, secondo la prescrizione dell'art. 4 del reg. n. 1/2019, il Garante ha fissato le linee della programmazione semestrale delle attività ispettive.

Per quanto concerne le modalità operative delle ispezioni svolte direttamente dall'Ufficio, un dato emerge con sempre maggiore frequenza: la complessità degli accertamenti da effettuare. Ciò ha reso ormai abituale il ricorso ad appositi team ispettivi costituiti da funzionari del dipartimento giuridico competente, da ispettori con funzioni di ufficiale di polizia giudiziaria e da informatici appartenenti al Dipartimento tecnologico dell'Autorità.

L'attenzione ai profili tecnologici e, all'interno di questi, alla verifica degli apprestamenti a tutela della cd. *cybersecurity*, ha acquisito un rilievo centrale di cui vi è poi traccia esplicita nei provvedimenti prescrittivi e/o sanzionatori che, anche a seguito degli accertamenti *in loco*, definiscono le relative istruttorie.

Per una migliore comprensione delle attività svolte può essere utile dedicare qualche breve cenno ad alcuni degli ambiti nei quali si sono concentrati alcuni dei più significativi interventi ispettivi:

- SPID. La costante attenzione dell'Ufficio verso le problematiche connesse all'identità digitale e al suo utilizzo ha portato allo svolgimento di un ciclo di ispezioni (destinato a prolungarsi anche nell'anno 2024) volte a verificare la correttezza dei procedimenti di rilascio e utilizzo dello SPID, specie con riguardo alla corretta identificazione dei soggetti che intendevano usufruire dello stesso, a partire dalle numerose segnalazioni di irregolarità e truffe pervenute all'Ufficio;

- ricerca scientifica. Una serie di ispezioni ha riguardato la correttezza delle procedure adottate, in particolare dagli IRCCS, nello svolgimento delle attività di ricerca, con particolare riguardo alle informative rese, ai consensi acquisiti e all'adozione di corrette tecniche di anonimizzazione dei dati;

19

- tecnologie di riconoscimento facciale. In relazione a queste tecnologie (oggetto di grande attenzione e di espliciti limiti normativi anche a livello eurounitario), sono stati condotti interventi ispettivi sia presso strutture aeroportuali che avevano avviato delle sperimentazioni in merito, sia presso imprese che impiegavano illecitamente tali tecnologie per il controllo delle presenze dei dipendenti. Nel corso di alcuni di questi interventi si è anche risaliti ai fornitori degli apparati e, tramite la documentazione contabile di questi ultimi, si sono individuati altri soggetti acquirenti, al fine di estendere il perimetro degli accertamenti e impedire il moltiplicarsi di utilizzi illeciti, spesso a danno di lavoratori dipendenti;

- *data breach*. La verifica sul campo delle ragioni che hanno determinato l'avvenuta violazione di dati personali ed il controllo sull'effettiva adozione di tutte le misure tecniche e organizzative necessarie a porvi rimedio rappresentano uno degli ambiti principali degli interventi ispettivi negli ultimi anni. In riferimento alle violazioni che hanno interessato banche dati di particolare delicatezza e/o grandi dimensioni, particolare attenzione è stata dedicata alle evidenze di accessi illeciti posti in essere da dipendenti di pubbliche amministrazioni;

- sistema VIS (*Visa Information System*). Si è completato nel corso del 2023 il ciclo ispettivo, già iniziato l'anno precedente (v. Relazione 2022, p. 167), dedicato ai controlli su questo sistema informatizzato di condivisione dei dati relativi ai visti di ingresso nello spazio Schengen. In particolare è stata svolta una verifica *in loco* presso il Consolato italiano di Tunisi, preceduto dalle necessarie interlocuzioni con il Ministero degli affari esteri e l'Ambasciata italiana in Tunisia;

- *marketing*. Sotto questa generica dizione sono comprese le molteplici attività ispettive *in loco* svolte nell'ultimo anno soprattutto nei confronti di società operanti nel settore energetico latamente inteso. In vista della generalizzata apertura al mercato si è infatti sviluppato il fenomeno del *cd. marketing selvaggio* che, a partire dall'acquisizione e dal commercio di enormi *database* di utenti degli *ex* monopolisti, porta ad una preoccupante proliferazione di telefonate a fini commerciali e pubblicitari in assenza del consenso degli interessati e alla sottoscrizione di contratti con firme false o ottenuti carpando la buona fede dei destinatari.

19.2. Controlli online sulle *cd. linee guida in materia di cookie*

Come già accennato nel par. 19.1, l'anno 2023 ha visto affiancarsi ai tradizionali controlli *in loco* anche le ispezioni da remoto, realizzate attraverso la verifica, tramite la rete internet, della conformità di un significativo numero di siti web alle regole individuate dall'Autorità con le linee guida in materia di *cookie* e altri strumenti di tracciamento del 10 giugno 2021, n. 231 (doc. web n. 9677876). Si tratta di una modalità operativa efficace che permette la realizzazione di un consistente numero di controlli, moltiplicando quindi le possibilità di verificare la concreta adesione dei titolari del trattamento ai principi fissati dalla normativa e alle indicazioni del Garante con particolare riguardo alla completezza delle informative fornite dai siti web e alla corretta acquisizione dei consensi degli interessati.

19.3. La collaborazione con la Guardia di finanza

Il rapporto di collaborazione con la Guardia di finanza, definito nel Protocollo di intesa del 21 Marzo 2021, (doc. web n. 9570071), è ormai una realtà consolidata e ha consentito al Garante, anche nel 2023, di aumentare il numero di interventi ispettivi *in loco*. Ciò è avvenuto principalmente con l'impegno dell'apposito Nucleo

speciale *privacy* e frodi tecnologiche della Guardia di finanza e, tramite lo stesso, in alcune circostanze, è stata attivata la collaborazione con i reparti territoriali del Corpo.

Le attività delegate hanno riguardato un ampio spettro di situazioni: dalla notifica di atti e documenti, alla raccolta di informazioni *in loco*, alla ricerca e identificazione, tramite verifiche sul campo e/o consultazione delle banche dati in uso al Corpo, di titolari e responsabili del trattamento. A queste attività, essenziali ma sicuramente più consuete, si sono aggiunte le ispezioni più complesse e delicate svolte in totale autonomia o con la contestuale partecipazione di personale dell'Ufficio. In questa prospettiva, è proseguito un impegno di formazione continua, attraverso incontri e approfondimenti presso la sede del Garante, allo scopo di qualificare e specializzare sempre di più gli ispettori del Nucleo e favorire così la realizzazione, in piena autonomia, di più numerosi cicli ispettivi.

19

20 Il contenzioso giurisdizionale

20.1. Considerazioni generali

In applicazione del quadro normativo vigente, tutte le controversie che riguardano l'applicazione della disciplina in materia di protezione dei dati personali devono essere comunicate al Garante, anche se non sono relative all'impugnazione di provvedimenti dell'Autorità (art. 152 del Codice e art. 10, comma 9, d.lgs. n. 150/2011, come modificato dall'art. 17 del d.lgs. n. 101/2018),

In relazione a tale obbligo informativo, si registra, nel decorso anno, un deciso aumento rispetto al passato: a fronte dei 58 ricorsi del 2021 e 70 del 2022, nel 2023 è stata comunicata all'Autorità la pendenza di 101 controversie in materia di protezione dati tra soggetti terzi.

Permane, invece, non sempre puntualmente adempiuto l'altro obbligo, a carico delle cancellerie, di trasmettere al Garante copia dei provvedimenti emessi dall'Autorità giudiziaria in materia di protezione dati e di criminalità informatica (art. 154, comma 6, del Codice). Tali comunicazioni contribuiscono ad arricchire la conoscenza da parte dell'Autorità dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e a individuare gli interventi normativi ritenuti necessari per la tutela dei diritti degli interessati, da segnalare al Parlamento e al Governo.

20.2. Le opposizioni ai provvedimenti del Garante e le decisioni giudiziali di maggior rilievo

L'anno 2023 ha registrato una rilevante riduzione nella proposizione delle opposizioni a provvedimenti dell'Autorità: 75 a fronte dei 123 ricorsi del 2022.

Nel decorso anno, inoltre, l'Autorità ha avuto notizia di 159 decisioni dell'Autorità giudiziaria relative a opposizioni a provvedimenti del Garante (di cui 37 relative a cartelle di pagamento), a fronte delle 113 pervenute nel 2022.

Di seguito si dà conto delle sentenze di maggior rilievo.

Con sentenza 9 giugno 2023, n. 451, il Tribunale di Cuneo ha respinto l'opposizione proposta da un comune ai sensi dell'art. 615, comma 1, c.p.c. avverso la cartella esattoriale recante la sanzione pecuniaria comminata dall'Autorità all'esito del provvedimento con il quale l'Ufficio aveva contestato la violazione dell'art. 13 del Codice, sanzionata dall'art. 161 del medesimo Codice, allora vigenti, per aver svolto trattamenti di dati personali senza aver reso un'idonea informativa agli interessati.

Il procedimento traeva origine da una segnalazione con la quale l'interessato aveva lamentato l'inidoneità dell'informativa in relazione al trattamento di dati personali effettuato dal comune tramite un dispositivo elettronico di rilevazione delle infrazioni semaforiche. Nelle more del procedimento era intervenuta la disciplina di cui al d.lgs. n. 101/2018, cosicché l'atto di contestazione immediata di cui all'art. 14 della l. n. 689/1981 aveva assunto il "valore dell'ordinanza-ingiunzione [...] senza obbligo di ulteriore notificazione" (ex art. 18, comma 3, d.lgs. n. 101/2018), onde l'Autorità aveva provveduto a iscrivere a ruolo la detta somma, dovuta dal comune in ragione del verbale di accertamento di violazione amministrativa del 7 dicembre 2016.

Occorre innanzitutto evidenziare che il giudice ha ritenuto non fondata in via

Trattamento di dati da parte di soggetti pubblici

preliminare l'eccezione spiegata dal Garante di inammissibilità del ricorso per intervenuta decadenza *ex art.* 10, comma 3, d.lgs. n. 150/2011. Ad avviso del Tribunale, infatti, “per effetto dell’art. 18 del d.lgs. n. 101/2018 (ritenuto in questa sede pienamente applicabile), l’atto endo-procedimentale di contestazione dell’infrazione notificato al presunto trasgressore il 7 dicembre 2016, è stato trasformato, *ope legis*, in provvedimento finale del procedimento sanzionatorio avente il valore di ordinanza-ingiunzione. In altri termini, in virtù della novella legislativa, il provvedimento sanzionatorio che ha pregiudicato la posizione dell’ente comunale coincide integralmente con l’atto di contestazione della violazione dell’art. 13 del Codice della *privacy* nella sua formulazione *pro tempore* vigente: si tratta di un provvedimento che si è formato in via progressiva *per silentium* e, in particolare, per effetto della notifica dell’atto di contestazione al presunto trasgressore e, a seguito dell’entrata in vigore del d.lgs. n. 101/2018, per l’omessa presentazione da parte di quest’ultimo delle memorie difensive all’autorità amministrativa nel termine perentorio previsto dal legislatore. Tanto premesso, l’ingiunto può far valere i vizi di illegittimità del provvedimento sanzionatorio (quali emergenti dall’atto di contestazione che ha valore di ordinanza-ingiunzione) – nonché i vizi di costituzionalità dell’art. 18 del d.lgs. n. 101/2018 che ha trasformato l’atto di contestazione dell’infrazione in provvedimento conclusivo del procedimento amministrativo e che, quindi, in via riflessa, si ripercuotono sulla validità del provvedimento sanzionatorio – nel termine decadenziale di cui all’art. 10, comma terzo, del d.lgs. n. 150/2011 decorrente, ovviamente, dalla data in cui si è perfezionata la notifica della cartella di pagamento, in quanto quest’ultimo rappresenta il primo atto con cui al comune è stata comunicata l’irrogazione della sanzione nei suoi confronti”.

L’opposizione all’esecuzione viene pertanto in questa sede ritenuta come “recuperatoria” di una garanzia negata all’intimato in virtù della normativa sopravvenuta e non viene accettata la tesi (sostenuta dall’Ufficio e dall’Avvocatura) per cui il *dies a quo*, da cui sono decorsi i 30 giorni per impugnare, andrebbe individuato nella data nella quale si consumavano i novanta giorni dopo l’entrata in vigore del decreto, scaduti i quali, in assenza di pagamento agevolato o produzione di nuove memorie, la contestazione si sarebbe convertita *ope legis* in ordinanza-ingiunzione.

Interessanti appaiono le considerazioni del giudice in punto di legittimità costituzionale dell’art. 18, commi 2 e 4, del citato d.lgs. n. 101/2018.

Nonostante la premessa sul rito precisata, il giudice ha in ogni caso ritenuto costituzionalmente legittimo l’impianto complessivo del d.lgs. n. 101/2018, evidenziandone la *ratio* di deflazione del carico amministrativo, fornendo una lettura della sentenza della Corte costituzionale n. 260/2021 che ha ritenuto tale normativa non conforme unicamente nella parte relativa all’interruzione del termine quinquennale di prescrizione del diritto dell’amministrazione a riscuotere le somme (comma 5).

Ha inoltre pienamente accolto tutte le eccezioni spiegate nel merito dalla difesa del Garante, confermando il provvedimento dell’Autorità e le inadempienze del comune in materia di informativa resa ai cittadini.

Con sentenza 31 maggio 2023, n. 8722, il Tribunale di Roma ha confermato il provvedimento correttivo-sanzionatorio del Garante 26 novembre 2020, n. 236 (doc. web n. 9522206) in tema di responsabilità amministrativa della persona giuridica per fatto del dipendente. La vicenda riguardava la diffusione in rete di un video riguardante un uomo, ripreso all’interno dei locali di un commissariato di pubblica sicurezza della Capitale, nell’atto di compiere gesti autolesionistici in uno stato di evidente alterazione psicofisica. Nel video si vedeva chiaramente il volto dell’uomo mentre si procurava lesioni al capo e si sentiva chiaramente che, tra i lamenti disperati, dichiarava di essere malato oncologico e di avere l’AIDS.

Il procedimento avviato d’ufficio dal Garante aveva portato all’accertamento

20

dell'illiceità del trattamento complessivamente posto in essere dagli operatori di polizia, infliggendo al Ministero dell'interno una sanzione pecuniaria pari a 60.000 euro, nonché impartendo allo stesso misure correttive. Con la sentenza in esame, che il Tribunale di Roma ha rigettato il ricorso proposto dal menzionato Ministero, che è stato altresì condannato alla rifusione delle spese di lite in favore della controparte.

In particolare, il Tribunale ha ritenuto pienamente condivisibile quanto sostenuto dal Garante nel provvedimento impugnato ove si afferma che “i dati, di cui il Ministero disponeva in ragione e per lo svolgimento dei propri compiti istituzionali, che erano in suo pieno ed esclusivo controllo ed in relazione ai quali aveva un obbligo di custodia ben dettagliato dalle norme sulla protezione dei dati personali, sono stati comunicati e diffusi in violazione delle norme stesse ed in modo gravemente lesivo della dignità della persona interessata”.

In merito poi alla riconducibilità al medesimo Ministero della responsabilità amministrativa per la divulgazione in esame, il Tribunale di Roma non ha ritenuto fondati i rilievi dell'amministrazione ricorrente per cui, tanto la condivisione del filmato sulla *chat* dell'applicazione WhatsApp, quanto la diffusione su internet sarebbero state opera individuale del singolo dipendente (perseguito penalmente e disciplinarmente), con la conseguenza che l'amministrazione non avrebbe potuto essere chiamata a rispondere dell'illecito in questione, in ragione della sussistenza di un mero nesso di “occasionalità necessaria”, in quanto “esterna” alla sua possibilità di controllo, diversamente da quanto accade per la responsabilità civile del dipendente in caso di illecito aquiliano (richiamando Cass., SS.UU., n. 13246/2019, oltre agli artt. 28 Cost. e 2049 c.c.).

È stata, pertanto, riconosciuta la responsabilità amministrativa del Ministero per la mancata adozione di misure minime di sicurezza volte ad impedire la condivisione e la diffusione dei dati.

Il Tribunale di Padova, con sentenza n. 649/2023, pubblicata il 31 marzo 2023, ha accolto il ricorso proposto da un comune contro l'Agenzia delle entrate-riscossione e il Garante per l'annullamento di una cartella esattoriale fondata su una contestazione di violazione amministrativa formulata dal Garante, che aveva assunto *ope legis* valore di ordinanza-ingiunzione, ai sensi dell'art. 18, comma 2, d.lgs. n. 101/2018.

La contestazione ha avuto origine da una segnalazione pervenuta all'Autorità nella quale l'interessato aveva rappresentato che, dopo aver scaricato dal sito della polizia locale alcune foto relative a una multa ricevuta, constatava che nei fotogrammi messi a disposizione era possibile visualizzare non soltanto la targa relativa alla propria moto, bensì anche quella, non oscurata, relativa ad altro veicolo, non interessato dal procedimento amministrativo. Dopo aver acquisito informazioni dal comune, che ha ammesso il fatto connotandolo come una “svista”, l'Autorità aveva rilevato che il comune aveva posto in essere un illecito trattamento di dati personali, mediante la pubblicazione sul proprio sito internet di fotogrammi relativi a una violazione del codice della strada, recanti dati non pertinenti ed eccedenti per il perseguimento della finalità di accertamento di comportamenti contrari alle disposizioni in materia di segnaletica stradale, in violazione delle prescrizioni contenute nel punto 5.3.1. del provvedimento generale del Garante dell'8 aprile 2010, contestando la relativa sanzione amministrativa.

Il Tribunale di Padova ha accolto il ricorso ritenendo in particolare che “[...] l'elemento del numero della targa, senza alcuna indicazione circa il conducente, non può farsi rientrare nel novero dei dati personali meritevoli di tutela da parte della normativa in materia di *privacy*, d.lgs. n. 196/2003 e succ. mod., in quanto trattasi di dati rinvenibili in pubblici registri, collegati a veicoli, di cui ne consentono l'individuazione e non a persone che rappresentano il bene tutelato dalla normativa citata”.

Per tali motivi l'Autorità ha proposto alla competente avvocatura di impugnare in

Cassazione la sentenza, anche in ragione dell'importanza del principio di diritto in discussione, tenuto conto della preesistente giurisprudenza in materia sia di ambito nazionale sia di matrice unionale.

La Corte di cassazione, con sentenza 11 settembre 2023, n. 26267/2023, ha confermato la legittimità della sanzione di 20.000 euro irrogata a una regione, per avere pubblicato sul sito web istituzionale una deliberazione della Giunta regionale avente a oggetto “Mobilità per esigenze organizzative di un dipendente nell'ambito dell'organico della giunta regionale”, contenente valutazioni sulla professionalità e sul contegno dell'interessato, espressamente identificato. La Corte ha riconosciuto la correttezza del provvedimento del Garante, poiché in base all'art. 19 del Codice (successivamente abrogato a seguito delle modifiche apportate dal d.lgs. n. 101/2018), la diffusione di dati personali da parte di un soggetto pubblico era ammessa unicamente quando prevista da una norma di legge o di regolamento. La Corte ha precisato che la finalità del controllo sull'agire dell'amministrazione mediante la trasparenza delle informazioni deve essere attuata mediante forme di pubblicità la cui conoscenza sia ragionevolmente ed effettivamente connessa all'esercizio di un controllo, nel rispetto dei limiti di proporzionalità e pertinenza, non giustificandosi una totale e indiscriminata ostensione dei dati stessi (cfr. Corte cost. n. 20/2019), nemmeno nel regime del d.lgs. n. 33/2013.

Con ordinanza 21 settembre 2023, n. 26974, adottata all'esito di un giudizio intentato da un comune, la Suprema Corte ha affermato che “l'art. 18 del d.lgs. n. 101 del 2018, attuativo del GDPR, ha introdotto una deroga all'art. 16 della l. n. 689 del 1981 quanto ai procedimenti sanzionatori per violazione degli artt. 161, 162, 162-bis, 162-ter, 163, 164, 164-bis, comma 2, del Codice in materia di protezione dei dati personali, tale per cui, in ipotesi di mancata definizione e di mancata presentazione di “nuove memorie difensive”, il titolo si cristallizza nel verbale di contestazione, ove codesto contenga tutti gli elementi necessari a individuare una ben determinata pretesa sanzionatoria; donde la cartella di pagamento che sia successivamente notificata costituisce non il primo atto teso a far valere la pretesa patrimoniale, sebbene e proprio l'atto della riscossione, la quale è consentita mediante il ruolo, stante la definitività del titolo a monte”. Inoltre, la Suprema Corte ha esaminato anche la questione di legittimità costituzionale della norma, ritenendo che la Corte costituzionale, con la nota sentenza n. 260/2021, ha ritenuto incostituzionale la disciplina censurata nei limiti del ripetuto quinto comma, per violazione del principio di ragionevolezza e del canone di proporzionalità, non ravvisando, “a sostegno della disposizione censurata, alcun motivo idoneo a giustificare un livello tanto intenso di compressione della posizione del privato” (così la Consulta). E con ciò - continua la Corte di cassazione con questa ordinanza - la Corte costituzionale “ha implicitamente ritenuto legittima, invece, la scelta legislativa nel suo ulteriore profilo precettivo, giacché la *ratio* è nella semplificazione della procedura, e tale *ratio* risiede nell'esigenza di far fronte al sovraccarico di oneri amministrativi derivanti per l'appunto dall'entrata in vigore del GDPR. Sicché solo l'interruzione della prescrizione è illegittima [e tale è stata dichiarata], perché si configura come un'ulteriore e non giustificata prerogativa dell'amministrazione per perseguire il fine citato. Ne segue che i profili di incostituzionalità della disciplina di legge afferente al caso concreto sono chiaramente infondati”.

Con sentenza 9 maggio 2023, n. 1544, la Corte d'appello di Milano ha accolto il ricorso presentato dal Garante e, per l'effetto, in totale riforma della decisione di primo grado, ha respinto l'opposizione proposta da una società avverso una cartella esattoriale emessa dall'Agenzia delle entrate a titolo di violazioni della disciplina in materia di protezione dei dati personali ai sensi dell'art. 18 del d.lgs. n. 101/2018.

In particolare la Corte ha affermato che, nel caso di specie, all'epoca di entrata

20

Ricorsi avverso cartelle
esattoriali

20

in vigore della novella, il procedimento non era ancora stato definito con l'ordinanza-ingiunzione, né la società aveva acceduto alla definizione agevolata nei termini di legge, né infine aveva provveduto alla presentazione di memorie, di talché alla luce della previsione suddetta, il verbale di contestazione della violazione, fondante l'emissione della cartella esattoriale opposta dalla società nelle forme di cui all'art. 615 c.p.c., ha acquistato valore (*rectius* si è convertito in) di ordinanza-ingiunzione "senza obbligo di ulteriore notificazione", opponibile soltanto nelle forme e nei termini di cui alla l. n. 689/81. Ragion per cui l'opposizione *ex art.* 615 c.p.c. proposta avverso la cartella esattoriale sulla base della sanzione irrogata dal Garante non poteva essere validamente accolta alla luce del fatto che la pretesa sanzionatoria è da ritenersi cristallizzata per mancanza di rituale opposizione, e cioè nei termini e nelle forme di cui alla normativa di riferimento.

Il Tribunale di Arezzo con sentenza 25 gennaio 2023, n. 74, ha rigettato l'opposizione proposta da una società avverso la cartella di pagamento emessa dall'Agenzia delle entrate a titolo di violazioni della disciplina in materia di protezione dei dati personali ai sensi dell'art. 18 del d.lgs. n. 101/2018, per la somma di 22.000 euro oltre agli oneri accessori.

In particolare, il Tribunale ha affermato che l'art. 18 del d.lgs. n. 101/2018 è chiaro nello stabilire che, decorso il termine di legge, l'atto con il quale sono stati notificati gli estremi della violazione assume il valore di ordinanza-ingiunzione, senza obbligo di ulteriore notificazione, salvo che il contravventore non produca "nuove" memorie difensive. Tale ultima circostanza pacificamente non ricorreva nel caso in esame, non avendo la società presentato alcuna nuova memoria a seguito della entrata in vigore del richiamato decreto legislativo. Ne consegue che, spirato il termine, il verbale si era convertito *ex lege* in ordinanza-ingiunzione (e costituiva dunque il titolo esecutivo sul quale si fondava la cartella di pagamento), senza che fosse necessaria ulteriore notificazione. Né ha ritenuto condivisibile l'assunto di parte ricorrente secondo cui, al momento dell'entrata in vigore della norma, erano decorsi i "termini perentori" per la conclusione del procedimento amministrativo, "essendo pacifico che l'ordinanza-ingiunzione può essere emessa sino a che non è spirato il termine di prescrizione quinquennale". Il Tribunale ha altresì rilevato che non sussistevano i denunciati profili di incostituzionalità della norma. Infatti, non risultava leso il diritto di difesa, potendo la parte esercitare appieno il proprio diritto, tanto in seno al procedimento amministrativo (con la presentazione di nuove memorie difensive) tanto in sede giurisdizionale (mediante tempestiva impugnazione del verbale di contestazione, divenuto ordinanza-ingiunzione); non sussisteva la violazione del principio di eguaglianza formale, dal momento che il legislatore ha dettato una disciplina uniforme per soggetti che si trovavano nella medesima situazione, né il meccanismo introdotto dal legislatore risultava manifestamente irragionevole, essendo controbilanciato dalla possibilità, per il trasgressore, di ottenere l'estinzione mediante pagamento in misura ridotta e comunque dalla facoltà di ottenere un provvedimento espresso mediante presentazione di nuove memorie difensive (fermo comunque il diritto di impugnare il provvedimento conclusivo). Avverso la sentenza in parola la società ha proposto ricorso davanti alla Corte di cassazione.

Merita di essere altresì segnalata la sentenza della Corte di cassazione in sede civile (sez. I, 20 dicembre 2023, n. 35568) la quale, nell'ambito di un contenzioso intentato da una società contro il Garante, ha ribadito che, in tema di protezione dei dati personali, l'art. 18 del d.lgs. n. 101/2018, attuativo del RGPD, "[...] ha introdotto un meccanismo di definizione agevolata delle violazioni ancora non definite con ordinanza-ingiunzione alla data di applicazione del Regolamento medesimo. Esso si traduce, ove mancante detta definizione e la presentazione di nuove memorie difensive, nella conversione *ex lege* del verbale di contestazione, già notificato,

in ordinanza-ingiunzione della quale non necessita ulteriore notificazione, sicché il *dies a quo* del termine per la proposizione dell'opposizione (...) va individuato (...) nell'ultimo momento utile per produrre le memorie suddette ai sensi del comma 4 del medesimo articolo, né il destinatario della prima può avvalersi della opposizione cd. recuperatoria".

Il Tribunale di Napoli con sentenza n. 3661 pubblicata il 5 aprile 2023 ha rigettato l'opposizione proposta dalla ricorrente avverso la cartella di pagamento emessa dall'Agenzia delle entrate a titolo di violazioni della disciplina in materia di protezione dei dati personali ai sensi dell'art. 18 del d.lgs. n. 101/2018, per la complessiva somma di 22.783,08 euro.

In particolare, il menzionato Tribunale aveva qualificato come opposizione agli atti esecutivi *ex art.* 617 c.p.c. la domanda proposta nella parte relativa alla lamentata mancata notificazione del titolo esecutivo, asseritamente da rinvenirsi nella sentenza n. 1764/19 (pronunciata dal medesimo Tribunale a definizione del giudizio concernente l'annullamento del provvedimento dirigenziale del 25 gennaio 2018, a seguito del quale, nelle more della notifica dell'atto di citazione, il Garante aveva contestato la violazione amministrativa). Il Tribunale di Napoli ha quindi dichiarato inammissibile tale domanda per decorrenza del termine previsto dall'art. 617 c.p.c. atteso che la cartella di pagamento era stata notificata il 12 novembre 2021 ed il giudizio radicato solo il 12 aprile 2022.

Inoltre, avendo qualificato come opposizione all'esecuzione *ex art.* 615 c.p.c. la domanda della ricorrente, il Tribunale ha ritenuto in concreto realizzata la conversione *ex lege* dell'atto di contestazione in ordinanza-ingiunzione ai sensi dell'art. 18, comma 2, d.lgs. n. 101/2018, la quale poteva essere preclusa soltanto dal deposito di memorie successive all'entrata in vigore dell'art. 18.

La Corte di cassazione civile (sez. I, ord. 1° agosto 2023, n. 23405), ricalcando una precedente pronuncia (n. 13406 del 12 maggio 2023), ha affermato che, in tema di sanzioni amministrative, l'audizione del trasgressore e la relativa convocazione non costituiscono atti idonei a interrompere la prescrizione, ai sensi dell'art. 28, secondo comma, l. n. 689/1981, non essendo funzionali a far valere il diritto dell'amministrazione alla riscossione della pena pecuniaria, in maniera tale da costituire esercizio della pretesa sanzionatoria. Se, infatti, non è in discussione che allorché l'amministrazione provveda, a titolo esemplificativo, a rideterminare la sanzione, riducendola anche in accoglimento dei rilievi difensivi del trasgressore (v. Cass. n. 787/2022), esprima comunque la propria volontà di dar corso al procedimento sanzionatorio e, quindi, di proseguire nell'azione punitiva, diverso significato deve, invece, attribuirsi alla convocazione per l'audizione, *ex art.* 18, comma 2, l. n. 689/1981, disposta su richiesta dell'interessato, la quale ha solo la funzione di consentire l'esercizio del diritto di difesa prima che l'amministrazione proceda a una valutazione definitiva della correttezza dell'accertamento precedentemente eseguito (nel caso di specie l'atto di contestazione). Dunque, l'atto di convocazione, avendo natura neutra rispetto alla pretesa sanzionatoria, rispondendo solo ad un'esigenza di salvaguardia del principio del contraddittorio, che deve essere tutelato anche nel procedimento amministrativo (come si desume dall'art. 10, l. n. 241/1990), non può certo ritenersi idoneo a costituire in mora il destinatario dell'atto di accertamento, a norma dell'art. 2943 c.c.

Sul tema della procedura in questione, si segnala anche la sentenza della Corte di cassazione n. 22798/2023 che ha chiarito alcuni aspetti della disciplina transitoria per la definizione agevolata delle violazioni in materia di protezione dei dati personali, di cui al ripetuto art. 18, precedentemente oggetto di contrasto nella giurisprudenza di merito. In particolare, la Cassazione ha stabilito, come sopra ricordato, che la procedura transitoria di cui ai primi 4 commi dell'art. 18 comporta

20

Spamming

che se il contravventore non effettua il pagamento nella misura agevolata o non produce nuove memorie nei termini indicati dalla norma, la conversione della contestazione in ordinanza avviene *ope legis* e non è ammessa azione recuperatoria. Il Supremo Collegio ha anche ritenuto che la procedura transitoria di cui ai primi 4 commi dell'art. 18 è costituzionalmente legittima e non comprime i diritti di difesa, osservando che “la Corte costituzionale, con sentenza n. 260/2021 che ha dichiarato l'illegittimità costituzionale, per violazione del principio di ragionevolezza e del canone di proporzionalità, dell'art. 18, comma 5, d.lgs. n. 101 del 2018, [...] ha implicitamente riconosciuto la tenuta costituzionale dei primi quattro commi del medesimo articolo, i quali delineano il meccanismo di definizione agevolata delle violazioni in materia di protezione dei dati personali”.

Con sentenza 17 maggio 2023, n. 1386, il Tribunale di Foggia - sez. San Severo, ha annullato l'ordinanza-ingiunzione 12 luglio 2012, n. 202 con la quale il Garante aveva intimato a una società il pagamento di 11.000 euro a titolo di sanzione amministrativa pecuniaria ai sensi degli artt. 161 e 162, comma 2-*bis*, del Codice per l'invio di *e-mail* pubblicitarie in violazione degli artt. 13, 23 e 130 del Codice, all'epoca vigenti.

Nell'accogliere l'opposizione il Tribunale ha rappresentato che anche nel caso di specie trovava applicazione l'orientamento espresso dalla Corte di cassazione penale, secondo cui “affinché la condotta assuma rilievo penale, occorre che si verifichi per ciascun destinatario un effettivo “nocimento”, che non può certo esaurirsi nel semplice fastidio di dover cancellare di volta in volta le *e-mail* indesiderate, ma deve tradursi in un pregiudizio concreto, anche non patrimoniale, ma comunque suscettibile di essere giuridicamente apprezzato [...]” (cfr. Cass. pen. n. 41604/2019). Ne consegue che è richiesta un'adeguata verifica fattuale volta ad accertare, ad es., se l'utente abbia segnalato al mittente di non voler ricevere un certo tipo di messaggi e se, nonostante tale iniziativa, il soggetto agente (ossia, titolare o responsabile del trattamento) abbia perseverato in maniera non occasionale a inviare messaggi indesiderati, creando così un reale disagio al destinatario. In relazione alla fattispecie *de qua*, ha in particolare aggiunto che “a fronte del non trascurabile importo ingiunto a titolo di sanzione, alcuna prova oggettiva l'opposta ha fornito circa l'effettivo numero di *e-mail* spedite dall'opponente”.

Telefonia

Nel 2023 si è chiuso il contenzioso fra TIM e il Garante sorto a seguito dell'impugnazione, da parte della Società di telefonia, di alcuni provvedimenti con i quali il Garante aveva sanzionato il mancato riscontro a richieste di avvocati dirette a ottenere i dati di traffico telefonico per esigenze difensive in ambito penale, effettuate sulla base dell'art. 132, comma 3, del Codice nel testo in vigore all'epoca dei fatti (si tratta di quattro ricorsi giudiziari relativi all'impugnazione di altrettanti provvedimenti del Garante: ordinanza-ingiunzione 14 maggio 2020, n. 85 (doc. web n. 9442587); ordinanza-ingiunzione 27 maggio 2021, n. 216; ordinanza-ingiunzione 13 gennaio 2022, n. 10 (doc. web n. 9744518); ordinanza-ingiunzione 8 luglio 2021, n. 272 (doc. web n. 9693464).

Nella specie, a fronte del menzionato omesso riscontro, gli interessati si erano rivolti all'Autorità che, configurando le doglianze in termini di reclamo al Garante, aveva effettuato la relativa istruttoria, all'esito della quale aveva ingiunto a TIM di fornire i dati richiesti e adottato sanzioni pecuniarie.

Il ricorso di TIM, in estrema sintesi e con varie sfumature sulla base delle particolarità dei singoli casi, è stato fondato sulla ritenuta sussistenza del principio *electa una via, altera non datur*, nel senso che a fronte della richiesta diretta al fornitore, da parte dei difensori, volta ad ottenere i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'art. 391-*quater* c.p.p., il rimedio esperibile in caso di inerzia sarebbe unicamente quello previsto dalla medesima norma processuale, ossia l'istanza al PM, con eventuale intervento del GIP (artt. 367 e 368 c.p.p.).

20

Il Garante aveva sostenuto invece che la disposizione di cui all'art. 132 non escludeva la possibilità, in caso di diniego all'accesso, di presentare reclamo al Garante; infatti, non solo una tale esclusione non è prevista dall'art. 132 del Codice, ma essa non sarebbe nemmeno astrattamente ipotizzabile, poiché il diritto dell'interessato di proporre reclamo all'autorità di controllo è stabilito senza limitazioni dall'art. 77 del RGPD. L'art. 23 del RGPD, prevede che eventuali limitazioni possono essere introdotte dalla legislazione nazionale con riferimento alla "portata degli obblighi e dei diritti di cui agli articoli da 12 a 22", ma non al diritto di ricorrere, in caso di violazioni, al Garante. Su tale questione non è ammissibile alcuna artificiosa distinzione tra procedura di accesso di cui all'art. 15 del RGPD e procedura di accesso ai sensi dell'art. 132, comma 3, del Codice, in quanto la questione riguarda la tutela dei diritti e non le procedure: il diritto di accesso, riconosciuto in termini generali dagli artt. 15 e seguenti del RGPD, non può conoscere alcuna limitazione in termini di tutela in caso di inadempimento, compreso il caso dell'accesso ai dati del traffico telefonico.

Nel primo caso della serie (ordinanza-ingiunzione 14 maggio 2020, n. 85) il Tribunale di Milano aveva respinto il ricorso di TIM (sentenza 9 aprile 2021). Tale decisione era stata tuttavia ribaltata dalla Corte di cassazione (sentenza n. 21314/2022), secondo cui, ove sia esperita l'istanza diretta del difensore *ex art. 391-quater c.p.p.*, come richiamato dal vecchio testo dell'art. 132, comma 3, del previgente Codice, l'*iter* successivo in caso di mancato riscontro deve essere unicamente quello previsto dal c.p.p. rispetto al quale il Garante non è competente.

A fronte della predetta sentenza di legittimità, il Tribunale di Milano, avanti al quale pendevano gli altri contenziosi, ha accolto i restanti ricorsi di TIM (sentenze nn. 591/2023; 841/2023; 4100/2023); tuttavia, probabilmente in considerazione del contrasto di giurisprudenza evidenziato in riferimento alla prima causa, il Tribunale ha disposto la compensazione delle spese per tutti i ricorsi.

L'Autorità ha ritenuto di non proseguire il contenzioso mediante ricorso per cassazione avverso le predette sentenze di merito, anche considerando che la questione controversa attiene all'applicazione di norme non più vigenti.

Con la sentenza della I sez. civile 23 dicembre 2023, n. 5648, la Corte di cassazione ha rigettato il ricorso presentato da una società avverso un'ordinanza-ingiunzione con la quale il Garante aveva intimato il pagamento di 30.000 euro a titolo di sanzione pecuniaria per avere illecitamente realizzato una piccola parte dei parchimetri del Comune di Roma (i cd. parchimetri evoluti) attraverso "[...] l'inserimento facoltativo della targa del veicolo, in modo da evitare al conducente di dover esporre il tagliando o lo scontrino di pagamento sul cruscotto del veicolo". La Suprema Corte ha accolto integralmente gli argomenti difensivi del Garante, confermando la sanzione comminata e disponendo la rifusione, da parte del soccombente, delle spese di giudizio sostenute dal Garante, liquidate in 5.000 euro. Innanzitutto, ha sancito, inequivocabilmente e in coerenza con la tesi sostenuta dal Garante, che la targa dell'autoveicolo è da considerarsi dato personale (tesi più volte contraddetta dai giudici di primo grado). Inoltre la Cassazione ha stabilito un importante principio, ovvero che "L'esistenza di obblighi contrattuali di natura privatistica tra l'opponente e la sua committenza non può valere a giustificare un trattamento effettuato senza il rispetto delle prescrizioni regolamentari". Dunque, se esiste un contratto tra la parte opponente e un soggetto terzo, ciò non basta a qualificare il soggetto terzo come responsabile del relativo trattamento dei dati che deriva dall'esecuzione del suddetto contratto.

Con sentenza n. 603 pubblicata il 13 gennaio 2023, il TAR Lazio ha rigettato il ricorso con cui una importante società di servizi autostradali aveva impugnato, chiedendone l'annullamento, il provvedimento n. 28601 dell'AGCM adottato nei suoi confronti per pratica commerciale scorretta ai sensi degli artt. 21 e 22 del

Mobilità e tecnologie

20

codice del consumo in relazione ad una contestazione relativa ad omesse informazioni nei confronti degli utenti che richiedono preventivi su polizze RC auto tramite una specifica applicazione.

L'Autorità, intervenuta nel giudizio, ha rilevato che nella controversia l'AGCM non aveva acquisito il suo parere, ai sensi dell'art. 27, comma 1-*bis*, del codice del consumo, e che il Garante ha il “mandato eurounitario” di assicurare “non solo la protezione dei diritti individuali nella elaborazione dei dati personali (e dunque nella autodeterminazione informativa del singolo), ma anche la “libera circolazione dei dati”; in tale sede ha altresì richiamato il principio di leale collaborazione tra autorità (art. 154, comma 4, del Codice), nonché le conclusioni dell'Avvocato generale nella causa C-252/21 *Meta c. Autorità per la concorrenza della RFT*.

Sotto il profilo di interesse, il TAR ha affermato che “non sussisteva alcun obbligo di legge di interpellare il Garante, in quanto non si trattava di richiedere un parere obbligatorio nell'ambito di un settore regolato, ai sensi dell'art. 27, comma 1-*bis* del codice del consumo. Il Garante per la protezione dei dati personali è autorità generalista preposta alla tutela trasversale di un diritto fondamentale e non un'Autorità regolatoria di settore. Sotto altro aspetto, il mancato coinvolgimento del Garante neppure può ridondare come vizio di istruttoria, attesa la predetta totale autonomia dei piani di tutela”.

Telepass ha impugnato la sentenza in parola dinanzi al Consiglio di Stato. Il Garante si è costituito in giudizio, ribadendo il proprio ruolo di primazia riconosciutogli dall'ordinamento eurounitario nell'assicurare non solo la protezione dei dati personali, ma anche la libera circolazione di tali dati. In ragione di tale primazia, l'Autorità ha chiesto di “affermare il principio, pienamente rispettoso delle rispettive competenze, della necessaria leale collaborazione fra Autorità il cui compasso regolatorio è suscettibile di coprire casi e situazioni che si sovrappongono”. Al riguardo, è stato ricordato anche quanto statuito dalla Corte di giustizia dell'UE nella causa C-252/21 sopra ricordata, in continuità con le conclusioni formulate dall'Avvocato generale, e in particolare la necessità per tali Autorità di utilizzare le reciproche competenze e conoscenze nello spirito di leale collaborazione, al fine di fugare ogni dubbio sulla portata delle decisioni da assumere nel singolo caso.

Tale linea è stata accolta in pieno dal Consiglio di Stato con sentenza n. 497/2024 pubblicata il 15 gennaio 2024.

Con sentenza 20 luglio 2023, n. 912, parzialmente favorevole, il Tribunale di Reggio Emilia ha ridotto la sanzione da 5.000 a 3.000 euro e compensato le spese in un caso in cui un dipendente aveva lamentato l'uso della posta elettronica aziendale con indirizzo comprensivo del proprio nome, anche oltre la cessazione del rapporto di lavoro.

Con sentenza 16 maggio 2023 il Tribunale di Pordenone, in parziale accoglimento del ricorso proposto da un'azienda sanitaria regionale in relazione a una vicenda relativa al trattamento di dati personali attraverso il FSE, ha rimodulato la sanzione originariamente irrogata, pari a 50.000 euro, riducendola a 5.000. Il Tribunale ha comunque confermato la correttezza del provvedimento del Garante, respingendo la tesi del ricorrente sulla sua non colpevolezza, in quanto l'azienda sarebbe stata solo formalmente titolare del trattamento, a fronte del ruolo della società *in house*, responsabile del trattamento tramite il FSE per conto della generalità delle aziende sanitarie regionali, nonché della regione stessa. È stato quindi confermato il principio secondo cui la titolarità del trattamento impone precisi obblighi sanciti dal RGPD cui non è dato sottrarsi, quanto meno attraverso una continua attività di direttiva e di controllo nei confronti del proprio responsabile del trattamento.

La Corte di cassazione in sede civile (sez. I, ord. 11 ottobre 2023, n. 28417), cassando con rinvio la sentenza del Tribunale di Ravenna (31 marzo 2022, n. 188), che

Posta elettronica
aziendale

Dati sulla salute

aveva accolto l'opposizione proposta dalla ASL di zona avverso il provvedimento del Garante 27 gennaio 2021, n. 36, ha affermato che il fatto di comunicare l'esigenza di un trattamento sanitario e, quindi, l'esistenza di una "malattia" in senso lato – intesa dunque come situazione che renda necessario un trattamento sanitario – attiene a dato sulla salute: non occorre cioè, a tal fine, che sia specificato di quale trattamento sanitario o di quale malattia si tratti. La Corte cita numerosi precedenti sul concetto "lato" di dato sulla salute. Inoltre, in tema di sanzioni amministrative, richiamando numerosi precedenti, la Corte ha ritenuto che l'opposizione all'ordinanza-ingiunzione non configura un'impugnazione dell'atto, ma introduce, piuttosto, un ordinario giudizio sul fondamento della pretesa dell'autorità amministrativa, devolvendo al giudice adito la piena cognizione circa la legittimità e la fondatezza della stessa, avendo il giudice il potere-dovere di esaminare l'intero rapporto, con cognizione estesa – nell'ambito delle deduzioni delle parti – all'esame completo nel merito della fondatezza dell'ingiunzione, ivi compresa la determinazione dell'entità della sanzione sulla base di un apprezzamento discrezionale.

Il Tribunale di Milano, con sentenza 28 febbraio 2023, n. 9157 ha rigettato un ricorso presentato da una società contro un provvedimento prescrittivo del Garante in materia di *data breach* e violazione di misure di sicurezza, condannando alle spese la soccombente. Ciò ha comportato la vittoria del Garante nella causa connessa, relativa all'ordinanza-ingiunzione che era stata comminata dall'Autorità per il *data breach*, anche se il giudice ha ridotto l'importo della sanzione da 600.000 a 400.000 euro (Trib. Milano 31 gennaio 2024, n. 1165). Allo stato non risultano depositate le motivazioni della sentenza.

Con la sentenza 13 dicembre 2023 il Tribunale di Milano ha respinto il ricorso in opposizione proposto da una società avverso il provvedimento del Garante 2 dicembre 2021, n. 424 (doc. web n. 9731682) con il quale era stato definito un reclamo afferente all'invio di un SMS e al conseguente esercizio del diritto di accesso a dati personali. Nel ricorso veniva lamentata l'entità della sanzione irrogata dal Garante, tenuto conto che le violazioni sarebbero state esigue rispetto alla rilevanza dell'attività di *marketing* posta in essere e che il trattamento dei dati in questione non aveva creato pregiudizi agli interessati. Il giudice, concordando con la linea difensiva proposta dal Garante, ha ritenuto in particolare che l'Autorità avesse già operato un bilanciamento dei fattori (da un lato, il massimo editto previsto dall'art. 83, comma 5, del RGPD, ampiamente superiore alla somma oggetto di ingiunzione; la durata della violazione, articolata nel corso del 2019 e del 2020; l'assenza della dimostrazione dei controlli cui l'opponente aveva fatto riferimento anche nel ricorso in discussione; il limitato grado di cooperazione attivato nei rapporti con l'Autorità; dall'altro, la natura dei dati trattati, di tipo comune; i risultati economici registrati a bilancio nel 2020; l'assenza di precedenti procedimenti a carico dell'opponente) che potevano incidere sulla quantificazione dell'importo oggetto di ingiunzione, in modo tale che la somma individuata non poteva ritenersi eccessiva.

Con sentenza 26 giugno 2023, n. 2 il Tribunale de L'Aquila ha fatto chiarezza su due importanti aspetti, spesso ricorrenti nei giudizi relativi all'impugnazione dei provvedimenti del Garante: uno di natura meramente procedurale e l'altro relativo ad una questione di competenza. La vicenda trae origine da un atto presentato personalmente dall'opponente con cui si proponeva opposizione avverso un provvedimento del Garante (nota 21 ottobre 2022) con il quale era stato archiviato il reclamo presentato dallo stesso.

Il Tribunale, facendo riferimento all'art. 10 del d.lgs. n. 150/2011, nella parte in cui dispone che i provvedimenti in materia di protezione dati seguono il rito del lavoro, pur considerando la possibilità per il ricorrente di farsi rappresentare da un ente del terzo settore, ha ribadito comunque l'applicabilità delle norme del codice di

20

Data breach

Telemarketing

*Ricorsi verso
provvedimenti di
archiviazione di reclami*

20

procedura civile sulla rappresentanza in giudizio, e quindi della obbligatoria difesa tecnica. Nel caso di specie, essendo stato il ricorso presentato personalmente dalla parte, non erano state seguite le obbligatorie forme di proposizione della domanda giudiziale, e il difensore è stato officiato solo nel corso del giudizio. Il giudice ha ritenuto che tale costituzione non potesse sanare il vizio originario ed ha pertanto ritenuto il ricorso inammissibile.

Il giudice ha poi individuato un ulteriore profilo per non accogliere il ricorso. Il ricorrente infatti lamentava che, in un avviso di asta giudiziaria, all'interno di una procedura esecutiva, fosse stata allegata una CTU nella quale non erano stati oscurati i propri dati in qualità di debitore e della moglie (oltre che dei terzi confinanti). Il Garante aveva al riguardo disposto l'archiviazione sostenendo di non poter interferire nell'attività giudiziaria.

Il Giudice ha ritenuto la deduzione fondata rilevando che si trattava di questione che andava fatta valere nel procedimento giudiziario, “comunque, rispetto alla quale il Garante non ha alcun compito, ai sensi degli artt. 184 comma 7 e 160-bis Codice *privacy*, conformemente alle disposizioni del Regolamento UE 2016/679”.

Con sentenza 12 settembre 2023 (n.r.g. 4262/2022) il Tribunale di Roma ha respinto l'opposizione proposta dal ricorrente avverso il provvedimento di archiviazione del reclamo da questi presentato dinanzi all'Autorità. Il reclamante aveva lamentato di essere venuto a conoscenza di una presunta violazione della *privacy* ai suoi danni consistente nella trasmissione di suoi dati personali, conferiti alla ASL di zona, titolare del loro trattamento, al fine di iscriversi all'albo dei professionisti esterni, ad altro soggetto pubblico (l'Avvocatura regionale) in assenza di un suo consenso. Il giudice ha respinto il ricorso, condividendo in pieno le motivazioni rese dal Garante nel provvedimento impugnato, secondo cui: “per i soggetti pubblici il trattamento dei dati personali è lecito se necessario “per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri” (art. 6, par. 1, lett. e), del RGPD) prescindendo, dunque, dal consenso dell'interessato (con. 43 del RGPD)”.

La sentenza del Tribunale di Milano 10 novembre 2023, n. 8893 è tornata a esaminare la questione dell'ostensione dei dati di terzi beneficiari di polizze sottoscritte dal *de cuius*, in relazione alla quale il Garante è incompetente non potendosi applicare ai dati di un terzo (il beneficiario della polizza) la disciplina dell'accesso ai dati personali dell'interessato (in tal caso del *de cuius*), e trovando invece applicazione l'art. 24, comma 1, lett. f), del Codice (il trattamento dei dati è scriminato dalla finalità di difesa in giudizio). Pertanto ogni valutazione è rimessa al giudice e non già all'Autorità, il cui intervento in questo tipo di contenzioso si appalesa superfluo (per carenza di legittimazione passiva).

Con sentenza favorevole al Garante il Tribunale di Mantova (n.r.g. 2833/2022) in data 31 ottobre 2023 ha precisato il concetto di “essenzialità” della notizia in relazione alla richiesta di dichiarare l'illegittimità della pubblicazione di dati personali come il luogo e la data di nascita del ricorrente.

Con sentenza 24 maggio 2023, n. 160, il Tribunale di Verbania ha disposto l'annullamento della sola parte del dispositivo del provvedimento del Garante che aveva imposto a una società di servizi di comunicazione elettronica di ordinare i risultati cronologicamente dal più recente al meno recente, cosa che l'opponente aveva dimostrato, in corso di causa, essere tecnicamente non realizzabile, oltre a configurare un *ultra petitum* rispetto a quanto richiesto ed ottenuto dal reclamante. Le spese sono state integralmente compensate a causa della particolarità e novità del giudizio; per queste ragioni non si è ritenuto opportuno proporre ricorso in Cassazione.

Il Tribunale di Milano, con sentenza 30 novembre 2023 (n.r.g. 15976/2023) ha rigettato il ricorso presentato da una casa editrice avverso un provvedimento del

Conoscibilità dei dati
dei beneficiari di
polizze assicurative

Altra casistica

Garante (ordinanza-ingiunzione 2 marzo 2023, n. 62, doc. web n. 9880427 con cui veniva irrogata la sanzione di 2.000 euro) concernente l'illecita pubblicazione dei dati personali e delle ulteriori informazioni in contrasto con gli artt. 5, par. 1, lett. a) e c), del RGPD e 137, comma 3, del Codice, oltre che con gli artt. 5, comma 2, e 6 delle regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica. Il Tribunale ha accolto le motivazioni espresse dall'Avvocatura in difesa dell'Autorità, con particolare riferimento al principio sancito dalla Suprema Corte (sez. unite, 22 luglio 2019, n. 19861), per il quale la "menzione deve ritenersi lecita solo nell'ipotesi in cui si riferisca a personaggi che destino nel momento presente l'interesse della collettività, sia per ragioni di notorietà che per il ruolo pubblico rivestito. In caso contrario, prevale il diritto degli interessati alla riservatezza rispetto ad avvenimenti del passato che li feriscano nella dignità e nell'onore e dei quali si sia ormai spenta la memoria collettiva".

20

20.3. *Il contributo del Garante nei giudizi in materia di protezione dati*

Come si è visto al paragrafo 20.1, l'Autorità giudiziaria deve comunicare al Garante la pendenza di una controversia, trasmettendo copia degli atti introduttivi (art. 10, comma 9, d.lgs. n. 150/2011, come modificato dall'art. 17 del d.lgs. n. 101/2018). Tale comunicazione consente all'Autorità, "nei casi in cui non sia parte in giudizio", di "presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai profili relativi alla protezione dei dati personali".

Conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato, il Garante, nei giudizi diversi da quelli direttamente attinenti a pronunce dell'Autorità, limita, in generale, il proprio contributo ai soli casi in cui sorga, o possa sorgere in prosieguo, la necessità di difendere o comunque far valere particolari questioni di diritto.

In tal senso si segnala il caso comunicato dal Tribunale di Bari relativo alla pendenza di un giudizio instaurato dai genitori di un giovane deceduto, quali eredi e in proprio, nei confronti di una società in ragione del diniego opposto alla loro istanza di accesso ai dati personali del figlio defunto, ai sensi e per gli effetti di cui agli artt. 15 del RGPD e 2-terdecies del Codice. All'esito di una complessa istruttoria, l'Autorità ha trasmesso al giudice un articolato parere sulla delicata questione.

L'Autorità ha comunque seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo alle avvocature distrettuali dello Stato di essere informata sull'evoluzione delle vicende processuali e di ricevere comunicazione in merito agli esiti.

21 Le relazioni comunitarie e internazionali

Il 2023 ha visto, a livello europeo, un grande impegno delle autorità di protezione dei dati volto a migliorare e favorire la cooperazione tra le stesse al fine di garantire una più armonizzata e rapida azione, specie nei casi di trattamenti di dati personali che abbiano carattere transfrontaliero. Come si vedrà di seguito, a tal fine, la Commissione europea ha avviato, anche su impulso del Comitato europeo per la protezione dei dati (di seguito CEPD), il processo legislativo inteso ad adottare nuove regole procedurali che consentano una più efficace applicazione del RGPD, senza tuttavia modificare alcuna disposizione dello stesso.

Un'altra linea di tendenza ha riguardato l'incremento delle attività internazionali del Garante nel corso del 2023: oltre agli organismi da sempre attivamente seguiti dall'Autorità, come il Consiglio d'Europa e l'OCSE, si è registrata la crescita delle attività legate anche ad altre istanze internazionali, come nel caso della *Global Privacy Assembly*, nell'ambito della quale è stato istituito un segretariato permanente, e delle iniziative delle autorità di protezione dati dei Paesi G7, anche in preparazione della presidenza italiana prevista per il 2024. La proliferazione delle attività internazionali ha portato alla creazione di una specifica *Task Force* all'interno del CEPD affinché sia garantito un adeguato coordinamento tra le autorità UE.

Il 2023 è stato altresì contrassegnato dall'intensificarsi, a livello europeo e internazionale, dell'attività legata all'approfondimento dell'interrelazione tra la protezione dei dati e le discipline della concorrenza e della tutela dei consumatori.

È infatti cresciuta l'attenzione riguardo alla necessità che le autorità garanti della concorrenza e della protezione dei dati cooperino su questioni e casi nei settori di interesse comune, anche in virtù della sentenza della Corte di giustizia cd. *Bundeskartellamt* (Causa C-252/21) che non solamente ha aperto la strada all'interazione tra la disciplina della concorrenza e la protezione dei dati, ma ha anche affermato gli obblighi di cooperazione tra autorità competenti.

Le riflessioni sul rapporto tra tali settori hanno portato nell'ambito del CEPD alla istituzione di una apposita *Task Force* (*Task Force Competition and Consumer Protection Law*) e a livello internazionale all'intensificarsi del lavoro svolto dall'omologo gruppo di lavoro *Digital Citizen and Consumer Working Group della Global Privacy Assembly* (GPA) cui il Garante ha aderito.

Profili di sovrapposizione tra protezione dei dati, concorrenza e tutela dei consumatori sono del resto anche presenti nel *Digital Markets Act* (DMA), la normativa europea, applicabile dal 2 maggio 2023, volta a garantire che le grandi piattaforme *online* che fungono da *gatekeeper* dei mercati digitali, controllandone l'accesso, mantengano un comportamento corretto. Il DMA ha previsto un apposito *High Level Group*, poi istituito dalla Commissione europea ai sensi dell'art. 40 del DMA il 23 febbraio 2023, di cui fanno parte, oltre a vari regolatori e reti europee (comunicazioni elettroniche, concorrenza, tutela dei consumatori, *media* audiovisivi) anche il CEPD (Garante europeo per la protezione dei dati) e il CEPD (che è rappresentato da cinque delegati tra cui il Presidente del Garante Prof. Pasquale Stanzone). Tale Gruppo fornisce alla Commissione consulenza e competenze per garantire che la legge sui mercati digitali e altri regolamenti settoriali applicabili ai *gatekeeper* siano attuati in modo coerente e complementare e fornisce competenze nelle indagini di mercato sui servizi e sulle pratiche emergenti, contribuendo così a garantire che la

Protezione dati,
concorrenza, tutela dei
consumatori

legge sui mercati digitali sia adeguata alle esigenze future. In particolare, il 20 settembre 2023, CEPD e GEPD (attraverso la *Task Force* sopra menzionata) hanno fornito il loro contributo congiunto alla Commissione europea sul modello relativo alla descrizione delle tecniche di profilazione dei consumatori, che i *gatekeeper* sono tenuti a presentare annualmente alla stessa ai sensi all'art. 15 del DMA. CEPD e GEPD hanno sottolineato che, per essere efficace nel garantire piena trasparenza sulle tecniche di profilazione dei *gatekeeper*, la descrizione dovrebbe far evidenziare in che modo questi ultimi rispettino la normativa sulla protezione dei dati, fornendo alle autorità di controllo informazioni sufficienti al riguardo.

Invero, altre discipline dell'UE sul digitale e sui dati, recentemente adottate, contengono profili di sovrapposizione con il RGPD, come il *Digital Services Act* (DSA), il *Data Governance Act* (DGA - la normativa europea, applicabile dal 24 settembre 2023, volta a creare un quadro armonizzato per la condivisione dei dati e a stabilire alcuni requisiti di base per la *governance* dei dati), il *Data Act*, e l'emanando regolamento UE sull'IA. In tale contesto, il CEPD e il GEPD assicurano la propria partecipazione, ciascuno con un proprio rappresentante, al Comitato europeo per l'innovazione in materia di dati (EDIB), il gruppo di esperti istituito dalla Commissione europea il 20 febbraio 2023 in attuazione dell'art. 29 del DGA, con il compito di fornire consulenza e assistenza alla Commissione europea sui principali aspetti legati all'attuazione del DGA stesso, tra i quali, in particolare, l'elaborazione di orientamenti per gli spazi comuni dei dati, del modulo europeo di consenso all'altruismo dei dati, nonché in materia di standardizzazione e interoperabilità.

21.1. *La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati*

Dal 25 maggio 2023, il Comitato ha un nuovo Presidente, Anu Talus, a sua volta Presidente dell'Autorità finlandese per la protezione dei dati, che è stata eletta in sostituzione della Presidente uscente Andrea Jelinek. Nel corso del 2023 la plenaria del CEPD si è riunita 15 volte, cinque delle quali in presenza. Quasi duecento sono state le riunioni dei sottogruppi e delle *Task Force* in cui si articola il lavoro del CEPD e che si occupano dell'applicazione del RGPD e della direttiva *law enforcement* nei diversi settori. Le informazioni fornite nei paragrafi seguenti sui documenti prodotti danno conto solo parzialmente della mole di lavoro alla quale anche il Garante ha contribuito, poiché per molti documenti (v., in particolare, le linee guida sul legittimo interesse, o sui trattamenti di dati che coinvolgono minori) il confronto e l'analisi sono proseguite indefessamente, pur senza giungere a conclusione, nel periodo considerato.

In vista della valutazione che la Commissione europea sarà chiamata a pubblicare nel 2024, la seconda dopo la piena applicazione del RGPD, il CEPD ha adottato il proprio contributo informativo il 12 dicembre 2023. Ne emerge un consolidamento della posizione di organismo dell'UE incaricato di garantire l'applicazione coerente del RGPD, avvalendosi dell'intera gamma di strumenti a disposizione, dalle linee guida alle decisioni adottate nell'ambito delle procedure di coerenza. Il Comitato si è fermato a riflettere, sulla base dei dati e delle informazioni di tipo statistico relative all'attività svolta dalle autorità europee nell'ambito dei meccanismi di cooperazione e coerenza negli ultimi due anni, sul funzionamento degli strumenti di cooperazione previsti dal RGPD e ha riconosciuto come gli stessi abbiano il potenziale per conseguire tale obiettivo, in particolare ove utilizzati in modo sufficientemente armonizzato.

Il CEPD, insieme al GEPD, ha fornito un parere congiunto sulla proposta di regolamento che stabilisce norme procedurali supplementari relative all'applicazione del RGPD nei procedimenti relativi a trattamenti transfrontalieri, presentata dalla Commissione europea il 4 luglio 2023 nell'ambito delle attività volte a favorire e

21

Strategia digitale dell'UE**Valutazione dell'applicazione del RGPD****Proposta di norme procedurali supplementari**

21

migliorare il funzionamento dei meccanismi di cooperazione e coerenza previsti dal RGPD (parere congiunto 1/2023). La proposta – che tiene conto della dichiarazione di Vienna del 28 e 29 aprile 2022, in occasione della quale lo stesso CEPD aveva indirizzato alla Commissione europea una lettera per evidenziare alcuni profili procedurali (v. Relazione 2022, p. 177) – intende integrare le disposizioni del RGPD, armonizzando alcuni aspetti legati, tra gli altri, ai requisiti di ricevibilità o rigetto dei reclami nei casi transfrontalieri, ai termini procedurali, allo *status* e ai diritti delle parti, all’attuazione pratica della procedura di cooperazione. Nel parere, il CEPD e il GEPD hanno accolto con favore molte disposizioni della proposta, ma hanno suggerito anche diversi emendamenti in ordine ad alcune disposizioni procedurali, ai meccanismi di cooperazione e di risoluzione delle controversie dinanzi all’EDPB, ai diritti procedurali delle parti oggetto di indagine e dei reclamanti.

In particolare, in merito ai requisiti di ricevibilità dei reclami, il CEPD e il GEPD hanno esortato i co-legislatori a prevedere un’armonizzazione esaustiva dei requisiti di ammissibilità per superare le differenze attualmente esistenti nei diversi Paesi SEE e a chiarire e integrare la proposta per consentire a tutte le autorità di protezione dei dati di procedere alla composizione amichevole delle controversie (*amicable settlement*), in particolare negli Stati membri che attualmente non dispongono di norme procedurali nazionali per risolvere i reclami in modo amichevole.

Per quanto riguarda il meccanismo di sportello unico, il parere ha accolto con favore l’introduzione di nuove fasi procedurali formali che richiedono all’autorità capofila (LSA) di condividere informazioni chiave con le autorità interessate (CSA) in una fase iniziale, ma ha chiesto ai co-legislatori di chiarire che la LSA possa seguire un approccio proporzionato al caso, modulando le informazioni da condividere a seconda della sua complessità. Il CEPD e il GEPD hanno inoltre chiesto alla Commissione di prevedere un maggiore e costante coinvolgimento delle CSA in ogni fase del procedimento, chiarendo l’obbligo per la LSA di collaborare con le autorità di controllo interessate sulla base delle loro osservazioni al fine di risolvere qualsiasi disaccordo in fase precoce. In caso di disaccordo sul merito del singolo caso, il parere raccomanda che il ricorso alle procedure di cooperazione di cui agli artt. 61 e 62 del RGPD (previsto come obbligatorio dalla proposta) sia reso facoltativo per ridurre i tempi di trattazione, e di prevedere che la richiesta di risoluzione d’urgenza di tali controversie da rivolgere al Comitato *ex art.* 65 del RGPD in tale fase preliminare di trattazione possa essere avviata anche dalla/e CSA verificata l’impossibilità di raggiungere un consenso. Il parere ha chiesto inoltre di chiarire gli effetti di tale decisione di urgenza resa dal CEPD.

In merito alle procedure di risoluzione delle controversie dinanzi al CEPD successivamente alla presentazione formale di una proposta di decisione da parte dell’autorità capofila, il parere ha accolto con favore le previsioni tese alla loro razionalizzazione, seppur con alcune modifiche che tengono conto del breve termine previsto dal RGPD per l’adozione di decisioni vincolanti in questi casi.

Nell’ottica di contribuire alla corretta applicazione dei meccanismi di cooperazione, il CEPD ha adottato in via definitiva, dopo la consultazione pubblica, alcune modifiche alle linee guida per l’individuazione dell’autorità capofila (linee guida 8/2022, v. Relazione 2022, p. 185) al fine di assicurare piena coerenza con le linee guida su titolare e responsabile. La versione definitiva delle linee guida ha confermato le principali precisazioni introdotte nel testo, in particolare escludendo che l’accordo (necessario) fra contitolari del trattamento comporti la possibilità di definire anche l’autorità di controllo competente ai sensi degli artt. 55 e 56 RGPD o di modificare in qualsiasi misura la capacità di tali autorità di esercitare i propri compiti e poteri ai sensi degli artt. 57 e 58 RGPD, e confermando che lo stabilimento principale di un titolare del trattamento non può essere considerato lo stabilimento principale del contitolare del trattamento – cosicché i contitolari non possono designare uno stabilimento principale comune.

Linee guida CEPD
su procedure di
cooperazione

Sempre al fine di favorire e sostenere il funzionamento efficiente ed armonizzato del meccanismo di cooperazione e coerenza, è stato adottato dal CEPD anche un modello per i reclami transfrontalieri degli interessati che le autorità di controllo possono utilizzare su base volontaria, al fine di agevolare lo scambio transfrontaliero di informazioni. Il modello è redatto in modo da consentire a tutte le autorità di adottarlo, adeguandolo ai rispettivi requisiti nazionali. Tale modello può essere utilizzato sia per i casi in cui il reclamo è presentato personalmente dalla persona fisica, sia per i casi in cui lo stesso è presentato da un rappresentante legale, un soggetto che agisce per conto della persona fisica o di propria iniziativa.

Il CEPD ha inoltre adottato un modello di ‘avvenuta ricezione’ del reclamo – anche questo da utilizzare su base volontaria – che mira a fornire al reclamante informazioni generali sulle fasi successive alla presentazione del reclamo e sottolinea il diritto a un ricorso giurisdizionale effettivo contro una decisione giuridicamente vincolante assunta da un’autorità di controllo.

Ancora in tema di cooperazione e coerenza tra le autorità di controllo, sono state adottate in via definitiva, dopo consultazione pubblica, le linee guida sulla composizione delle controversie *ex art. 65, par. 1 lett. a)*, del RGPD (linee guida 3/2021) che concernono il meccanismo volto a risolvere opinioni contrastanti tra le autorità nei casi di trattamento transfrontaliero di dati personali. Il documento riporta un numero limitato di modifiche non sostanziali funzionali a richiamare le linee guida relative all’art. 60 (nota 12), le disposizioni del regolamento del CEPD relative alle traduzioni delle sue decisioni vincolanti (punto 46) e l’ordinanza del Tribunale T- 709/21 (note 129 e 135).

Diritto di accesso: nel mese di marzo 2023 è stata adottata la versione finale delle linee guida in materia di diritto di accesso modificate alla luce dei contributi pervenuti nella consultazione pubblica cui la versione preliminare era stata sottoposta. Il testo definitivo presenta poche variazioni rispetto a quello precedente (v. Relazione 2022, p. 176) in particolare con riferimento ai requisiti per l’identificazione e l’autenticazione dell’interessato che richieda accesso ai propri dati e alla completezza delle informazioni fornite a seguito della richiesta di accesso. Inoltre, attraverso specifici esempi, sono offerti chiarimenti riguardo alle ipotesi in cui il titolare, in presenza di una grande mole di dati trattati, possa chiedere all’interessato di circostanziare la richiesta nonché alla possibilità per il titolare di conservare per un tempo ulteriore i dati personali ai fini del riscontro di eventuali richieste di accesso.

Sanzioni amministrative pecuniarie: a maggio 2023, il CEPD ha adottato la versione definitiva delle linee guida sul calcolo delle sanzioni amministrative pecuniarie, già adottate il 12 maggio 2022 e sottoposte poi a consultazione pubblica (v. Relazione 2022, p. 179). Le linee guida hanno mantenuto la struttura e i contenuti del precedente testo e sono state integrate con l’introduzione di ulteriori esempi o chiarimenti concernenti questioni sostanziali, quali i criteri per correlare le dimensioni dell’impresa a un adeguamento della sanzione pecuniaria inflitta. Sono state aggiunte due tabelle: una relativa alla definizione dell’importo di partenza al fine del calcolo della sanzione e l’altra che illustra i valori minimi e massimi applicabili in rapporto alla specifica categorizzazione della violazione, all’interno dei quali andrà a collocarsi la sanzione effettivamente comminata.

Notifica di *data breach*: a dicembre 2023 sono state adottate, in via definitiva, dopo la consultazione pubblica, le linee guida 9/2022 che recano l’aggiornamento delle linee guida del Gruppo Art. 29 sulle notifiche di violazione dei dati personali (WP250 rev.01). L’aggiornamento riguarda solo una riformulazione del processo di notifica della violazione dei dati per i titolari del trattamento non stabiliti nel SEE. Conformemente alle linee guida 8/2022 sull’identificazione dell’autorità di controllo capofila del titolare o responsabile del trattamento, le linee guida riviste affermano ora che “la mera presenza di un rappresentante in uno Stato membro non attiva il sistema dello

21

[Linee guida CEPD su procedure di coerenza](#)

[Altre linee guida CEPD](#)

21

Modelli di
progettazione
ingannevoli nei *social
media*

*Data Protection Guide
for small business*

Trasferimento dei dati –
adeguatezza *ex art. 45*
del RGPD – DPF

sportello unico”. In caso di *data breach*, i titolari del trattamento che non hanno una sede nell’UE dovranno quindi confrontarsi con le autorità di controllo locali in ciascuno Stato membro in cui operano, tramite i rispettivi rappresentanti locali. Il CEPD ha deciso di pubblicare sul proprio sito web un elenco di contatti per la notifica di violazione dei dati con i collegamenti pertinenti e le lingue accettate per tutte le autorità di protezione del SEE, al fine di agevolare il processo di notifica delle violazioni.

Il CEPD ha adottato, a dicembre 2023, in via definitiva, dopo consultazione pubblica (26 i contributi ricevuti), le linee guida sui modelli di progettazione ingannevoli nelle piattaforme di *social media* (linee guida 3/2022 già adottate dal CEPD il 14 marzo 2022 – v. Relazione 2022, p. 185). Le linee guida – il cui titolo è stato modificato a seguito della consultazione pubblica per evitare l’originario riferimento ai cd. *dark pattern* – forniscono indicazioni per valutare ed evitare le tecniche sleali che inducono gli utenti a compiere azioni indesiderate e ad assumere decisioni potenzialmente dannose in merito al trattamento dei loro dati personali. Il testo ora contiene esempi di *best practices* (quali *dashboard* in materia di *privacy*, informazioni contestuali, URL auto esplicativo per le impostazioni di protezione dei dati, modulo per l’esercizio dei diritti dell’interessato), due nuovi allegati relativi a casi d’uso e un sommario introduttivo.

Il CEPD ha adottato, ad aprile 2023, una guida sulla protezione dei dati per sensibilizzare le piccole e medie imprese in merito al RGPD e fornire alle stesse informazioni pratiche sulla conformità al RGPD in un formato accessibile e facilmente comprensibile.

La guida copre vari aspetti del RGPD, dalle basi giuridiche per il trattamento dei dati, ai diritti degli interessati, alle violazioni dei dati e altro ancora. Contiene video, infografiche, diagrammi di flusso interattivi e altri materiali pratici per aiutare le PMI a rispettare il RGPD. Inoltre, la guida contiene una panoramica dei materiali utili sviluppati per le PMI dalle autorità nazionali per la protezione dei dati. La guida, attualmente disponibile in inglese, sarà tradotta in altre lingue dell’UE; essa rappresenta una delle azioni di sensibilizzazione del CEPD per l’anno di riferimento ed è stata inclusa come iniziativa chiave nella strategia 2021-2023 del Comitato.

Nel menzionato contributo alla revisione del RGPD del 12 dicembre 2023 (v. *supra*), il CEPD ha ribadito, in tema di trasferimento dei dati fuori dall’Unione europea, l’importanza di continuare a lavorare sulle decisioni di adeguatezza di Paesi terzi e organizzazioni internazionali e, nel 2023, è intervenuto due volte sul tema con il parere (parere n. 5/2023) sul progetto di decisione sull’adeguatezza del “Quadro sulla *privacy* dei dati UE-USA” (*EU-US Data Privacy Framework*, di seguito anche DPF UE-USA), presentato dalla Commissione europea il 13 dicembre 2022 (v. Relazione 2022, p. 181), e con uno *statement* relativo alla revisione della decisione di adeguatezza relativa al Giappone.

Con il parere 5/2023, il CEPD ha accolto con favore i miglioramenti sostanziali del DPF UE-USA che, come il *Privacy Shield*, è un sistema di autocertificazione attraverso il quale le organizzazioni statunitensi aderenti si impegnano a rispettare una serie di principi sulla *privacy* – i cd. *Data Privacy Framework Principles* (all. I al progetto di decisione) – emanati dal Dipartimento del commercio degli Stati Uniti. In particolare, il CEPD ha apprezzato sia l’introduzione dei principi di necessità e proporzionalità per la raccolta di dati per finalità di *intelligence* e delle maggiori garanzie previste in merito all’indipendenza del *Data protection review Court* (DPRC) rispetto al precedente meccanismo del difensore civico (*Ombudsperson*), sia il nuovo meccanismo di ricorso soggetto all’esame da parte del *Privacy and Civil Liberties Oversight Board* (PCLOB).

Tuttavia, il CEPD ha anche evidenziato alcuni punti di criticità. In merito alle garanzie legate agli aspetti commerciali dell’accordo, ha invitato la Commissione a fornire chiarimenti sulle garanzie previste in merito al diritto di accesso e alla

esenzione per le informazioni accessibili al pubblico, sull'assenza di alcune definizioni chiave, sull'applicazione dei principi DPF ai responsabili del trattamento, e sulla mancanza di norme specifiche in merito al processo decisionale automatizzato e alla profilazione. Il CEPD ha ribadito inoltre che il livello di protezione non deve essere compromesso dai trasferimenti successivi e ha invitato la Commissione a chiarire che le garanzie imposte dal destinatario iniziale all'importatore nel Paese terzo devono essere efficaci alla luce della legislazione di un Paese terzo, prima di procedere al trasferimento successivo.

Per quanto riguarda l'accesso del governo ai dati trasferiti negli Stati Uniti, il CEPD ha riconosciuto i miglioramenti significativi apportati dall'*Executive Order* (EO) 14086 che introduce i concetti di necessità e proporzionalità per quanto riguarda la raccolta di dati da parte dell'*intelligence* statunitense, ma ha sottolineato l'importanza di attendere l'adozione, da parte delle agenzie di *intelligence* statunitensi, delle procedure aggiornate per concretizzare l'ordine esecutivo 14086. Il CEPD ha espresso inoltre preoccupazione per la mancanza di un obbligo di autorizzazione preventiva da parte di un'autorità indipendente per la raccolta di dati *in bulk* ai sensi dell'ordine esecutivo 12333, nonché per la mancanza di una revisione indipendente sistematica *ex post* da parte di un tribunale o di un organismo equivalentemente indipendente.

Il CEPD ha invitato inoltre la Commissione a prevedere che, dopo il primo riesame della decisione di adeguatezza, i successivi riesami debbano aver luogo almeno ogni tre anni coinvolgendo lo stesso CEPD.

Alla luce delle criticità sopra evidenziate e della risoluzione del Parlamento europeo dell'11 maggio (2023/2501(RSP)) – che condivideva le perplessità ed evidenziava ulteriori aspetti dell'accordo da chiarire –, la Commissione ha modificato il progetto originariamente presentato e, all'esito dell'introduzione nell'ordinamento statunitense delle attese norme procedurali interne volte a dare applicazione all'accordo (i cd. *implementing acts*), ha adottato la decisione di esecuzione 4745/2023 relativa al livello adeguato di protezione dei dati personali nell'ambito del quadro UE-USA sulla *privacy* dei dati (che contiene in allegato il quadro UE-USA sulla *privacy* dei dati - DPF UE-USA).

A seguito dell'adozione della decisione, il CEPD ha predisposto una nota informativa intesa a fornire alcune indicazioni sui trasferimenti verso gli Stati Uniti. La nota spiega che la decisione di adeguatezza coprirà tutti i trasferimenti effettuati verso società autocertificate e presenti nella *Data Privacy Framework List* (che potranno essere posti in essere senza la necessità di adottare alcuna misura di protezione ulteriore) e che le garanzie introdotte nell'ordinamento USA sono applicabili anche ai trasferimenti effettuati, sulla base di altri strumenti (quali le SCC o le BCR), verso soggetti che non rientrino nel DPF.

Sempre in tema di adeguatezza dei Paesi terzi, a luglio 2023 il CEPD ha adottato una dichiarazione relativa al primo rapporto presentato dalla Commissione europea in merito alla revisione della decisione di adeguatezza del Giappone già adottata il 23 gennaio 2019. La dichiarazione si è concentrata sulla valutazione delle recenti modifiche del quadro giuridico giapponese che hanno interessato solo i trattamenti per finalità commerciali. Il CEPD ha accolto con favore le modifiche che sembrano avvicinare ulteriormente i due sistemi giuridici, in particolare con riguardo all'estensione del diritto di opporsi a un trattamento, al rafforzamento dell'obbligo di notificare le violazioni dei dati all'Autorità giapponese per la protezione dei dati e alle persone fisiche nonché all'ampliamento dell'ambito di applicazione della legge giapponese sulla protezione delle informazioni personali (la quale non esclude più i dati personali che sono "impostati per essere cancellati" entro sei mesi). Allo stesso tempo, il CEPD ha concordato con la Commissione europea sull'opportunità di monitorare l'applicazione delle nuove disposizioni per quanto riguarda la nuova

**La prima revisione
della decisione di
adeguatezza del
Giappone**

Certificazioni e trasferimenti dei dati**Interplay tra art. 3 e capo V del RGPD****BCR e raccomandazioni 1/2022**

categoria di informazioni personali “pseudonimizzate” e l’uso del consenso in situazioni ove sussista uno squilibrio di potere fra interessati e titolari del trattamento.

Nel corso del 2023 il CEPD ha definito alcune delle linee guida in materia di trasferimenti di dati già adottate nel 2022 e poi sottoposte a consultazione pubblica (v. Relazione 2022, p. 180 e ss.).

Le linee guida 7/2022 sulle certificazioni come strumenti di trasferimento dei dati all’estero, adottate il 30 giugno 2022, sono state approvate in via definitiva, dopo la consultazione pubblica, a febbraio 2023. Tali linee guida hanno chiarito, tra l’altro, che la verifica effettuata dall’organismo di certificazione in merito alla valutazione dell’importatore circa legislazione e prassi del Paese terzo in cui lo stesso è stabilito può essere utilizzata come uno degli elementi mediante i quali l’esportatore può dimostrare il rispetto degli obblighi di cui al Capo V del RGPD. Inoltre le medesime linee guida hanno stabilito che gli “impegni vincolanti e esigibili” che devono accompagnare l’uso della certificazione ai fini del trasferimento non possono essere costituiti da un altro strumento del capo V (come, ad esempio, le SCC - clausole contrattuali modello), poiché tali impegni devono garantire il rispetto da parte dell’importatore dei criteri di certificazione sulla base dei quali lo stesso ha ottenuto il proprio certificato.

Dopo la consultazione pubblica che ha avuto termine a gennaio 2022, sono state adottate a febbraio 2023, in via definitiva, le linee guida sull’interazione tra art. 3 e Capo V del RGPD (linee guida 7/2022, v. Relazione 2022, p. 181). Anche tenuto conto dei contributi ricevuti nel corso della consultazione pubblica (una sessantina), il testo è stato modificato per fornire ulteriori chiarimenti su diversi aspetti. Sono stati a tal fine introdotti ulteriori 5 esempi che vanno ad aggiungersi ai 7 presenti nella prima versione. È stato aggiunto un chiarimento sulle responsabilità nei casi di trasferimento effettuato da un responsabile del trattamento (per conto del suo titolare). Al riguardo, è stato precisato che il responsabile deve garantire il rispetto delle disposizioni del Capo V del RGPD alla luce delle istruzioni ricevute dal titolare del trattamento e che quest’ultimo, poiché il trasferimento è un’attività di trattamento svolta per proprio conto, potrebbe anche essere responsabile per le violazioni del medesimo Capo V oltre che per l’eventuale individuazione di un responsabile del trattamento che non fornisca garanzie sufficienti ai sensi dell’art. 28 del RGPD. Ciò vale anche nel caso in cui il responsabile del trattamento situato in UE riceva richieste di accesso ai dati da parte di soggetti pubblici di Paesi terzi.

Nel testo, inoltre, è stata inclusa una nuova sezione sulle garanzie che titolari e responsabili devono assicurare qualora i dati personali siano trattati al di fuori del SEE, in assenza di alcun trasferimento. In breve, i titolari e/o i responsabili i cui trattamenti sono soggetti al RGPD sono responsabili delle operazioni di trattamento, indipendentemente dal luogo in cui le stesse hanno luogo, e il trattamento in Paesi terzi può comportare rischi maggiori (anche in relazione a un accesso sproporzionato ai dati da parte di soggetti pubblici di tali Paesi e possibili conflitti di legge) che devono essere identificati e affrontati affinché il trattamento sia lecito ai sensi del RGPD.

Nel giugno 2023 sono state adottate, in via definitiva e sempre a seguito di consultazione pubblica (quindici i contributi ricevuti), le raccomandazioni 01/2022 (v. Relazione 2022, p. 181) sulla domanda di approvazione e sugli elementi e principi contenuti nelle norme vincolanti d’impresa (BCR) per titolari del trattamento (art. 47 del RGPD). Le raccomandazioni sostituiscono il documento di lavoro WP 256, rev. 01 (v. Relazione 2017, p. 167) e contengono indicazioni in ordine alle garanzie che le BCR devono contenere per poter essere approvate ed utilizzate quali strumento di trasferimento verso Paesi terzi. Una sezione iniziale contiene anche il modello per presentare la richiesta di approvazione delle BCR all’autorità capofila.

Sulla base del WP 256 sono state altresì approvate diciotto BCR per titolari (tra le quali anche la prima BCR per la quale il Garante ha agito in qualità di autorità capofila, cfr. cap. 18). Nove sono state invece le BCR per responsabili adottate nel corso dell’anno.

Utilizzo del *cloud* da parte dei soggetti pubblici: il CEPD ha adottato, a gennaio 2023, la relazione predisposta dal *Coordinated Enforcement Framework* (CEF) sui risultati della sua prima azione coordinata di enforcement, incentrata sull'uso di servizi basati su *cloud* da parte del settore pubblico (v. Relazione 2022, p. 179). Sono state 22 le autorità (compreso il Garante) che, nel corso del 2022, hanno avviato indagini coordinate sull'uso di servizi basati su *cloud* da parte del settore pubblico. In tutto lo SEE sono stati interpellati circa 100 enti pubblici (ivi comprese le istituzioni europee) che hanno competenze in svariati settori (quali sanità, finanza, imposte, istruzione, acquirenti e fornitori di servizi informatici) ed è emerso che gli stessi spesso incontrano difficoltà nell'ottenere servizi e prodotti conformi al RGPD. La relazione, soffermatasi sugli aspetti maggiormente controversi, sottolinea la necessità per gli enti pubblici di agire nel pieno rispetto del RGPD e fornisce indicazioni per le organizzazioni che intendano utilizzare prodotti o servizi basati su *cloud*. In allegato la relazione contiene anche il *report* delle attività svolte da ciascuna autorità.

Responsabile della protezione dei dati (RPD): nel corso del 2023, 25 autorità fra cui il GEPD hanno avviato indagini coordinate sul tema del ruolo e delle funzioni del RPD nell'ambito della seconda azione coordinata del CEF. Sono stati contattati vari titolari e RPD che coprono un'ampia gamma di settori (sia pubblici che privati), e sono state ricevute e analizzate oltre 17.000 risposte che offrono preziose informazioni sul profilo, la posizione e l'attività dei RPD a distanza di 5 anni dalla piena applicazione del RGPD. Il Garante ha indirizzato il questionario a circa 60 RPD di primarie società operanti nel settore privato e di enti pubblici di grandi dimensioni. Le risposte in forma aggregata sono confluite all'interno dell'appendice della relazione del Comitato contenente statistiche e grafici, mentre gli esiti dell'azione condotta dal Garante a livello nazionale sono stati sinteticamente riportati nella relazione nazionale. I risultati dei questionari inviati dal Garante hanno evidenziato diversificazioni negli enti coinvolti in ordine, fra l'altro, al possesso delle necessarie competenze previste dal Regolamento e all'effettivo coinvolgimento del RPD nelle questioni attinenti alla protezione dei dati personali oltre che nella chiara definizione del complesso dei compiti affidati dal titolare al RPD.

Anche nel 2023, diverse autorità di protezione dei dati, destinatarie di 101 reclami presentati dall'associazione NOYB in merito ai trasferimenti di dati effettuati a seguito dell'utilizzo dei servizi di Google Analytics, Facebook Pixel e Facebook Connect, si sono attivamente confrontate nell'ambito di una *Task Force* appositamente costituita al fine di consentire l'applicazione coerente del RGPD nei casi in questione (cfr. par. 18). Il *report* della *Task Force*, adottato a marzo 2023, contiene una sintesi della posizione comune e, in particolare, la determinazione relativa alla necessità di sospensione dei flussi di dati all'estero nei casi in cui le appropriate garanzie previste dal Capo V del RGPD non possono essere applicate alla luce della legislazione del paese di destinazione.

Anche nel 2023 il CEPD ha garantito un approccio uniforme tra le autorità di protezione dei dati nella definizione ed applicazione dei requisiti di accreditamento per gli organismi di monitoraggio dei codici di condotta. Il RGPD non fissa un unico insieme di requisiti per l'accREDITAMENTO di tali organismi, bensì demanda all'autorità di controllo competente la redazione dei requisiti per l'accREDITAMENTO degli organismi di monitoraggio sulla base dell'art. 41, par. 2, del RGPD. Questi ultimi sono quindi adottati da ciascuna autorità di controllo competente in linea con il parere espresso dal CEPD, in ottemperanza al meccanismo di coerenza. Nel corso del 2023, il CEPD si è espresso in particolare sui progetti dei requisiti di accREDITAMENTO presentati dall'Autorità di controllo svedese (parere 11/2023).

Requisiti per l'accREDITAMENTO degli organismi di certificazione: altrettanto importante è stata l'attività del CEPD volta ad assicurare la coerenza nell'applicazione del RGPD con riferimento alla definizione dei requisiti aggiuntivi di accREDITAMENTO degli

Azioni coordinate del CEPD

Report della Task Force 101 complaint

Codici di condotta e organismi di monitoraggio

Certificazione dei trattamenti

21

organismi di certificazione da parte delle autorità di controllo competenti ai sensi dell'art. 43, par. 3, del RGPD (cfr. le linee guida del CEPD 4/2018 sull'accREDITAMENTO degli organismi di certificazione, Relazione 2018, p. 145). Nel 2023 il CEPD ha reso il parere previsto dall'art. 64, par. 1, lett. c), del RGPD in ordine ai progetti di requisiti aggiuntivi per l'accREDITAMENTO degli organismi di certificazione predisposti dalle Autorità di controllo slovena (parere 38/2023), lussemburghese (parere 37/2023), croata (parere 13/2023), cipriota (parere 12/2023) e maltese (parere 4/2023).

Procedura per l'adozione dei pareri del CEPD in materia di certificazioni: il CEPD ha adottato (febbraio 2023) una procedura per l'adozione dei pareri relativi ai criteri nazionali di certificazione e ai sigilli europei di protezione dei dati. Il documento è rivolto a tutti i titolari di schemi di certificazione e mira a semplificare e facilitare l'adozione dei pareri del CEPD in merito, chiarendo il processo di approvazione dei criteri di certificazione nazionali ed europei, nonché dei criteri di certificazione intesi come strumenti per i trasferimenti internazionali. A tal fine il documento delinea i passaggi procedurali che le autorità di controllo devono compiere dal momento in cui i criteri vengono sottoposti al loro esame dai titolari dello schema di certificazione fino al momento in cui comunicano al Presidente del CEPD se intendono seguire il parere di quest'ultimo.

Pareri su schemi di certificazione della protezione dati a livello nazionale: il CEPD il 19 settembre 2023 ha adottato ai sensi dell'art. 64 del RGPD il parere 15/2023 sulla decisione dell'Autorità olandese di approvazione dei criteri dello schema di certificazione della protezione dei dati a livello nazionale, *Brand Compliance*. Lo schema, applicabile ai titolari, ai contitolari e ai responsabili del trattamento, è volto a dimostrare la conformità delle attività di trattamento coperte dalla certificazione al complesso delle regole e dei principi RGPD. Il parere mira a garantire la coerenza e la corretta applicazione dei criteri di certificazione tra le diverse autorità di controllo nel SEE. A tal fine, il CEPD ha indicato una serie di modifiche al progetto di criteri di certificazione ritenute necessarie per assicurare un'applicazione coerente del RGPD, tra cui la necessità di chiarire l'ambito nazionale dello schema di certificazione, la possibilità di certificare i sub-responsabili del trattamento, nonché i criteri sui trasferimenti internazionali. A seguito dell'approvazione definitiva dei criteri da parte dell'Autorità di controllo olandese, aziende, autorità pubbliche, associazioni e altre organizzazioni con sede in Olanda hanno la possibilità di dimostrare che le loro attività di trattamento dei dati sono conformi al RGPD.

Lettera ad Accredia: nel contesto dell'approvazione dei criteri di certificazione di *Europrivacy*, come sigillo europeo per la protezione dei dati, il CEPD, in risposta ad Accredia, l'ente di accREDITAMENTO italiano, con lettera 1° agosto 2023 ha avuto occasione di pronunciarsi sull'interpretazione e l'applicazione del RGPD in materia di certificazione e accREDITAMENTO, chiarendo, tra l'altro, i ruoli e le competenze dei diversi attori coinvolti nelle procedure di certificazione e accREDITAMENTO ai sensi del RGPD.

Uno dei punti cardine del lavoro del CEPD in materia finanziaria ha riguardato l'euro digitale la cui fase preparatoria, finalizzata allo sviluppo e alle sperimentazioni di tale moneta, è stata avviata dalla Banca centrale europea (BCE) a novembre 2023. L'euro digitale mira a fornire ai cittadini un mezzo di pagamento aggiuntivo, oltre al contante, che permetta di effettuare pagamenti elettronici, sia *online* che *offline*.

La discussione, avviata nel 2021, anche attraverso l'interlocuzione con la BCE, è culminata nell'adozione, il 17 ottobre 2023, del parere congiunto CEPD/GEPD 2/2023 sulla proposta di regolamento sull'istituzione di un euro digitale.

Il CEPD e il GEPD riconoscono che la proposta di regolamento affronta molti profili concernenti la riservatezza ed in particolare la previsione sulla modalità *offline* per ridurre al minimo il trattamento dei dati personali. Il parere accoglie inoltre con favore il fatto che gli utenti dell'euro digitale avranno sempre la possibilità di scegliere se pagare in euro digitali o in contanti. Allo stesso tempo formula diverse

Euro digitale

raccomandazioni per garantire i più elevati standard di protezione dei dati personali e *privacy* e per garantire che vengano trattati solo i dati personali necessari degli utenti evitando un'eccessiva centralizzazione delle informazioni da parte della BCE o delle banche centrali nazionali. Secondo la proposta di regolamento, infatti, la BCE e le banche centrali nazionali possono istituire un unico punto di accesso per verificare che l'importo di euro digitali detenuti da ciascun utente non superi l'importo massimo consentito, attraverso specifici identificatori degli utenti. Al riguardo, il parere consiglia di valutare se il punto di accesso unico a tal fine istituito sia necessario e proporzionato, sottolineando che, in alternativa, sono fattibili misure tecniche che consentono una memorizzazione decentralizzata di tali identificatori. Viene inoltre raccomandato di introdurre una "soglia di *privacy*" al di sotto della quale non vengano tracciate né le transazioni *offline* né quelle *online* di basso valore a fini di antiriciclaggio (AML) e per combattere il finanziamento del terrorismo (CFT). Infine, il parere sottolinea l'opportunità di precisare ulteriormente nella proposta di regolamento le responsabilità in materia di protezione dei dati della BCE e dei fornitori dei servizi di pagamento, definendo le basi giuridiche dei rispettivi trattamenti e le categorie di dati personali necessari per l'emissione, la distribuzione e l'uso dell'euro digitale.

Un'altra tematica in ambito finanziario che ha notevolmente impegnato il CEPD concerne il trattamento dei dati personali nell'ambito delle disposizioni contro il riciclaggio e il terrorismo (AML/CFT), un settore in continua evoluzione per il susseguirsi di iniziative legislative UE ed oggetto di uno specifico piano di azione della Commissione europea (7 maggio 2020) e di un pacchetto di quattro proposte legislative pubblicate dalla Commissione il 20 luglio 2021.

In particolare, con lettera 28 marzo 2023, il CEPD ha indirizzato alla Commissione, al Consiglio e al Parlamento UE una serie di considerazioni in merito alla proposta di regolamento della Commissione del 20 luglio 2021 sulla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. A fronte dell'introduzione da parte del Consiglio di emendamenti che prevedono nuove norme sulla condivisione di dati (cd. *data sharing*) tra i soggetti obbligati (cd. *obliged entities*) e pubblici, e tra le stesse *obliged entities*, la lettera evidenzia come le nuove proposte non rispondano ai principi di proporzionalità e di necessità, né di qualità della legislazione, e raccomanda di non includere tali proposte nel testo legislativo finale.

Applicazione dell'art. 5, par. 3, della direttiva *e-Privacy*: il 15 novembre 2023 il CEPD ha adottato linee guida sull'ambito tecnico di applicazione dell'art. 5, par. 3, della direttiva 2002/58/CE che mirano a chiarire quali operazioni, in particolare quali tecniche di tracciamento nuove ed emergenti, siano coperte dalla normativa vigente, nonché a fornire maggiore certezza giuridica ai titolari del trattamento e agli interessati. Per chiarire l'operatività dell'articolo, le linee guida esaminano le nozioni ivi richiamate quali "informazione", "apparecchiatura terminale di un abbonato o utente", "rete di comunicazione elettronica", "accesso" e "accesso a informazioni memorizzate/archiviazione". Le linee guida includono anche una serie di casi d'uso pratici che presentano tecniche di tracciamento comuni.

Iniziativa volontaria *cookie pledge*: il CEPD ha elaborato una lettera rivolta alla Commissione europea in merito all'iniziativa volontaria cd. *cookie pledge*. L'iniziativa – accolta con favore del CEPD – è stata sviluppata dalla Commissione europea per rispondere alle preoccupazioni relative al fenomeno della cosiddetta *cookie fatigue* e consiste in un impegno volontario delle imprese a semplificare la gestione dei *cookie* e le scelte pubblicitarie personalizzate da parte dei consumatori. In base ai principi dell'iniziativa, gli utenti dovrebbero poter ricevere informazioni concrete su come vengono trattati i loro dati, nonché sulle conseguenze dell'accettazione dei diversi tipi di *cookie*, garantendo loro un maggiore controllo sul trattamento dei dati che li riguardano. Sempre nell'ottica della riduzione dell'affaticamento determinato dai

21

Antiriciclaggio
e contrasto al
finanziamento del
terrorismo

Direttiva *e-Privacy*

21

**Linee guida sul
riconoscimento facciale
nel settore delle attività
di polizia e giustizia**

**Linee guida sui
trasferimenti soggetti
a garanzie adeguate ai
sensi della LED**

cookie, il consenso non dovrebbe essere chiesto nuovamente nell'anno successivo a quello in cui è stato rifiutato. Resta fermo tuttavia che, come espressamente segnalato nella lettera del CEPD, l'adesione ai principi volontari dell'iniziativa non equivale al pieno rispetto del RGPD o della direttiva *e-Privacy* e che le autorità per la protezione dei dati restano competenti a esercitare i propri poteri quando necessario.

Il 26 aprile 2023, a seguito della consultazione pubblica, il CEPD ha adottato la versione finale delle linee guida 5/2022 sulla tecnologia di riconoscimento facciale nel settore delle attività di polizia e giustizia (v. Relazione 2022, p. 187 e ss.). Le linee guida forniscono indicazioni ai legislatori nazionali e dell'UE, nonché alle autorità di contrasto, sull'implementazione e l'utilizzo dei sistemi tecnologici di riconoscimento facciale. In particolare, le linee guida sottolineano che gli strumenti di riconoscimento facciale dovrebbero essere utilizzati solo nel rigoroso rispetto della direttiva 2016/680 (LED) solo ove ciò risulti necessario e proporzionato, come stabilito nella Carta dei diritti fondamentali. Nelle linee guida si ribadisce la richiesta di vietare l'uso della tecnologia di riconoscimento facciale in spazi accessibili al pubblico, come già richiesto nel parere adottato congiuntamente con il GEPD sulla proposta di regolamento UE sull'IA (cfr. cap. 16).

Il 19 settembre 2023 il CEPD ha adottato le linee guida sull'art. 37 della LED che disciplina i trasferimenti di dati personali da parte delle autorità competenti dei Paesi UE per le attività di polizia giudiziarie verso le altre autorità competenti di Paesi terzi o organizzazioni internazionali. Le linee guida, sottoposte a consultazione pubblica, mirano a fornire indicazioni pratiche in merito alle garanzie adeguate che le autorità competenti devono adottare nei trasferimenti internazionali, con particolare riguardo ai fattori rilevanti per valutare l'esistenza di tali garanzie. In proposito, le linee guida costituiscono un punto di riferimento per i Paesi dell'UE che intendono configurare o modificare gli strumenti giuridicamente vincolanti per i trasferimenti di dati previsti dall'art. 37 della LED, elencando, tra l'altro, gli elementi che tali strumenti dovrebbero contenere per fornire garanzie adeguate. Al contempo, le linee guida offrono indicazioni alle autorità di controllo nel caso in cui siano consultate o altrimenti coinvolte nella negoziazione di tali strumenti, o laddove ne verifichino successivamente l'attuazione. Inoltre, le linee guida chiariscono il ruolo delle autorità di protezione dei dati rispetto agli obblighi di responsabilizzazione incombenti sui titolari del trattamento ove questi ritengano, dopo aver valutato le circostanze relative ai trasferimenti, che sussistano garanzie adeguate alla protezione dei dati, e forniscono altresì alcuni esempi utili a classificare e valutare tali circostanze.

21.2. *La cooperazione delle autorità di protezione dati nel settore libertà, giustizia e affari interni*

L'Autorità ha continuato a partecipare attivamente alle riunioni dei gruppi di lavoro in ambito europeo in materia di sicurezza e giustizia.

21.2.1. *Comitato di controllo coordinato*

Com'è noto, il Comitato di controllo coordinato (CSC) si occupa del coordinamento tra le autorità nazionali di controllo e il GEPD per la supervisione dei sistemi IT su larga scala utilizzati per le attività di cooperazione di polizia e giudiziaria.

Nel corso del 2023, è stata data definitiva attuazione alla transizione all'interno del Comitato dei lavori dei sottogruppi, prima autonomi, riguardanti il controllo dei sistemi SIS, EUROPOL, EUROJUST, EPPD.

Al riguardo si segnala che, a livello metodologico, a partire dall'incontro tenutosi a giugno 2023, il Comitato ha avviato un dialogo con i rappresentanti della società

civile e autorità non governative al fine di attuare uno scambio di opinioni e indicazioni operative relative agli aspetti più critici dei vari sistemi.

Come anticipato, è stato completato il passaggio di consegne delle attività ancora in essere dal SIS SCG al CSC, in particolare con riferimento a quelle relative al “Questionario sull’art. 36” (vecchio regolamento SIS). Nel mese di aprile 2023 è stata pubblicata la cosiddetta guida all’accesso Schengen (cfr. *A guide for exercising data subjects’ rights: the right of access, rectification and erasure*, disponibile sul sito del GEPD). Tra le questioni trattate, la presidenza del Comitato ha evidenziato quella dei cd. nuovi *alert*, con particolare riferimento a quelli definiti all’art. 40 del reg. 1862/2018 e relativi alle “Segnalazioni di ignoti ricercati a fini di identificazione in conformità del diritto nazionale”, circa i quali è stata rilevata la necessità di monitorare con attenzione le statistiche fornite dalle autorità di polizia al fine di valutare le modalità di utilizzo dei medesimi. Sulla scorta della relazione successivamente presentata dal responsabile della protezione dei dati di EU-LISA relative al monitoraggio e controllo del sistema centrale Schengen, è stata condivisa la necessità di una riflessione sull’opportunità di effettuare una verifica in ciascuno Stato membro circa i criteri di ammissibilità dell’utilizzo di dati biometrici (impronte digitali) per le segnalazioni sopra menzionate ove riferite a soggetti sospettati della commissione di crimini gravi, anche con riguardo alla loro base legale.

Per parte sua, la Commissione europea ha illustrato nel corso dell’anno le statistiche e le novità introdotte dal nuovo sistema SIS. In particolare, quanto all’inserimento di impronte digitali, si prevede una soglia alta per l’ammissibilità di un *alert* sulle medesime (es. gravità crimine, certezza sull’autore del reato, ecc).

In previsione della realizzazione di ispezioni da effettuarsi insieme con il GEPD presso la sede centrale di EUROPOL, si è convenuto sulla necessità di una preliminare indagine a livello nazionale, a cura di ciascuna autorità – attraverso richieste di informazioni e ispezioni presso le competenti autorità nazionali di polizia – finalizzata alla verifica delle modalità con cui sono trattati i dati che vengono inviati al sistema EUROPOL.

In particolare, le verifiche dovrebbero riguardare le procedure con cui nella prassi le autorità nazionali di polizia effettuano la valutazione sui rischi del trattamento, l’eventuale acquisizione di informazioni non pertinenti, eccedenti o non proporzionate e, più in generale, i modi con cui vengono acquisiti i dati che, successivamente, confluiscono nel sistema. Le predette verifiche dovrebbero concentrarsi anche sulle modalità di raccolta dei dati relativi ai PNR e al loro utilizzo da parte delle autorità nazionali di polizia, con particolare riferimento a quegli Stati membri che sono risultati attivi nel processo di raccolta e trasmissione di detti dati ad EUROPOL, con indicazione delle categorie di dati che sono state specificamente raccolte e trasmesse. Sulla base di tali verifiche si procederà alla redazione di una lista di *best practices* e punti critici, da utilizzare nelle ispezioni programmate.

In modo simile è stato convenuto di operare con riguardo al sistema informativo FRONTEX, in merito al quale le autorità hanno sollevato dubbi e manifestato la necessità di approfondire le verifiche con riferimento al suo effettivo funzionamento e al contributo al medesimo operato delle autorità nazionali di polizia.

Alla luce delle informazioni comunicate circa l’evoluzione tecnica dell’architettura del sistema EUROPOL, che consente di effettuare la ricerca di ulteriori categorie di dati contenuti all’interno del sistema, anche attraverso interrogazioni complementare automatizzate (si vedano quelle che utilizzano il *database* del NCMEC - *National Center for Missing and Exploited Children*, incrociandone i dati con quelli provenienti da altri archivi), sono state condivise tra i partecipanti le preoccupazioni e criticità nella prospettiva della progressiva interoperabilità del sistema EUROPOL con altri sistemi d’informazione, con particolare riguardo alla necessità di sensibi-

Sistema d’informazione Schengen (SIS)

Sistema d’informazione EUROPOL

21

Sistema d'informazione EUROJUST

Sistema d'informazione della Procura europea (EPPO)

lizzare le autorità nazionali di polizia a non abusare di queste nuove potenzialità. È stata esaminata e poi approvata la guida all'esercizio dei diritti degli interessati per l'accesso al sistema EUROPOL, che è stata aggiornata per quanto concerne i dettagli di contatto per ogni Stato membro. Il GEPD, che ha presentato gli esiti dell'ispezione annuale effettuata presso EUROPOL, ha sottolineato l'importanza di attenzionare la figura del minore, da considerarsi sempre una vittima nello scenario criminale, e ha ribadito l'importanza di programmare ispezioni a cura delle singole autorità di controllo presso i cd. NCP (*National Contact Point*).

È stato altresì discusso di una possibile azione coordinata con riferimento ai dati PNR e sulla classificazione degli interessati nelle diverse categorie. Nello specifico, è stata richiamata l'attenzione sulla "PNR request form" e sulla sua struttura, sottolineando l'importanza di assicurare il rispetto dei requisiti di necessità e proporzionalità, ed è stata effettuata una riflessione sui criteri stabiliti per consultare i dati PNR.

Con riferimento ai reclami presentati nei confronti di EUROPOL, è stata evidenziata la difficoltà di rispettare il termine di tre mesi previsto dal relativo regolamento per fornire riscontro alle richieste di accesso.

Quanto al sistema di informazione EUROJUST, sono state evidenziate alcune criticità nell'ambito della cooperazione con le strutture nazionali di EUROJUST (quali il mancato riscontro alle richieste inviate a mezzo posta) nell'ottica della possibile definizione di un approccio comune all'interno del gruppo.

Con riguardo alla partecipazione della Danimarca alla supervisione dei sistemi informativi EUROJUST ed EUROPOL, ai sensi dell'art. 62 del reg. (EU) 2018/1725 (EU-DPR), tenuto conto che la stessa, pur essendo membro dell'Unione europea, non ha implementato né il reg. (EU) 2016/794 (EUROPOL Regulation, ER) né il reg. (EU) 2018/1727 (EUROJUST Regulation, EJR), si è rilevato che da un punto di vista formale l'attuale quadro normativo impedisce una cooperazione con gli Stati che non hanno implementato i due regolamenti ER ed EJR nei propri ordinamenti nazionali: si configurano, pertanto, diverse criticità in caso di accesso delle rispettive autorità di polizia e giudiziarie ai due *database* in questione (es. in caso di presa visione di documentazione riservata ovvero in caso di votazione su di una decisione del Comitato). Le autorità sono state invitate a svolgere una valutazione approfondita del tema a livello nazionale. Per altri aspetti, l'*audit* svolto dal GEPD ha indicato che la maggior parte delle raccomandazioni formulate sono state implementate da EUROJUST.

È stato predisposto, a cura del GEPD, un protocollo d'intesa con EPPO e sono state pianificate attività di *audit* nel corso del 2023. È stata condotta un'attività di controllo presso l'ufficio nazionale portoghese dell'EPPO, con esiti positivi grazie all'integrazione dei *database* con i fascicoli (*case files*) nazionali e alla maggiore comprensione del ruolo svolto da GEPD e autorità nazionali nella supervisione dei sistemi informativi EPPO.

21.2.2. Gruppo di supervisione del sistema EURODAC

Anche nel caso del sistema EURODAC occorre evidenziare l'ampliamento delle capacità tecniche di elaborazione dati, mentre per quanto riguarda il testo del nuovo regolamento EURODAC se ne prevede l'adozione nei primi mesi del 2024. Al riguardo, è stato programmato un approfondimento dell'interazione delle sue disposizioni con altre normative di settore e, in modo particolare, con il regolamento che istituisce accertamenti nei confronti dei cittadini di Paesi terzi alle frontiere esterne degli Stati membri (cd. *Screening Regulation*), anch'esso da adottarsi nel medesimo periodo.

È stato realizzato un questionario in merito all'accesso al sistema EURODAC da parte delle autorità di *law enforcement*, con l'obiettivo di verificare l'utilizzo corrente della procedura e di fornire una guida nelle investigazioni dei crimini più rilevanti.

21.2.3. Gruppo di coordinamento della supervisione del Sistema informativo doganale

La ventunesima riunione del Gruppo di supervisione del Sistema informativo doganale (SID), l'unica tenutasi nel 2023, ha evidenziato il progressivo incremento del numero di sistemi informativi che rientrano nell'applicazione dell'art. 62 del reg. UE 2018/1725 con un conseguente aumento del carico di lavoro. È stato dunque proposto di aumentare il numero degli incontri, anche al fine di una maggiore continuità.

21.3. La partecipazione dell'Autorità in seno al Consiglio d'Europa, all'OCSE e ad altri gruppi di lavoro internazionali

È proseguita l'attività dell'Autorità nell'ambito del Consiglio d'Europa, in particolare attraverso la partecipazione al Comitato consultivo della Convenzione 108/1981, cd. T-PD, e al gruppo ristretto T-PD *Bureau* incaricato di preparare i documenti da sottoporre alla plenaria.

Anche il 2023 è stato contrassegnato da un intenso impegno del Comitato consultivo e del segretariato nell'attività di promozione della Convenzione 108 modernizzata (cd. Convenzione 108+). Nel corso dell'anno, il Protocollo emendativo della Convenzione che ne ha attualizzato i principi in uno scenario fortemente mutato da nuove tecnologie e globalizzazione è stato ratificato da un considerevole numero di Paesi e conta, al 31 dicembre 2023, 15 firme e 31 ratifiche tra cui quella dell'Italia. In entrambe le plenarie dell'anno (14-16 giugno e 15-17 novembre 2023) si è svolto un giro di tavolo di tutte le delegazioni dei Paesi che non hanno ancora ratificato e ne è emerso un certo ottimismo rispetto al tempestivo raggiungimento delle 38 ratifiche necessarie a garantire l'entrata in vigore della Convenzione 108+.

Nel corso della plenaria di giugno è stato adottato il modello di clausole contrattuali per i trasferimenti di dati personali verso Paesi terzi, ossia Paesi che non sono parte della Convenzione.

Si tratta di un documento molto importante alla luce della vocazione globale della Convenzione 108+. Esso offre un modello di clausole di cui i titolari del trattamento potranno avvalersi, in base all'art. 14(2.b) della Convenzione modernizzata, per garantire un livello appropriato di protezione nei trasferimenti di dati personali tra titolari (*controller to controller*) verso Paesi terzi. Uno degli obiettivi principali della Convenzione 108+ è infatti quello di facilitare il libero flusso di informazioni sia tra le Parti sia verso i Paesi terzi, garantendo un appropriato livello di protezione dei dati personali. La pratica dimostra che tali strumenti offrono una modalità conveniente e semplice per il trasferimento di dati oltre frontiera fra esportatori e importatori di dati nel settore privato. Oltre alle clausole tra titolare e titolare, nella plenaria di giugno è stato adottato un ulteriore modello di clausole che riguardano i trasferimenti da titolare a responsabile del trattamento (*controller to processor*), ed è stato conferito mandato al *Bureau* di cominciare a lavorare su un modello di clausole utilizzabili nei trasferimenti verso Paesi terzi tra responsabili del trattamento (*processor to processor*).

Nella plenaria di giugno sono state adottate anche le linee guida in materia di trattamenti di dati personali ai fini di antiriciclaggio e contrasto al finanziamento del terrorismo (AML/CFT), che mirano a fornire orientamenti su come integrare i requisiti della Convenzione 108+ nel settore AML/CFT assicurando un livello adeguato di protezione dei dati nei flussi di dati transfrontalieri, oltre a evidenziare alcuni aspetti concernenti l'applicazione dei principi AML/CFT in cui le garanzie di protezione dei dati dovrebbero essere rafforzate. Le linee guida sono state adottate dopo un'ampia consultazione con varie parti interessate, incluso il segretariato del GAFI, e in stretta collaborazione con il Comitato di esperti per la valutazione delle misure antiriciclaggio e il finanziamento del terrorismo (MONEYVAL) del Consiglio d'Europa.

21

Comitato consultivo
della Convenzione
108/1981 (T-PD)

La Convenzione 108+

Modello di clausole
contrattuali per i
trasferimenti di dati
personali verso Paesi
terzi

Antiriciclaggio
e contrasto al
finanziamento del
terrorismo (AML/CFT)

**Art. 11 della
Convenzione
modernizzata**

**Protezione dei dati
nell'ambito delle
elezioni e delle
procedure di voto**

Neurotecnologie

**CAI - Comitato *ad hoc*
sull'IA**

**OCSE - DGP (Gruppo di
lavoro *Data Governance
and Privacy*)**

**Report analitico sul
flusso libero dei dati
con fiducia (*data free
flow with trust - DFFT*)**

Il Comitato ha inoltre proseguito le attività di approfondimento rivolte alla stesura degli ulteriori documenti previsti dal programma di lavoro. È proseguita pertanto la riflessione sull'art. 11 della Convenzione 108+, relativo ai criteri che devono accompagnare le possibili restrizioni ed eccezioni ai principi della stessa 108+ per garantire il rispetto del diritto alla protezione dei dati.

Il Comitato ha cominciato a lavorare alle linee guida sul trattamento di dati, in particolare quelli biometrici, nell'ambito delle elezioni e delle procedure di voto, con il supporto di un esperto scientifico esterno.

L'intento delle linee guida è di invitare alla più grande cautela nell'impiego di sistemi biometrici in un settore tanto delicato, in ossequio ai principi di necessità e proporzionalità e valutando quindi la possibilità che siano adoperate modalità di trattamento alternative e meno intrusive.

È stato avviato il lavoro di approfondimento sulle neurotecnologie e diritti fondamentali in vista della futura elaborazione di specifiche linee guida. L'evoluzione di tali tecnologie e la loro combinazione con i sistemi di intelligenza artificiale stanno via via incrementando la possibilità non solo di "lettura" del cervello umano, ma anche la sua alterazione o manipolazione. Ciò impone una riflessione sulle implicazioni sui diritti fondamentali, tra cui il diritto alla *privacy* (cd. *mental privacy*) e la libera manifestazione del pensiero.

Una delle prime questioni affrontate è stata quella se e in quale misura si possa contare sugli strumenti normativi esistenti per far fronte alle nuove sfide dettate dalle neurotecnologie e se invece sia opportuno incentivare in via normativa la creazione di "nuovi diritti", come alcuni ordinamenti (ad es. in America latina) mostrano di voler fare.

Nell'ambito del Consiglio d'Europa è proseguita l'attività del Comitato *ad hoc* sull'IA - CAI che, nel solco del lavoro svolto dal precedente comitato CAHAI (v. Relazione 2021, p. 235) ha proseguito l'elaborazione di un quadro giuridico per lo sviluppo, la progettazione e l'applicazione dell'IA, basato sugli standard del Consiglio d'Europa sui diritti umani, la democrazia e lo Stato di diritto (cfr. cap. 16). Il T-PD ha seguito i lavori del CAI affinché la nuova Convenzione in materia di IA lasci immutato il quadro di tutela garantito dalla Convenzione 108+ garantendo un'applicazione coerente dei due strumenti normativi.

È proseguita l'attività dell'Autorità in ambito OCSE, in particolare attraverso la partecipazione al DGP (*Working Party on Data Governance and Privacy*), di cui il Garante detiene la vicepresidenza dal 2012 (già nel WPSPDE - *Working Party on Security and Privacy in Digital Economy*) e ha conservato la vicepresidenza per il 2024 (confermata nelle elezioni della plenaria di novembre 2023). Oltre alle attività di cui si dà conto nel prosieguo, il DGP ha continuato il monitoraggio dell'implementazione di documenti e raccomandazioni adottati dall'OCSE negli scorsi anni (fra i quali ricordiamo la raccomandazione sulla protezione dei minori *online*).

Il Gruppo nel corso del 2023 ha portato a compimento il lavoro sul flusso libero dei dati con fiducia, completando il relativo *report* che raccoglie il punto di vista del settore privato allo scopo di fornire una comprensione più completa delle sfide e delle vie da seguire per l'agenda politica globale sul tema. In particolare, le imprese indicano la necessità di principi e regole coerenti che siano trasparenti e prevedibili, forniscano un equilibrio pratico tra certezza e flessibilità e offrano soluzioni che corrispondano alle realtà aziendali, sempre nel rispetto della protezione dei dati. Il *report* evidenzia la necessità di una maggiore cooperazione normativa internazionale e di sfruttare l'intera gamma di opzioni per assicurare la fiducia delle parti nel difficile contesto del flusso di dati. Tale lavoro è stato pensato anche in coerenza con quanto svolto sul medesimo tema nel 2023 dal G7 delle autorità di protezione

dei dati per evitare la duplicazione degli sforzi, analizzando le aree di convergenza e individuando possibili azioni concrete per facilitare il DFFT globale.

Nel corso del 2023, il Gruppo ha lavorato sul tema dell'IA nella consapevolezza delle grandi opportunità, ma anche dei rischi, che il suo sviluppo sta evidenziando e della necessità di una maggiore cooperazione internazionale tra più *stakeholder* nella *governance* dei dati personali e nella *privacy*. In tale scenario, nella plenaria del DGP di aprile 2023, sono stati discussi i recenti progressi nell'IA generativa e, per il Garante, si è dato conto dell'azione italiana relativa a ChatGPT anche alla luce del provvedimento del Garante dell'11 aprile 2023, n. 114, doc. web n. 9874702, con cui sono state fornite le prescrizioni su trasparenza, diritti degli interessati e base giuridica del relativo trattamento. Alla luce delle varie presentazioni è stato ritenuto necessario l'avvio di attività congiunte con il Gruppo di lavoro OCSE sulla *governance* dell'IA (AIGO). È stata altresì presentata la prima bozza di uno schema esteso per un *report* intitolato "AI, dati e *privacy*: considerazioni preliminari su sinergie e aree di interesse e cooperazione internazionale presso l'OCSE", che intende identificare le aree prioritarie di necessaria cooperazione fra i diversi *stakeholder* per aumentare la consapevolezza sulla portata delle regole in materia di protezione dei dati e promuovere una comprensione condivisa e un'implementazione coerente. A tal fine, è stata presentata nella plenaria di novembre una proposta per la costituzione di un Gruppo di esperti dell'OCSE su AI che dal 2024 riunirà in uno stesso *forum* le diverse competenze in materia di *privacy* e *data protection* nonché nel settore dell'IA, al fine di effettuare approfondimenti sulle aree di intersezione tra i due ambiti e fornire *output* sulle scelte di *policy* da adottare in prospettiva e all'interno della cornice sovranazionale.

Il Gruppo ha focalizzato la propria attenzione anche sul tema della "finanza aperta" (*open finance*), lavorando su una bozza di *report* alla cui redazione hanno contribuito i delegati del DGP unitamente ad altri gruppi di esperti in ambito OCSE. Poiché la finanza aperta consente la condivisione e l'accesso ai dati (anche personali) del settore finanziario, essa richiede un particolare *focus* sulla protezione dei dati medesimi. Il *report* analizza i vantaggi, i rischi e le sfide connessi alla implementazione della finanza aperta e fornisce raccomandazioni per un'efficace e corretta condivisione dei dati nell'*open finance*. Il documento analizza anche altri profili inerenti alla tutela dei consumatori, in particolare quelli relativi alla prestazione del consenso e alla responsabilità, e contiene una serie di considerazioni sulla possibile creazione di un'infrastruttura tecnica per promuovere l'interoperabilità dei dati.

Nel corso del 2023, il DGP ha messo a fuoco le varie linee di congiunzione tra il settore *privacy* e quello della concorrenza *antitrust*, tema destinato ad essere sempre più centrale nei tavoli OCSE. Il Gruppo, partendo dalle diverse esperienze nazionali, ha analizzato l'impatto dei dati dei consumatori sulla concorrenza nei mercati *online* e si è interrogato sulla possibile creazione di barriere all'ingresso dovute al controllo sui dati dei consumatori nonché sui possibili rimedi. È stata condivisa la necessità di proseguire in questo lavoro e valutare (anche attraverso futuri documenti da elaborare nel 2024) come migliorare la cooperazione tra le autorità garanti in materia di concorrenza e quelle garanti della *privacy* e protezione dei dati.

Altro tema delicato e centrale è stato quello della implementazione della dichiarazione OCSE sull'accesso affidabile dei governi ai dati detenuti dai privati (*trusted government access to data*) adottata alla ministeriale OCSE di Gran Canaria nel mese di dicembre 2022 (v. Relazione 2022, p. 194). La dichiarazione parte dalla constatazione che i flussi transfrontalieri di dati sono parte integrante dell'economia digitale globale e passaggio inevitabile per cogliere appieno i vantaggi della digitalizzazione. Pertanto si rende necessaria una *governance* adeguata, unitamente a efficaci garanzie sull'accesso da parte dei governi ai dati personali detenuti dal settore privato, in

Intelligenza artificiale

Open finance

Privacy e concorrenza

Accesso affidabile dei governi ai dati dei privati

21

modo da creare fiducia e ridurre al minimo gli ostacoli ai flussi dei dati stessi. Nelle plenarie del 2023 il DGP ha preso atto che la dichiarazione rappresenta un buon passo avanti e che la comunità internazionale per la protezione dei dati ha cominciato a impegnarsi e fornire *feedback* sull'attuazione della stessa; tuttavia, si è anche rilevato che la dichiarazione non definisce ulteriori passi concreti per la sua attuazione. Alcune delegazioni hanno suggerito la realizzazione di un compendio di tutte le leggi pertinenti nei Paesi membri dell'OCSE, che potrebbe costituire un utile strumento di riferimento da affiancare alla dichiarazione.

21.4. *Le Conferenze internazionali ed europee***Global Privacy
Assembly**

La 45^a conferenza annuale della *Global Privacy Assembly* (GPA) che riunisce le autorità di protezione dati a livello globale si è tenuta ad Hamilton (Bermuda), dal 16-20 ottobre.

Come di consueto, la Conferenza si è articolata in una sessione aperta, con il coinvolgimento di diversi attori pubblici e privati, e in una sessione riservata alle sole autorità di protezione dei dati.

Il Garante ha preso parte ai *panel* della sessione aperta dedicati all'IA e alle tecnologie emergenti con un intervento sul tema della protezione dei dati personali nel settore finanziario. Nella sessione riservata alle autorità di protezione dati sono state adottate numerose risoluzioni su tematiche di grande interesse (si ricordano quelle sull'IA nel contesto lavorativo, della quale il Garante è stato autorità proponente; sull'utilizzo dei dati relativi alla salute nella ricerca scientifica; sul raggiungimento di standard globali di protezione dati; sull'istituzione di un gruppo di lavoro sulla prospettiva di genere nella protezione dei dati). Inoltre, tale sessione, occasione unica di confronto tra le autorità a livello mondiale, nel 2023 è stata caratterizzata da alcuni "*Capacity Building Workshop*" dedicati alle tecnologie quantistiche, al metaverso, alle tecnologie per la tutela ambientale e protezione dei dati e alla digitalizzazione nel settore pubblico.

Merita segnalare che l'Autorità filippina ha assunto il ruolo di primo segretario permanente della GPA, per la prima volta finanziato dalle autorità secondo i criteri definiti dalla risoluzione sul futuro della Conferenza adottata dalla GPA nel 2021.

Nel corso della Conferenza sono state annunciate le date della prossima GPA che si terrà a Jersey dal 28 ottobre al 1° novembre 2024.

**Conferenza di primavera
(Spring Conference)**

La Conferenza di primavera delle autorità di protezione dati europee, tradizionale momento di scambio e *best practice*, si è tenuta a Budapest dal 10 al 12 maggio. Nel corso dell'evento, si è discusso dell'impatto sociale e individuale delle nuove tecnologie e si è fatto il punto sulla giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia UE in materia di protezione dei dati e *privacy*. Un'apposita sezione ha esaminato le problematiche legate al ruolo svolto dai RPD, anche alla luce delle buone prassi sviluppate da soggetti pubblici e privati e dalle autorità di supervisione.

È stata inoltre adottata una risoluzione conclusiva sulla necessità di rafforzare la cooperazione nell'ambito della protezione dei dati e del diritto alla concorrenza, nella quale si è rinnovato l'impegno unitario dei Garanti nella tutela dei diritti fondamentali e incoraggiato lo scambio di informazioni fra autorità *privacy* e della concorrenza, nell'ottica di promuovere la parità sui mercati nel rispetto della normativa sulla protezione dei dati.

Infine, in occasione della *Spring Conference*, l'11 maggio il Garante ha organizzato nella sede dell'Istituto italiano di cultura di Budapest una *workshop* dal titolo "Persone vulnerabili: strumenti di tutela *online*. I minori e la verifica dell'età" (cfr. par. 23.3).

Il 20 ed il 21 giugno si è tenuto a Tokyo il G7 delle autorità di protezione dati (*Roundtable of G7 Data Protection Authorities*).

Sono stati presentati i *report* dei tre gruppi di lavoro istituiti nel 2022 durante il G7 delle DPA tenutosi a Bonn, i quali hanno iniziato a confrontarsi su tre temi individuati come prioritari, ossia:

- libera circolazione dei dati basata sulla fiducia (*Free Data Flow with Trust*);
- tecnologie emergenti e tecnologie di potenziamento della *privacy* (PET);
- cooperazione internazionale nell'applicazione del quadro normativo.

Il G7 ha confermato di voler sviluppare il lavoro su tali tematiche anche per il prossimo anno.

Le delegazioni hanno quindi esaminato e approvato il Piano di azione 2023-2024 e il comunicato stampa finale, nonché una dichiarazione dedicata all'IA generativa e fortemente voluta dall'Autorità giapponese in cui sono state ricordate le iniziative in corso da parte delle diverse autorità di protezione dati, con particolare riguardo all'attività svolta dal Garante italiano nei confronti di ChatGPT, invitando le aziende sviluppatrici a prestare la dovuta attenzione ai requisiti giuridici e agli orientamenti forniti dalle autorità di protezione dei dati sull'IA, a garanzia della *privacy* e degli altri diritti umani fondamentali.

La delegazione italiana ha presentato e commentato un breve video relativo al prossimo G7 delle autorità di protezione dati, che sarà organizzato e ospitato a Roma il 9-11 ottobre 2024.

G7 delle autorità di protezione dati

21.5. Le domande pregiudiziali davanti alla Corte di giustizia dell'Unione europea

L'attività internazionale del Garante ha riguardato anche le cause pregiudiziali proposte dinanzi alla CGUE dai giudici degli Stati membri, ai sensi dell'art. 267 del TFUE, in materia di protezione dei dati personali. Al riguardo, deve segnalarsi un considerevole incremento del numero di tali cause nel corso del 2023, principalmente in rapporto all'interpretazione di disposizioni del RGPD, anche se non sono mancate questioni connesse alla direttiva 2016/680 e all'annoso tema della conservazione prolungata dei dati di traffico e dell'accesso a comunicazioni elettroniche nell'ottica della direttiva 2002/58/CE. Nel prosieguo si segnalano, in particolare, le seguenti sentenze adottate dalla CGUE nel corso del 2023, rappresentando che su ulteriori questioni pregiudiziali sono pervenute le conclusioni degli Avvocati generali presentate nel medesimo anno, delle quali non è possibile dare conto in questa sede:

- sentenza 12 gennaio 2023, causa C-132/21, in materia di mezzi di ricorso ai sensi del RGPD;
- sentenza 12 gennaio 2023, causa C-154/21, in materia di diritto di accesso ex art. 15 RGPD;
- sentenza 26 gennaio 2023, causa C-205/21, concernente i limiti al trattamento di dati biometrici e genetici ai sensi della direttiva (UE) 2016/680;
- sentenza 9 febbraio 2023, causa C-453/21, in materia di RPD e presupposti per la lecita rimozione ai sensi della legislazione nazionale;
- sentenza 9 febbraio 2023, causa C-560/21, in materia di RPD e di sospensione dall'incarico per motivi non inerenti ai compiti;
- sentenza 16 febbraio 2023, causa C-349/21, in materia di accesso ai dati delle comunicazioni elettroniche in procedimenti giudiziari ai sensi della direttiva 2002/58/CE;
- sentenza 2 marzo 2023, causa C-268/21, concernente l'esibizione di documentazione contenente dati personali in procedimenti civili e i relativi limiti;
- sentenza 30 marzo 2023, causa C-34/21, sulla necessità del consenso per la didattica in videoconferenza durante la pandemia di Covid-19;

Rinvii pregiudiziali ex art. 267 TFUE

21

- sentenza 4 maggio 2023, causa C-487/21, sul concetto di “copia” dei dati personali nelle richieste di accesso *ex art.* 15 RGPD;
- sentenza 4 maggio 2023, causa C-60/22, sulla nozione di contitolarità del trattamento e l’esercizio dei diritti degli interessati ai sensi del RGPD;
- sentenza 4 maggio 2023, causa C-300/21, in merito alle condizioni per il diritto al risarcimento del danno da trattamento di dati personali e alla nozione di danno immateriale;
- sentenza 22 giugno 2023, causa C-579/21, sulla portata (anche nel tempo) del diritto di accesso *ex art.* 15 RGPD e sulla nozione di “destinatari” dei dati;
- sentenza 4 luglio 2023, causa C-252/21, sulla leale cooperazione fra autorità garanti della concorrenza e autorità di controllo della protezione dei dati nel constatare non conformità rispetto al RGPD;
- sentenza 7 settembre 2023, causa C-162/22, sulla conservazione prolungata dei dati delle comunicazioni elettroniche e sulla loro messa a disposizione successiva in altri procedimenti;
- sentenza 5 ottobre 2023, causa C-659/22, sulla nozione di “trattamento” di dati personali in rapporto alla verifica della validità di “certificati Covid digitali dell’UE”;
- sentenza 26 ottobre 2023, causa C-307/22, sul diritto di accesso *ex art.* 15 RGPD e sulla motivazione della relativa richiesta;
- sentenza 9 novembre 2023, causa C-319/22, sulla nozione di “dato personale” nel contesto dei servizi relativi alle informazioni sulla riparazione e la manutenzione dei veicoli a motore;
- sentenza 16 novembre 2023, causa C-333/22, sull’esercizio dei diritti dell’interessato tramite l’autorità di controllo ai sensi della direttiva (UE) 2016/680;
- sentenza 5 dicembre 2023, causa C-807/21, sulla nozione di “titolare del trattamento” e i poteri correttivi delle autorità di controllo nei confronti di persone giuridiche;
- sentenza 5 dicembre 2023, causa C-683/21, concernente la nozione di “contitolarità” del trattamento e il perimetro di responsabilità ai fini dell’irrogazione di sanzioni amministrative pecuniarie;
- sentenza 7 dicembre 2023, cause riunite C-26/22 e C-64/22, sulla portata del controllo giurisdizionale rispetto alla decisione di un’autorità di controllo concernente un reclamo in caso di trattamento illecito di dati;
- sentenza 7 dicembre 2023, causa C-634/21, concernente la nozione di processo decisionale automatizzato e le attività di società che forniscono informazioni commerciali;
- sentenza 14 dicembre 2023, causa C-340/21, in materia di responsabilità del titolare del trattamento e di diritto al risarcimento di un danno immateriale in caso di violazione commessa da terzi;
- sentenza 14 dicembre 2023, causa C-456/22, sulla nozione di “danno immateriale” e sul diritto al risarcimento in caso di pubblicazione *online* senza consenso dell’interessato;
- sentenza 21 dicembre 2023, causa C-667/21, in materia di risarcimento di un danno immateriale, della sua funzione compensativa e dell’incidenza della colpa del titolare del trattamento.

21.6. I progetti per l’applicazione del RGPD finanziati dall’Unione europea

Progetto ARC II

Nella Relazione 2022 (v. p. 197) si è dato conto dell’avvio, nel mese di settembre 2022, di un progetto co-finanziato al 90% dalla Commissione europea, denominato ARC II (<https://arc-rec-project.eu/riguardo-al-progetto-arc-ii/>), in partenariato con l’Autorità garante per la protezione dei dati personali della Croazia (capofila del

progetto), l'Università degli studi di Firenze (Dipartimento di scienze giuridiche) l'Università di Zagabria (Facoltà di informatica) e l'Università di Bruxelles (Vrije).

In questo contesto, nel corso del 2023 è stato sviluppato uno strumento digitale *open source* denominato OLIVIA, liberamente accessibile, interoperabile e innovativo, adattato alle esigenze specifiche delle PMI, per conformare la loro attività al RGPD. In Italia sono stati condotti, da personale del Garante, cinque dei dieci seminari da remoto sul RGPD previsti dal progetto, durante i quali le PMI hanno potuto ricevere supporto diretto per affrontare problemi specifici relativi alla conformità al RGPD. È stata inoltre condotta una campagna di sensibilizzazione sui canali *social* del Garante ed è stato organizzato un *workshop* di verifica dello strumento digitale OLIVIA.

21

22 Attività di normazione tecnica internazionale e nazionale

Il Garante ha proseguito la collaborazione in tema di elaborazione di norme tecniche internazionali nell'ambito del *Working Group 5* del sottocomitato SC27, che si occupa della sicurezza delle informazioni all'interno del comitato tecnico JTC1 dell'Organizzazione internazionale per la normazione (ISO). Il gruppo di lavoro segue gli aspetti di sicurezza nella gestione delle identità relativamente alle tecnologie biometriche e alla protezione dei dati personali. Armonizzando la propria posizione con quelle delle altre autorità di protezione dati tramite il CEPD, che ha un collegamento in proposito con ISO, l'Autorità ha seguito lo sviluppo delle seguenti norme tecniche:

- ISO 27701:2019 - *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*, revisione a seguito della pubblicazione della ISO 27002:2022;

- ISO 27566 - *Information security, cybersecurity and privacy protection - Age assurance systems - Framework*, che si propone di stabilire principi chiave, che includono anche la *privacy*, per abilitare decisioni di fornitura di beni, servizi o contenuti che dipendano dall'età del soggetto richiedente mediante la definizione di un *framework* di indicatori di confidenza di età o di *range* di età delle persone fisiche nonché, con la Parte 2, definire le misure e il *testing* delle componenti per la *age verification* in prospettiva di utilizzo per il *conformity assessment* e con la Parte 3 indicare elementi per *Interoperability, technical architecture and guidance on use*;

- ISO TS 27006 - *Requirements for bodies providing audit and certification of privacy information management systems according to ISO/IEC 27701 in combination with ISO/IEC 27001*, che definisce requisiti aggiuntivi alla ISO 17021 e 27006 per gli organismi di certificazione che svolgono *audit* e rilasciano certificazioni secondo la nuova ISO 27701 (*Privacy Information Management System*);

- PWI PII - *Processing Record Structure*, nuovo progetto che intende riutilizzare le strutture dati descritte dalla ISO/IEC 27560 - *Consent Receipt and Record Standard* a tutte le possibili basi giuridiche per il trattamento di dati personali;

- ISO TS 27561 - *Privacy operationalisation model and method for engineering (POMME)*, che, sulla base del modello OASIS-PMRM (*Privacy Management Reference Model*), fornisce elementi e supporta le organizzazioni al fine di definire un modello e metodi standardizzati per la *privacy engineering* di sistemi complessi;

- ISO 29151:2017 - *Code of practice for personally identifiable information protection* – revisione sistematica che terrà conto dell'applicabilità dei controlli individuati nelle organizzazioni (in particolare PMI) che non implementano sistemi di gestione;

- ISO 27018:2019 - *Code of practice for protection of PII in public clouds acting as PII processors* revisione della norma tecnica – che individua controlli specifici per i provider di servizi cloud che, trattando dati personali, agiscono in qualità di responsabile del trattamento – per allineamento alla nuova versione della ISO 27002:2022;

- ISO 27562 - *Privacy guidelines for fintech services* che propone una linea guida per la *privacy* per i *fintech services* identificando i modelli di *business*, i ruoli delle relazioni C2B, B2B, i rischi e i requisiti *privacy* e fornendo specifici controlli *privacy* per tali servizi tenendo conto del contesto (legale) e dei ruoli;

- ISO 27091 - *Cybersecurity and privacy - Artificial intelligence – Privacy protection*

che fornisce una guida alle organizzazioni che utilizzano o sviluppano sistemi di intelligenza artificiale e modelli di *machine learning* per indirizzare i rischi *privacy* identificando i rischi nel ciclo di vita dei sistemi IA e stabilendo meccanismi per valutare le conseguenze e trattare tali rischi mediante misure di mitigazione.

L'Autorità inoltre, nell'ambito del *Working Group 5* del comitato tecnico JTC13 del CEN CENELEC che si occupa dello sviluppo di norme tecniche riguardanti *Data Protection, Privacy and Identity Management*, ha contribuito allo sviluppo delle seguenti norme tecniche:

- EN 17529 - *Privacy Protection by design and by default*, che, in risposta al mandato della Commissione europea (Direzione generale sicurezza e affari interni), individua obiettivi, requisiti di protezione dati e linee guida per supportare sviluppatori, produttori e fornitori di servizi e prodotti nell'implementazione dei principi in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita nello sviluppo, produzione di prodotti e servizi;

- EN 17799 - *Personal data protection requirements for processing activities*, che, sulla base della prassi di riferimento UNI 43.2:2018 *Guideline for personal data management within ICT according to Regulation EU 679/2016 (GDPR) - Requirements for the protection and conformity assessment of personal data within ICT*, propone requisiti per la protezione dei dati personali gestiti da sistemi informativi utilizzabili anche per certificazioni ai sensi dell'art. 42 del RGPD;

- EN 17740 - *Requirements for professional profiles related to personal data processing and protection*, che, sulla base della norma tecnica UNI 11697:2018, individua requisiti armonizzati a livello europeo e in accordo con il *European Qualifications Framework (EQF)*, certificabili, circa le competenze, conoscenze e abilità dei professionisti che svolgono attività nell'ambito del trattamento e della protezione dati personali;

- EN 17926 - *Privacy Information Management System per ISO/IEC 27701 - Refinements in European context*, che adatta il *framework* internazionale offerto dalla ISO 27701 nel contesto europeo;

- JT013068 - *Certification scheme as per ISO/IEC 17065 for certification against*
- EN 17926 - *Privacy Information Management System per ISO/IEC 27701 - Refinements in European context* che intende definire uno schema di certificazione ai sensi dell'art. 42 RGPD basato sulla norma tecnica EN 17926;

JT013072 - *Scheme for certification of personal data processing operations against* EN17799 che intende definire uno schema di certificazione ai sensi dell'art. 42 del RGPD basato sulla norma tecnica EN 17799.

Del pari è proseguita la collaborazione con le diverse commissioni tecniche UNINFO, l'Ente di normazione federato con UNI (Ente nazionale italiano di unificazione).

In ambito ENISA si segnalano la pubblicazione, in occasione dello *EU Data Protection Day* a fine gennaio 2023, del report in materia di *Data Protection Engineering, Scope and Application* e il completamento del report in materia di *data protection engineering* all'interno degli *EU Data Spaces* (in particolare in ambito sanitario), che sarà pubblicato in occasione dello *EU Data Protection Day* a fine gennaio 2024.

Con riferimento al cosiddetto Gruppo di Berlino (*International Working Group on Data Protection in Technology* - cfr. cap. 23.1), il Garante ha collaborato alla stesura come *lead rapporteur* del parere in materia di *data sharing*, ha partecipato alla definizione dei documenti di lavoro sui temi della telemetria (testo adottato nel corso della riunione che si è svolta a Roma il 6-7 giugno 2023), e ha collaborato al documento di lavoro in materia di moneta digitale (approvato dal Gruppo a novembre 2023) nonché alle fasi iniziali di redazione delle linee guida in materia di *large scale language models* e di quelle relative all'impiego di neurotecnologie.

22

Particolarmente significativa, infine, è stata la collaborazione con l'Agenzia nazionale per la cybersicurezza al fine di predisporre delle linee guida in materia di funzioni crittografiche per la conservazione delle *password* (provv. 7 dicembre 2023, n. 594, doc. web n. 9962384), al fine di fornire indicazioni a titolari e responsabili del trattamento, e ai produttori di prodotti, servizi e applicazioni, sulle misure tecniche in grado di garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento delle *password* di utenti.

23 L'attività di comunicazione, informazione e di rapporto con il pubblico

23.1. La comunicazione del Garante: profili generali

Nel 2023 l'Autorità ha dato ulteriore impulso all'attività di promozione del diritto alla protezione dei dati presso cittadini, istituzioni, imprese e associazioni, anche attraverso innovative strategie di comunicazione.

Tale attività di comunicazione ha riguardato innanzitutto i fenomeni più invasivi della riservatezza delle persone, quali il *telemarketing* e, in relazione alle tecnologie emergenti, i sistemi di raccolta di dati biometrici e l'uso del riconoscimento facciale. Grande impegno è stato rivolto anche all'IA, in particolare a quella cd. generativa, che si è concretizzata in un intervento – il primo a livello mondiale – nei confronti di una piattaforma come ChatGPT.

Sempre sul fronte dell'IA, ampio ed accurato spazio è stato dedicato all'indagine conoscitiva avviata dal Garante sui siti internet pubblici e privati per verificare l'adozione di idonee misure di sicurezza volte ad impedire la raccolta massiva (*web scraping*) di dati personali a fini di addestramento degli algoritmi di IA da parte di soggetti terzi.

Costante attenzione (cfr. 12.7) è stata posta alle iniziative a tutela dei minori ed in particolare alla richiesta rivolta alle piattaforme più frequentate di individuazione e adozione di soluzioni affidabili di *age verification*, allo stop a Replika (il *chatbot*, dotato di una interfaccia scritta e vocale che basandosi sull'intelligenza artificiale genera un amico virtuale) nonché all'attività di sensibilizzazione per un utilizzo responsabile della rete e dei nuovi *social media*. Specifica attività di informazione è stata inoltre svolta nei confronti dei *media* a tutela delle vittime di violenza.

Nel mese di gennaio è stata avviata una campagna di comunicazione istituzionale intitolata "Finalmente un po' di *privacy*", finanziata dal Ministero delle imprese e del *made in Italy* con il fondo a vantaggio dei consumatori e funzionale all'acquisizione della consapevolezza del valore dei dati e dell'importanza della loro protezione, che si è sviluppata attraverso 9 spot radio tv, prodotti *social* e affissioni digitali.

Gli spot radio tv hanno affrontato diversi temi: dall'uso delle *app* alle frodi digitali, dal cyberbullismo al *revenge porn*, dal *telemarketing* selvaggio agli assistenti digitali, dai dati sanitari alla profilazione e all'uso delle *password*. Il *claim* finale "Se proteggi i tuoi dati proteggi te stesso" è un invito ad essere sempre più consapevoli del "valore *privacy*".

Nel mese di gennaio il Garante ha, inoltre, bandito un concorso rivolto agli studenti delle classi I e II delle scuole superiori di secondo grado, chiamandoli a realizzare un video per spiegare ai coetanei cosa è per loro la *privacy* e come tutelarla, allo scopo di coinvolgere insegnanti e ragazzi in progetti di informazione e sensibilizzazione su tematiche connesse alla protezione dati soprattutto nella dimensione digitale. Tale iniziativa è stata intitolata "Diventa ambasciatore della *privacy*" e ad essa hanno aderito numerosi istituti scolastici di diverse regioni italiane. Per la realizzazione dei video l'Autorità ha messo a disposizione delle scuole un apposito kit didattico per sviluppare percorsi di formazione su temi di grande impatto, soprattutto per i più giovani: il cyberbullismo, i furti di identità, il *revenge porn*, la profilazione *online*, gli assistenti digitali, i dispositivi indossabili e i *deepfake*.

Le attività di
comunicazione
strategica

23

I premi in denaro da destinare ad acquisti di prodotti tecnologici per la didattica sono stati assegnati al Liceo scientifico Corradino D’Ascanio di Montesilvano, in provincia di Pescara (primo classificato), all’Istituto tecnico commerciale e per geometri Pareto di Pozzuoli, in provincia di Napoli (secondo classificato) e all’Istituto superiore di istruzione secondaria F. De Sanctis - O. D’Agostino di Domicella, in provincia di Avellino (terzo classificato) per i video rispettivamente realizzati. Il conferimento dei premi è avvenuto nel corso dell’evento “*Privacy Talks*” tenutosi il 25 ottobre a Napoli (v. *infra*).

Il 10 marzo l’Autorità ha preso parte alla Fiera “Didacta”, l’evento più importante dedicato al settore della scuola che si svolge ogni anno a Firenze, e ha organizzato due seminari dedicati ai docenti e ai dirigenti scolastici sul tema “La scuola a prova di *privacy*”. Nell’occasione è stata presentata l’edizione aggiornata del *vademecum* dedicato alla scuola.

È stata inoltre curata la partecipazione dell’Autorità all’edizione 2023 del Forum PA “Ripartiamo dalle persone”, manifestazione dedicata alla formazione e alla condivisione di *best practice* della p.a. e delle imprese innovative, che si è svolta presso il Palazzo dei Congressi di Roma dal 16 al 18 maggio. All’evento hanno partecipato i componenti del Collegio, dirigenti e funzionari del Garante con interventi su temi riguardanti in particolare la digitalizzazione della pubblica amministrazione. Presso lo stand del Garante sono stati organizzati alcuni seminari ed è stato distribuito materiale documentale, anche su supporto digitale quale la “Guida all’applicazione del Regolamento europeo in materia di protezione dei dati personali”, il testo aggiornato del Codice *privacy* e il secondo volume di “Applicare il GDPR. Le linee guida europee 2019-2022”.

Particolare attenzione è stata dedicata alla seconda edizione di “*State of Privacy*”, l’evento-dialogo del Garante che vede la partecipazione dei rappresentanti dei principali *stakeholder* pubblici e privati con l’obiettivo di sviluppare un confronto aperto e costruttivo sul futuro della protezione dei dati e sui problemi posti dallo sviluppo delle più recenti tecnologie. L’incontro, svoltosi il 18 settembre presso il Museo nazionale etrusco di Villa Giulia a Roma, organizzato in collaborazione con le Università di Roma Tre e di Firenze, ha riunito più di 250 rappresentanti di istituzioni nazionali e internazionali, pubbliche amministrazioni, *big tech*, *media*, grandi aziende, mondo finanziario, oltre naturalmente a esperti, studiosi e personalità del mondo universitario e scientifico. Al centro i lavori di 19 tavoli tematici dedicati ad una serie di rilevanti settori: *advertising*, *cloud*, *cybersecurity*, diritti umani, DPO, *enforcement*, genetica, IA, IoT e *smart cities*, *legal design*, *media* e comunicazione, minori, neuroscienze, pubblica amministrazione digitale, procedimento legislativo, salute, servizi finanziari, sostenibilità, *telemarketing*.

Nel corso dell’evento, condotto da Riccardo Luna, direttore di Italian Tech, sono intervenuti il Sottosegretario alla Presidenza del Consiglio dei ministri con delega all’innovazione tecnologica, Alessio Butti, e i Rettori delle due Università di Roma Tre e di Firenze, Massimiliano Fiorucci e Alessandra Petrucci.

In questa occasione è stato lanciato il *Privacy Tour*, finalizzato a diffondere la cultura della protezione dei dati personali nel sud e nei piccoli centri del nostro Paese dove risulta ancora scarsa la piena consapevolezza del loro valore, allo scopo di scongiurare il rischio di nuovi *divide* culturali tra chi conosce opportunità e rischi della società digitale e sa come difendersi, e chi queste conoscenze non le possiede. Quanti hanno aderito e aderiranno al progetto si impegnano a organizzare nel corso del 2024, secondo un *format* disegnato dall’Autorità, eventi, iniziative, percorsi di formazione, anche a distanza, che affrontino i temi della *privacy* e siano rivolti alle persone più esposte ai pericoli della rete, in particolare i bambini e i nativi non digitali. Tra i primi aderenti al *Privacy Tour* ricordiamo la Polizia postale, l’Università Roma

Tre, le Ferrovie dello Stato italiane, la Fondazione Magna Grecia, la Fondazione Telefono Azzurro, Iliad Italia, Digital Angels, @LawLab (Luiss), la Società Editrice Sud - Gazzetta del Sud - Giornale di Sicilia, Google Italia, Huawei Italia, Meta, Microsoft, Mondadori, Kaspersky, Sky Italia, TikTok, Yoox, Rai radiotelevisione italiana.

L'impegno organizzativo ha riguardato altresì la seconda edizione dei *Privacy Talks* tenutasi il 25 ottobre, presso l'Auditorium dell'Università degli Studi Federico II a San Giovanni a Teduccio di Napoli. Si tratta di un'iniziativa divulgativa dell'Autorità con finalità promozionali della cultura della *privacy* tra le nuove generazioni. I protagonisti del *format* sono stati adolescenti tra i 13 e i 17 anni chiamati a riflettere sulle opportunità e sui pericoli nascosti nei dispositivi tecnologici di uso quotidiano. In tale occasione l'Autorità ha utilizzato tecniche di divulgazione il più possibile empatiche e coinvolgenti per spiegare l'importanza di proteggere i dati personali e la sfera più intima, propria e altrui.

Durante l'evento sono stati premiati i video vincitori di "Diventa ambasciatore della *privacy*", il concorso organizzato dall'Autorità e rivolto agli studenti delle classi I e II delle scuole superiori di secondo grado per raccontare la propria idea di *privacy* e come difenderla (v. supra).

Il 6 e 7 giugno l'Autorità ha ospitato a Roma il 71° incontro dell'*International Working Group on Data Protection in Technology* (IWGDPT), noto come Gruppo di Berlino. All'evento - organizzato e preparato congiuntamente al Commissario federale per la protezione dei dati e la libertà di informazione (BfDI) in qualità di Presidente del Gruppo di Berlino - hanno preso parte il Presidente Pasquale Stanzone e la Vice Presidente Ginevra Cerrina Feroni e oltre 40 membri del Gruppo provenienti da diverse aree del mondo (Europa, America settentrionale, America latina, Asia) in rappresentanza di autorità per la protezione dei dati nazionali, della società civile e di organismi internazionali.

L'incontro ha consentito un proficuo scambio di opinioni, fra l'altro, sui temi dell'IA, e ha visto l'adozione di un documento dedicato a "Dati telemetrici e diagnostici", già elaborato sotto la guida del BFDI. Il Gruppo ha, inoltre, stabilito di proseguire i lavori finalizzati alla redazione di un documento sulle "Valute digitali introdotte da banche centrali" nonché sul tema del *data sharing* e ha programmato di focalizzare l'attenzione sull'intelligenza artificiale generativa e sulle neurotecnologie.

Alla figura del RPD è stato dedicato l'evento organizzato dall'Autorità, in collaborazione con la Regione Emilia-Romagna e la società Lepida, che si è svolto a Bologna il 23 giugno dal titolo "RPD al centro". A cinque anni dall'applicazione del RGDPR l'Autorità ha incontrato gli RPD del settore pubblico e privato per fare un bilancio dell'esperienza fin qui maturata e per individuare le aree di intervento finalizzate a rafforzare il ruolo del RPD nel prossimo futuro. I lavori sono stati aperti con i saluti del Presidente della Regione Emilia-Romagna, Stefano Bonaccini, del Presidente del Garante, Pasquale Stanzone, e di Gianluca Mazzini, Direttore generale di Lepida e sono proseguiti con gli interventi di dirigenti e funzionari dell'Autorità e di alcuni RPD.

23.2. I prodotti informativi

Nel corso del 2023 sono stati diffusi 62 comunicati stampa e 17 numeri della *Newsletter*.

La *Newsletter* del Garante è una pubblicazione periodica, registrata al Tribunale di Roma, giunta al XXV anno di diffusione (per un totale di 515 numeri e 1.759 notizie). È inviata in via telematica a redazioni, professionisti, amministrazioni pubbliche, imprese e cittadini che ne fanno esplicita richiesta o si iscrivono *online* sul sito dell'Autorità.

23

Gli eventi

23

La *Newsletter* è da anni uno strumento conosciuto ed apprezzato attraverso il quale l’Autorità fornisce un’ampia rassegna dei più importanti provvedimenti adottati, della sua attività in ambito nazionale, europeo ed internazionale e delle molteplici iniziative legate alla protezione dei dati personali e alla tutela dei diritti fondamentali.

Sul sito è possibile consultare l’archivio tematico della pubblicazione che raccoglie, divisi per categorie, i 25 anni di articoli prodotti dalla redazione, nonché l’intero archivio dei comunicati stampa.

Anche quest’anno il Garante ha pubblicato 12 numeri del GPDPDigest, il *magazine online* che raccoglie mensilmente i principali interventi e le campagne di comunicazione dell’Autorità, nonché una sintesi delle principali attività del CEPD, del GEPD e una rassegna di comunicati della Corte di giustizia dell’UE in tema di protezione dei dati e di educazione digitale.

23.3. Il sito istituzionale, i prodotti multimediali e le pubblicazioni

Nel 2023 sono state incrementate la quantità e la varietà dei prodotti di comunicazione digitale destinati alla diffusione tramite il sito web e i canali *social media* e di messaggistica del Garante. Particolare attenzione è stata rivolta all’aspetto creativo e qualitativo, con la ricerca e lo sviluppo di nuovi *format* e stili allineati alle più recenti e avanzate tendenze della comunicazione digitale. Quasi tutti i *format* e i contenuti sono stati ideati e sviluppati *in house* ed hanno riguardato (tra l’altro) l’educazione digitale, l’informazione sui rischi e sulle buone pratiche nel campo della cybersicurezza, l’IA, la conoscenza dei diritti e dei principali adempimenti connessi alla normativa in materia di protezione dei dati personali.

Nel 2023 la produzione di video è sensibilmente aumentata, sia per tener conto dei nuovi *trend* del consumo digitale, sia per valorizzare le potenzialità dei canali *social*, in particolare di Instagram e di YouTube. Quest’ultimo, dopo un periodo di inattività legato a necessarie valutazioni di ordine giuridico-normativo, è stato rivitalizzato, ammodernato e popolato di nuovi contenuti. Nell’anno sono stati realizzati 45 video, tutti *in house* (con una sola eccezione), tra cui interviste, *teaser*, *tutorial*, video informativi e promozionali, montaggi e rielaborazione di eventi.

Il Garante è stato anche impegnato nello sviluppo di campagne informative integrate e multicanale che hanno portato alla creazione di nuove sezioni tematiche del sito web, di *vademecum* e di contenuti *social*, tra cui in particolare, la scheda sui modelli di progettazione ingannevoli (*Dark Pattern*), quella su “*Dating online*” e su “*App* e dispositivi *fitness tracker*”.

Sono state pubblicate, inoltre, le edizioni aggiornate dei *vademecum* “La scuola a prova di *privacy*” e la “Guida all’applicazione del Regolamento europeo in materia di protezione dei dati personali”.

È cresciuta in modo significativo la pubblicazione di contenuti sul sito web del Garante (2.440 contenuti, +26% rispetto al 2022) e sui profili *social media* dell’Autorità su LinkedIn, YouTube, Telegram, Instagram e Twitter (2.822 contenuti, pari al +12% rispetto al 2022). Importante anche la crescita del numero di *follower* totali dei profili *social media* e di messaggistica, che ha raggiunto il numero complessivo di 92.177 (+13,6% rispetto al 2022). Sul sito web dell’Autorità sono state create *ex novo* o significativamente aggiornate 47 pagine tematiche.

Sul fronte editoriale, si segnala in particolare la realizzazione di alcune pubblicazioni: “La protezione dati. Da 25 anni la bussola del futuro” (atti del Convegno svolto nel luglio 2022 in occasione delle celebrazioni per i 25 anni del Garante per la protezione dei dati personali); “Il Metaverso tra utopie e distopie” (atti del convegno per la Giornata europea dei dati personali 2023); “Applicare il GDPR. Le linee guida

europee - Volume 2”; “Persone vulnerabili: strumenti di tutela *online*. I minori e la verifica dell’età” (atti dell’omonimo evento organizzato dal Garante e collegato alla *Spring Conference 2023*).

I *media*, nazionali ed esteri, hanno mostrato una costante attenzione agli interventi messi in atto e alle questioni sollevate dal Garante. In particolare, il caso ChatGPT ha avuto vastissima eco internazionale. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali ed esteri, dei principali quotidiani locali, delle testate *online* e *blog* che hanno trattato i temi legati alla *privacy* sono state 7.312, quelle relative all’attività del Garante 5.706. Gli articoli aventi per oggetto le interviste, interventi e dichiarazioni del Garante sono stati 155 su stampa e web, mentre 56 su radio e televisione. Si contano, infine, 1.931 articoli relativi ai comunicati stampa e 616 relativi a temi affrontati nelle *Newsletter*.

23

23.4. Le manifestazioni e i convegni

A partire dal 2007, promossa dal Consiglio d’Europa con il sostegno della Commissione europea e di tutte le autorità europee per la *privacy* e la protezione dei dati, il 28 gennaio di ogni anno viene celebrata in tutta Europa la “Giornata europea per la protezione dei dati personali”, che ha lo scopo di sensibilizzare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali.

Il Garante ha dedicato la Giornata europea 2023 al Metaverso. Il Convegno, intitolato “Il Metaverso tra utopie e distopie: orizzonti e sfide della protezione dei dati”, si è svolto in presenza ed in diretta *streaming* presso lo spazio Esperienza Europa del Parlamento europeo in Italia - “David Sassoli”. Attraverso gli interventi dei componenti del Collegio e di esperti di chiara fama, nazionali e internazionali, sono state approfondite le problematiche legate all’impatto che il nuovo *habitat* digitale avrà sulle relazioni sociali e sui comportamenti dei singoli, sulle loro libertà e diritti, così come sui processi decisionali della collettività.

Il 22 febbraio, presso la stessa sede, è stato presentato il libro “La *privacy* dell’era digitale - Le Relazioni dei presidenti dell’Autorità Garante 1997-2022”, curato dal Presidente del Garante Pasquale Stanzione. Il libro, attraverso i discorsi dei suoi presidenti, ha ripercorso i venticinque anni di storia del Garante.

Diritto alla protezione dei dati personali, valorizzazione e monetizzazione dei dati, intelligenza artificiale e minori sono stati i temi trattati dal Collegio nel corso della sessione italiana del “*Privacy Symposium*”, la conferenza internazionale organizzata a Venezia ad aprile. Obiettivo della manifestazione, che ha visto coinvolti oltre 200 relatori in più di 80 sessioni, è stato quello di sostenere il dialogo internazionale, la cooperazione e la condivisione delle conoscenze in materia di protezione dati. La progressiva affermazione del diritto alla *privacy* come strumento di redistribuzione del potere informativo è stata oggetto dell’intervento di apertura della giornata tenuto dal Presidente Pasquale Stanzione. L’esigenza di implementare velocemente e in modo collaborativo strumenti per la verifica dell’età dei minori che accedono ai servizi digitali è stata ricordata dai componenti del Collegio, Guido Scorza e Agostino Ghiglia; quest’ultimo ha poi affrontato il rapporto tra intelligenza artificiale e *privacy* ribadendo la necessità di una regolamentazione dell’intelligenza artificiale e, pertanto, di un’accelerazione dell’*iter* di approvazione dell’*AI Act* europeo. Quanto alla monetizzazione dei dati, anch’essa bisognosa di *governance*, la Vice Presidente del Garante, Ginevra Cerrina Feroni, ha evidenziato come il valore economico del dato sia stato riconosciuto anche dalla giurisprudenza nazionale ed europea ma, al contempo, sia necessario guardare alla fragilità di quei soggetti deboli che vivono momenti di vulnerabilità, anche economica.

23

Nel mese di maggio l'Autorità ha organizzato un *workshop* dal titolo “Persone vulnerabili: strumenti di tutela *online*. I minori e la verifica dell'età” nell'ambito della Conferenza di primavera dei Garanti europei, tenutasi a Budapest. L'obiettivo dell'Autorità è stato quello di sensibilizzare i partecipanti a rafforzare la protezione dei minori *online* con nuovi strumenti tecnologici e con più forti norme a tutela della loro personalità.

Il 6 luglio, presso la sala dei gruppi parlamentari, alla presenza dei rappresentanti di Camera e Senato, Ministri, delle istituzioni, del mondo dell'impresa e delle associazioni di categoria si è svolta la cerimonia della presentazione della Relazione annuale per l'anno 2022. La Relazione ha illustrato i diversi e delicati fronti sui quali l'Autorità è stata impegnata nel far rispettare i diritti fondamentali delle persone e i principi alla base della legislazione in materia di *privacy*. L'intero evento è stato trasmesso in diretta televisiva e in *streaming* sul sito web istituzionale.

Si segnala, infine, che nel corso dell'anno il Presidente e i componenti del Collegio hanno partecipato a numerosi eventi, convegni e giornate di studio, di rilievo nazionale ed internazionale.

23.5. *L'attività internazionale*

L'Autorità ha svolto una rilevante attività attraverso il gruppo di comunicatori istituito presso il Comitato europeo per la protezione dei dati al fine di realizzare attività coordinate di comunicazione, con la condivisione, tra l'altro, di comunicati stampa e la gestione comune dei casi con valenza transnazionale.

Il Garante ha contribuito direttamente a numerose attività di comunicazione del Comitato, quali, tra le altre: produzione delle *news enforcement* per la sezione italiana del sito; collaborazione con gruppi di lavoro specifici, in particolare il “Gruppo di esperti di supporto”, e nella realizzazione delle attività relative al “Quadro di attuazione coordinata”; contributo all'avvio del progetto di comunicazione dedicato alle piccole e medie imprese; collaborazione all'aggiornamento delle statistiche sull'attività svolta; collaborazione allo sviluppo su nuove linee guida condivise per le attività di comunicazione sui casi transfrontalieri. Da segnalare anche le attività di comunicazione connesse al Progetto ARC II (cfr. 21.6).

23.6. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

Nel corso del 2023 l'Autorità ha continuato a curare attraverso il Servizio relazioni con il pubblico l'informazione sulle tematiche connesse alla disciplina sulla protezione dei dati personali, anche mediante un servizio di ascolto telefonico e la posta elettronica; quotidianamente vengono prospettati quesiti di varia natura provenienti da soggetti pubblici e privati e da cittadini, spesso di rilevante complessità e delicatezza. Il ricevimento del pubblico in presenza è stato riservato alla trattazione dei casi più articolati e complessi, mentre per il resto il Servizio si è avvalso prevalentemente di strumenti telematici.

Il Servizio relazioni con il pubblico ha continuato a rappresentare un punto essenziale di contatto dei cittadini con l'Autorità e contestualmente ha svolto anche una funzione di filtro, curando, laddove possibile, il diretto riscontro delle richieste pervenute.

Nel periodo in esame è stato notevole l'incremento di richieste di informazioni specifiche riferibili all'interpretazione del RGPD e al coordinamento tra la normativa di settori specifici e la protezione dei dati personali nonché alle modalità di tutela

presso il Garante, ricevute da parte non solo di cittadini interessati, ma anche da avvocati e consulenti, giornalisti, funzionari di enti pubblici, RPD, studenti/ricercatori in particolare in ambito pubblico e privato, sanitario, lavorativo e scolastico.

L'interesse degli utenti rispetto a tali temi è dimostrato dai dati numerici relativi ai contatti con il Servizio, che ammontano in totale a 15.048 di cui 10.815 *e-mail*, 161 fascicoli, circa 4.000 via telefono e 72 visitatori in sede (cfr. parte IV, tab. 15).

Ai fini del potenziamento degli strumenti informativi a disposizione del pubblico, alla luce delle questioni maggiormente segnalate e dell'evoluzione della normativa, sono state predisposte note su varie tematiche per fornire riscontri più approfonditi alle richieste degli utenti (tra le altre ad es. con riguardo al trattamento dei referti medici, alla CIE, al *whistleblowing*, al trattamento dei dati dei minori, all'IA, alla *Disability card*, nonché relativamente a Google Analytics 4 e alle novità del FSE).

Il Servizio ha altresì provveduto ad informare le altre unità organizzative dell'Autorità in merito alle questioni più delicate e di maggiore interesse per gli utenti, anche attraverso report a cadenza quadrimestrale.

Tra le attività ordinarie e di supporto agli utenti va evidenziata l'assistenza alle istanze concernenti i servizi telematici attivi sul sito istituzionale (in particolare il servizio di comunicazione dei dati di contatto dell'RPD, il servizio telematico dedicato al *data breach*, alla segnalazione di comunicazioni indesiderate e alla segnalazione per prevenire il fenomeno *revenge porn*) che hanno comportato un costante coordinamento con le altre unità organizzative interessate.

Per finalità di coordinamento e collaborazione sono state efficacemente prese in carico segnalazioni su eventuali anomalie riscontrate nei moduli messi *online* e richieste sul miglioramento/funzionamento del sito ufficiale. Tali istanze sono state riscontrate in autonomia in alcuni casi connessi alla interpretazione della normativa, e in collaborazione con il Servizio relazioni esterne e *media* nonché il Dipartimento tecnologie digitali e sicurezza informatica in altri inerenti a questioni tecniche.

Infine, si è dato pronto riscontro a molteplici richieste su fascicoli assegnati ad altre unità organizzative (per circa 900 *e-mail*).

Tra le tematiche di carattere generale si segnalano in primo luogo quelle concernenti le forme di tutela (circa 1.195 *e-mail* ricevute) e gli adempimenti previsti dal RGPD (oltre 1.900 *e-mail* hanno riguardato la designazione del RPD e la procedura *online* realizzata dal Garante per la comunicazione dei dati di contatto dello stesso).

Altre questioni ordinarie oggetto di interesse hanno riguardato i trattamenti di dati personali in ambito lavorativo pubblico e privato (oltre 250 *e-mail*); la videosorveglianza in ambito pubblico e privato e sul luogo di lavoro (quasi 600 *e-mail*); i trattamenti di dati personali nell'ambito della rete internet e dell'utilizzo di *Google Analytics*, dell'IA, nonché in ambito giornalistico, con riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca (oltre 650 *e-mail*).

In particolare a partire dal mese di settembre 2023 sono pervenute alcune richieste da parte di RPD circa lo svolgimento del loro ruolo (responsabilità, difficoltà nell'esercizio delle proprie funzioni, richiesta di avere un canale di contatto dedicato con il Garante, ecc.). Il tema è risultato di interesse in quanto il CEPD nella sua azione coordinata per l'attuazione del RGPD (*Coordinated Enforcement Framework* - CEF) ha individuato come focus del 2023 proprio il ruolo degli RPD (cfr. 21.1).

23

Tematiche d'interesse

PAGINA BIANCA



GPDP

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

L'Ufficio del Garante

**RELAZIONE ANNUALE
2023**

PAGINA BIANCA

III - L'Ufficio del Garante

24 Attività di studio e documentazione

L'attività di studio e ricerca ha riguardato molteplici questioni tecnico-giuridiche sulle materie di interesse, anche oggetto di rinvio pregiudiziale alla Corte di giustizia dell'Unione europea.

Particolari approfondimenti sono stati svolti tra l'altro in materia di eredità digitale, controlli a distanza, *whistleblowing* e accesso civico generalizzato.

In continuità con un'attività di studio oramai consolidata, è stato curato un Osservatorio, ad uso interno con cadenza mensile, quale documentazione di sintesi del costante monitoraggio della normativa, giurisprudenza e dottrina nazionale ed eurounitaria in materia di protezione dati, unitamente ad approfondimenti su questioni o settori specifici aventi profili di interesse in relazione alle competenze dell'Autorità.

Anche attraverso il menzionato Osservatorio sono stati svolti approfondimenti tematici, spesso in occasione della pubblicazione di sentenze provenienti da giurisdizioni europee e nazionali.

In attuazione della normativa nazionale ed europea (cfr. artt. 154, comma 1, lett. e), del Codice nonché 59 del RGPD) è stata curata la redazione del testo della Relazione, volta a rendere conto, anzitutto al Parlamento e al Governo, dell'attività svolta dall'Autorità. La struttura della Relazione, che presenta tradizionalmente una parte generale e molteplici sezioni tematiche (ivi comprese quelle contenenti dati di natura statistica), consente la rapida e sintetica consultazione di informazioni puntuali in particolare con riguardo all'attività provvedimentale, sanzionatoria e comunicativa del Garante, nonché all'ambito europeo ed internazionale.

In conformità a quanto previsto dall'art. 22, d.l. n. 90/2014 convertito in legge 11 agosto 2014, n. 114, la Relazione annuale del Garante (non diversamente da quella delle altre autorità amministrative indipendenti) è stata altresì trasmessa alla Corte dei conti.

**Attività di studio,
documentazione e
supporto giuridico**

Relazione annuale

25 La gestione amministrativa e dei sistemi informatici

25.1. *Il bilancio e la gestione economico-finanziaria dell'Autorità*

Il bilancio di previsione per l'esercizio 2023 è stato formulato nel rispetto delle vigenti disposizioni legislative in materia di armonizzazione dei conti delle amministrazioni pubbliche e ha tenuto conto delle misure regolamentari previste dall'ordinamento interno del Garante.

Per quanto attiene alla formulazione delle previsioni, le entrate sono state quantificate in ragione di un generale principio di prudenza mentre le spese sono state valutate assumendo i contratti perfezionati e le richieste di finanziamento rappresentate dalle competenti unità organizzative, avendo cura di assicurare il rispetto di precisi vincoli di bilancio.

Sul piano dei controlli, la complessiva gestione è stata sottoposta alla revisione dell'organo interno preposto alla verifica della regolarità amministrativo-contabile, che non ha rilevato irregolarità, mentre il rendiconto della gestione è stato trasmesso alla Corte dei conti, nel rispetto di puntuali disposizioni legislative, per le verifiche di competenza.

Le fonti di finanziamento sono rappresentate esclusivamente da trasferimenti erariali resi disponibili dal legislatore per consentire il funzionamento della struttura e l'espletamento delle molteplici competenze attribuite all'Autorità sia da norme nazionali che eurounitarie. Per l'anno 2023, la legge di bilancio 29 dicembre 2022, n. 197 ha previsto uno stanziamento di euro 47.367.934 cui si sono aggiunti rimborsi di varia natura erogati da amministrazioni nazionali e organismi dell'Unione europea per complessivi euro 23.347. Va evidenziato, tuttavia, che l'onere posto a carico del bilancio dello Stato per assicurare il corretto funzionamento dell'Autorità è parzialmente compensato dalle somme acquisite direttamente alle casse erariali derivanti dall'attività sanzionatoria del Garante.

Sotto il profilo strettamente contabile, a fronte degli introiti acquisiti dall'Autorità nel 2023 per complessivi 47,3 milioni di euro, e al netto delle partite di giro pari a 11,2 milioni di euro, sono stati registrati impegni di spesa per 38,2 milioni di euro. Il risultato finanziario dell'esercizio ha fatto pertanto registrare un avanzo di amministrazione di 9,1 milioni di euro, in ragione di una politica gestionale attenta a valorizzare ed ottimizzare l'impiego delle risorse erariali. Ad esempio, le procedure per l'immissione in servizio del nuovo personale, previsto con l'incremento della pianta organica, sono state ripartite su più esercizi finanziari, consentendo un migliore bilanciamento tra le esigenze di spesa e le risorse disponibili e generando un effetto positivo in termini di gestione finanziaria. Rispetto al precedente esercizio finanziario, l'incremento delle entrate complessive registrato nel 2023 è stato di 2,1 milioni di euro, con una variazione positiva del 4,59%.

Con riferimento alla spesa, invece, gli oneri registrati nell'anno, pari a 38,2 milioni di euro, risultano in aumento di 4 milioni di euro rispetto al 2022, con uno scostamento negativo di circa il 12%. La spesa complessiva è da imputare in massima parte alla gestione corrente, nella misura di 37,6 milioni di euro, mentre la parte residuale rappresenta la quota delle risorse finanziarie destinate ad acquisti durevoli costituiti prevalentemente da prodotti *software* e attrezzature informatiche utilizzate a supporto delle attività istituzionali. Anche per il 2023 la struttura della spesa fa emergere, come per il passato e in analogia con le altre autorità amministrative indipendenti,

una significativa incidenza degli oneri del personale rispetto alla spesa complessiva per il funzionamento. L'indennità di carica riconosciuta al presidente ed ai componenti del Collegio del Garante è stata definita nei limiti e sulla base di parametri specificati dalla legge e alla relativa erogazione l'Ufficio ha provveduto nel rispetto dei vincoli e delle prescrizioni vigenti.

Con riferimento, infine, agli oneri strettamente connessi alle esigenze gestionali, l'Autorità ha curato il rispetto dei limiti di legge. Si rinvia alla sez. IV, tab. 21, per una sintetica illustrazione dei valori della gestione finanziaria suddivisa tra entrate e spese correnti, in conto capitale e per meri trasferimenti. I relativi importi sono posti a raffronto con i corrispondenti valori del precedente esercizio finanziario in modo da evidenziare i rispettivi scostamenti, sia in valore assoluto che in termini percentuali.

25

25.2. *L'attività contrattuale, la logistica e la manutenzione dell'immobile*

Nel corso del 2023 è stato approvato il nuovo codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36), contenente numerose e sostanziali novità in tema di digitalizzazione del ciclo di vita dei contratti: utilizzo delle piattaforme telematiche, pubblicità degli atti di gara, trasparenza, accesso agli atti, *e-procurement* e adempimenti sulla banca dati ANAC. L'adeguamento alle nuove disposizioni ha determinato un rilevante incremento di attività per le risorse impiegate nel settore contratti, sia in termini organizzativi che di apprendimento di nuove competenze, anche attraverso apposite attività di formazione (v. *infra*).

Sono state conseguentemente aggiornate le disposizioni interne, le procedure e la modulistica. In tale ambito, ha assunto un rilievo particolare l'approvazione della nuova direttiva in materia di lavori, servizi e forniture, adottata nel mese di giugno 2023 con determinazione del Segretario generale. Anche in questo caso, le novità contenutistiche e procedurali delle relative disposizioni sono state oggetto di specifiche attività formative nel corso del 2023.

Tali percorsi di innovazione amministrativa e gestionale si sono aggiunti alle attività correnti e già avviate nel corso del 2022, finalizzate anche alla qualificazione dell'Ufficio del Garante quale stazione appaltante abilitata presso l'ANAC. All'esito di tale attività, conclusa nel mese di giugno 2023, l'Ufficio ha ottenuto tale qualificazione per appalti di servizi e forniture relativamente ad importi inferiori a 5 milioni di euro, rientrando così nel ristretto novero di stazioni appaltanti italiane (10%) che risultavano qualificate alla data di entrata in vigore del nuovo sistema di qualificazione (1° luglio 2023).

In materia di appalti pubblici, anche per l'anno in esame l'Autorità ha fatto ricorso, nel pieno rispetto della normativa vigente, a procedure di affidamento basate su comparazioni, adoperando prioritariamente gli strumenti di acquisto e negoziazione messi a disposizione da CONSIP S.p.A., ove disponibili. Va evidenziato che l'Autorità ha continuato ad applicare con rigore i principi fondamentali del codice dei contratti pubblici e in particolare quelli di rotazione delle imprese affidatarie e di concorrenza tra le stesse, come dimostrato dall'ampia diversificazione dell'identità delle imprese contraenti, pur in corrispondenza di affidamenti di modesto importo, anche in virtù del percorso agevolato costituito dal ricorso al Mercato elettronico della pubblica amministrazione (MEPA) e alle sue procedure di maggiore snellezza.

Dal punto di vista operativo, l'Autorità ha avviato nell'anno in corso l'esecuzione di due nuovi contratti: il primo relativo ad un *software* di gestione delle gare e del ciclo degli appalti su Piattaforma certificata da ANAC, il secondo relativo alla gestione degli adempimenti in materia di trasparenza (cfr. par. 25.4).

Programmazione

In materia di programmazione biennale delle richieste di acquisto di beni e servizi, a seguito delle previste attività di interlocuzione con le unità organizzative per la raccolta dei fabbisogni e la relativa verifica di copertura finanziaria, è stato approvato dal Segretario generale il Programma degli acquisti per il biennio 2023-2024. Al fine di adempiere agli obblighi di pubblicità e trasparenza, sono state avviate in questa fase le pubblicazioni del Programma sul sito del Ministero delle infrastrutture e dei trasporti e sul portale dell'Autorità.

Da un punto di vista procedurale, il processo di pianificazione degli acquisti di beni e servizi non ha subito modifiche sostanziali per effetto del nuovo codice dei contratti pubblici; tuttavia, si dovranno prevedere alcuni adattamenti organizzativi sia rispetto alla mutata frequenza di programmazione (che passa da biennale a triennale) sia riguardo alla diversa soglia prevista dal codice per i servizi e forniture da inserire nel documento di programmazione, pari a 140.000 euro a decorrere dal 2024.

Procedure di affidamento

Nel corso del 2023, l'attività contrattuale di maggior peso in termini di impiego di risorse – umane ed economiche – è stata la procedura aperta sopra soglia comunitaria per la gestione del piano sanitario 2023-2025, preceduta dalle necessarie interlocuzioni con le organizzazioni sindacali. La gara è stata aggiudicata in tempi relativamente brevi, mediante sottoscrizione della relativa Convenzione con una Cassa di assistenza sanitaria per la durata di due anni, salvo eventuale proroga.

Riguardo agli altri ambiti merceologici, l'attività negoziale dell'Ufficio si è esplicata prevalentemente nel settore ICT (per circa il 25% delle procedure e per quasi il 60% degli importi affidati), anche per effetto dell'incremento della pianta organica e della contestuale adozione di provvedimenti volti a stabilizzare la modalità di svolgimento da remoto della prestazione lavorativa, nonché per l'avvio di un nuovo sistema di digitalizzazione dei processi interni che ha comportato l'acquisizione di nuove soluzioni applicative dedicate alla gestione degli obblighi di trasparenza, alla formazione interna e all'automazione di alcune attività, coerentemente con il progetto più strutturale e strategico di progressiva transizione ai servizi digitali basati su *cloud*. In tale ottica si colloca, peraltro, l'adesione al Polo strategico nazionale, parzialmente finanziata con risorse comunitarie, la cui complessità ha comportato la rimodulazione della programmazione degli acquisti di ulteriori beni e servizi afferenti al settore ICT.

Nel 2023, sono state aggiudicate tre richieste di offerta sul MEPA, aventi ad oggetto rispettivamente: i servizi di rassegna stampa; i servizi di stampa dei prodotti editoriali dell'Autorità (Relazione annuale, opuscoli, *vademecum*, libri); il servizio di supporto operativo per l'elaborazione delle competenze economiche del personale. Al fine di garantire la massima concorrenza possibile, unitamente alla speditezza propria delle procedure gestite sul MEPA, è stata privilegiata la forma della Richiesta di offerta (RDO) "aperta", che ha come destinatari potenziali tutti gli operatori economici iscritti nella pertinente categoria del relativo bando MEPA.

Riguardo ai servizi di stampa di prodotti editoriali si è proceduto, come già in passato, alla sottoscrizione di un contratto quadro con un operatore economico, cui rivolgersi sulla base delle effettive necessità dell'Ufficio nel periodo di riferimento, evitandosi così la parcellizzazione e la frammentazione di singoli micro-affidamenti, appunto in un'ottica di programmazione delle attività. Tale RDO ha riscontrato un significativo interesse da parte degli operatori economici, che ha portato alla ricezione di quindici richieste di partecipazione. Numerose anche le procedure finalizzate all'affidamento diretto di contratti, tra le quali si richiamano: i servizi di gestione delle trasferte del personale, riguardo ai quali non sussistono i presupposti per una adesione al nuovo Accordo quadro CONSIP, la cui precedente edizione ha peraltro mostrato notevoli limiti; l'acquisizione di una piattaforma digitale per la formazione del personale; dotazioni informatiche per il personale (*notebook*, connettività, ecc.), anche in vista delle nuove assunzioni; servizi connessi con lo svolgimento di ulteriori procedure concorsuali, e altro.

Il portale Acquistinretepa.it gestito da CONSIP, al cui interno è collocato tra l'altro il MEPA, continua ad essere il punto di riferimento del settore contratti quanto a procedure adottate: su di esso è stato concluso il 56% del numero di affidamenti sotto soglia comunitaria dell'anno in esame, per un valore pari all'82% dell'importo totale degli stessi. Il portale CONSIP ha quindi continuato a rivestire un ruolo fondamentale, sia per l'ampia disponibilità di iniziative d'acquisto sia per l'efficacia degli strumenti di comparazione dei prezzi, sebbene nel periodo di riferimento la fruibilità del sito abbia scontato alcuni disservizi dovuti alle esigenze di aggiornamento alla nuova normativa del settore.

È altresì proseguita l'attività di costante aggiornamento dell'elenco di avvocati del libero foro cui l'Autorità può ricorrere per gli incarichi di patrocinio legale nell'interesse del Garante, nei rari casi in cui la sua difesa non possa essere assunta dall'Avvocatura dello Stato a causa della natura pubblica della controparte.

La sede degli uffici del Garante è condotta in locazione e l'Autorità non detiene immobili adibiti ad abitazione o foresteria. In considerazione della necessità di rimodulare la logistica della propria sede in funzione del previsto incremento di personale, nel 2023 sono state indette varie indagini di mercato volte ad acquisire manifestazioni di interesse circa la vendita ovvero la locazione passiva di un immobile adatto alla destinazione a uso ufficio come sede istituzionale del Garante. In esito a tali procedure, non sono state individuate soluzioni allocative soddisfacenti rispetto ai requisiti attesi e/o alle disponibilità economiche dell'Autorità.

Per quanto attiene ai servizi connessi alla sede – pulizie, *reception*, manutenzione ordinaria, impianti – in vista delle scadenze contrattuali previste al 31 gennaio 2024 è stato avviato un articolato processo di comparazione, tenendo conto degli strumenti di acquisto disponibili: la Convenzione CONSIP “*Facility management 4*”, l'Accordo quadro CONSIP “grandi immobili”, nonché la proroga del vigente contratto, nei termini già previsti in sede di gara effettuata sul Sistema dinamico della p.a. di CONSIP. Le perduranti incertezze in merito alla definitiva sistemazione della sede hanno infine indirizzato verso tale ultima soluzione, formalizzata a inizio del 2024, con riserva di procedere successivamente all'adesione a uno dei citati strumenti di acquisto.

Per quanto riguarda la manutenzione e l'efficientamento logistico dell'immobile attualmente in uso, sono stati effettuati interventi di ottimizzazione degli spazi, anche adottando soluzioni di arredo *open space* per l'allestimento di ambienti di lavoro più funzionali e versatili, sempre nel rispetto degli standard di sicurezza previsti dal d.lgs. n. 81/2008 e successive modifiche.

Il Garante ha inoltre avviato uno studio per la riorganizzazione degli spazi di ufficio secondo le esigenze derivanti dal ricorso sempre più esteso al lavoro agile. Infine, d'intesa con la proprietà dell'immobile che ospita la sede del Garante, è stato messo a punto un progetto per l'adozione di misure di contenimento della spesa energetica e di certificazione *green*, nel pieno rispetto delle direttive e delle disposizioni, anche di carattere locale, diramate in materia.

25.3. L'organizzazione dell'Ufficio

Nell'anno di riferimento è proseguito il processo di attuazione del piano strategico dell'Autorità per il pieno raggiungimento degli obiettivi programmati, secondo una duplice linea di azione che mira, dal lato interno, a rafforzare l'organico e reingegnerizzare i processi lavorativi, dal lato esterno, a valorizzare forme di collaborazione con *stakeholder* istituzionali e sociali che compartecipano nei rispettivi ambiti sulle tematiche della protezione dei dati personali (es. lotta al cyberbullismo, impatti dell'intelligenza artificiale, ecc.).

25

La sede del Garante e i contratti connessi alla attività di manutenzione

Il rafforzamento dell'Autorità

Con riguardo al reclutamento del personale, anche il 2023 è stato fortemente interessato dalla gestione di procedure concorsuali finalizzate alla progressiva copertura dei posti della pianta organica. In particolare, oltre al completamento di alcune delle procedure relative ai concorsi banditi nell'anno precedente (inclusa la fase di assunzione ed inserimento del nuovo personale assunto), i competenti uffici del Garante sono stati impegnati nella predisposizione degli atti e delle azioni necessarie allo svolgimento di nuove procedure concorsuali volte alla selezione e al reclutamento di sedici posti di funzionario con competenze specifiche in materia di protezione dei dati personali, e a un posto di funzionario per lo svolgimento di mansioni di traduttore linguistico specializzato nella traduzione dall'italiano all'inglese (bando congiunto con AGCM). Inoltre, è stata attivata e definita una procedura comparativa per il conferimento, ai sensi dell'art. 7, comma 6, d.lgs. n. 165/2001, di quattro incarichi di durata biennale a consulenti specializzati nel settore dell'intelligenza artificiale. I candidati risultati vincitori della procedura hanno peraltro rinunciato al conferimento dell'incarico.

Lavoro agile

Sulla base dell'esperienza maturata nel periodo emergenziale, l'Autorità ha ridefinito l'istituto del lavoro agile come modalità regolata, strutturale e flessibile di svolgimento della prestazione lavorativa, a conclusione di un percorso condiviso con le organizzazioni sindacali che ha portato alla stipula di un accordo coerente con la disciplina di riferimento, comprese le disposizioni normative a tutela dei lavoratori fragili.

Durante il 2023, l'Ufficio è stato inoltre impegnato costantemente nella gestione dell'accordo sul lavoro agile sottoscritto nel mese di aprile 2022 e prorogato per l'anno di riferimento, ivi compreso il rinnovo dei contratti individuali per il personale aderente con tutti i relativi adempimenti amministrativi.

Relazioni sindacali

Con riferimento alla gestione delle relazioni sindacali, anche il 2023 è stato contrassegnato dal costante confronto con le organizzazioni sindacali su varie questioni negoziali, come l'adeguamento delle tabelle stipendiali, il piano sanitario rivolto al personale e il già citato accordo per lo svolgimento dell'attività lavorativa in modalità agile.

Sicurezza sul lavoro

In tema di sicurezza e salute dei lavoratori, sono proseguite le attività di gestione dei profili di sicurezza individuali, soprattutto con riferimento all'esecuzione del piano di visite mediche per monitorare lo stato di salute psicofisica dei lavoratori, secondo le modalità stabilite dal d.lgs. n. 81 /2008. In particolare, nel corso del 2023 è stato completato il programma di visite mediche relative al primo ciclo di sorveglianza sanitaria che ha interessato la totalità del personale. Inoltre, è proseguita la costante interlocuzione con il medico competente al fine di garantire una corretta ed equa applicazione in tema degli istituti di sorveglianza sanitaria eccezionale e di proroga del lavoro agile emergenziale in favore dei lavoratori fragili, nonché con riguardo al tema della sicurezza e della salute nei luoghi di lavoro, qui anche con la collaborazione del Responsabile del servizio di prevenzione e protezione. L'Autorità ha incrementato il numero delle unità componenti le squadre di primo soccorso e di antincendio, al fine di assicurare le migliori condizioni di sicurezza all'interno della propria sede.

Formazione del personale

Anche nel 2023, il Garante si è attivato nella individuazione di soluzioni formative innovative per la crescita delle competenze individuali e di gruppo, coerentemente con le esigenze manifestate dai rispettivi Servizi e Dipartimenti. Allo scopo, è stato prorogato il rapporto collaborativo con la Scuola nazionale dell'amministrazione (SNA), il cui catalogo è costantemente aggiornato anche grazie al Club dei formatori della medesima scuola. Trattasi di un progetto al quale prendono parte anche i referenti dell'Autorità al fine di migliorare il grado di coerenza della programmazione didattica della SNA con le effettive esigenze formative delle amministrazioni e dello

stesso Garante. Contestualmente, l'Autorità ha aderito ai corsi compresi nell'iniziativa, gestita dall'INPS, denominata Valore PA e alla Piattaforma *online* Syllabus del Dipartimento della funzione pubblica, attraverso le quali è possibile partecipare a corsi di formazione fruibili a distanza, in modalità *e-learning*. Inoltre, tenuto conto dell'entrata in vigore del nuovo codice dei contratti pubblici, il Garante ha organizzato, nel corso del 2023, vari cicli di approfondimento tematico relativi alle nuove disposizioni, destinati al proprio personale, mediante corsi *online* o in regime di autoformazione. Sempre in materia di contratti pubblici, l'Ufficio ha operato a favore della formazione specifica, con particolare riguardo ai responsabili unici di progetto, anche tramite sessioni formative erogate a distanza da una società specializzata nel settore; tali attività rilevano anche ai fini della qualificazione della stazione appaltante presso l'ANAC.

Tali plurime iniziative si sono affiancate all'ordinaria attività di aggiornamento interno, assicurata mediante la predisposizione di *dossier* di documentazione tematici e il monitoraggio costante delle modifiche normative oltre che delle pertinenti decisioni di natura amministrativa (anzitutto da parte di ANAC) e giurisdizionale effettuata dal Servizio studi e documentazione (cfr. cap. 24). Il ricorso ai suddetti percorsi formativi, che non hanno comportato significativi oneri finanziari a carico del bilancio dell'Autorità, ha permesso di conseguire un notevole risparmio di spesa a fronte di un incremento quantitativo e qualitativo dell'offerta formativa a beneficio del proprio personale. La ricerca di soluzioni innovative ha anche portato, dopo un attento percorso di sperimentazione e *scouting* tecnologico, all'acquisizione di una soluzione digitale d'avanguardia volta a far convergere su un'unica piattaforma di *e-learning* una pluralità di contenuti didattici interni ed esterni, fruibili dal personale come eventi in diretta o in modalità differita e *on demand*.

Con riguardo, infine, agli obblighi di formazione e aggiornamento dei lavoratori in materia di salute e sicurezza, di cui al d.lgs. n. 81/2008, sono stati completati i relativi percorsi individuali "Rischio medio" per la totalità del personale. Sono stati altresì erogati i corsi formativi specifici destinati al personale individuato per le squadre di primo soccorso, antincendio e utilizzo dei defibrillatori, dislocati in numero adeguato presso i locali della sede dell'Autorità.

Il controllo di gestione presso l'Autorità continua ad incentrarsi sull'analisi periodica degli affari assegnati alle diverse unità organizzative mediante il sistema di protocollazione "Archiflow" e sulla conseguente produzione di una reportistica mensile di carattere statistico che si focalizza sull'andamento della trattazione degli affari, dando conto dei flussi relativi agli affari assegnati ed evasi dalle unità organizzative.

La Responsabile della protezione dati ha garantito sia il consueto supporto al titolare del trattamento che le attività di vigilanza previste dall'art. 39 del RGPD. L'attività della RPD nel corso dell'anno si è intensificata vista la necessità di dare riscontro ad un numero crescente di questioni di interesse interno come alle istanze provenienti da soggetti esterni. È stato in particolare fornito supporto alla rete degli RPD delle autorità di protezione dati europee, costituitasi nell'ambito del Comitato europeo per la protezione dei dati (EDPB-DPO *Network*) nella trattazione delle questioni di maggior interesse comune relative all'applicazione della normativa nazionale ed eurounitaria. Inoltre, a livello nazionale, per quanto concerne la rete costituita tra gli RPD delle autorità indipendenti, si è contribuito all'organizzazione di incontri tematici e seminari di approfondimento finalizzati alla condivisione di conoscenze e allo scambio di esperienze relative all'applicazione della normativa nel particolare contesto delle autorità italiane.

In crescita anche il numero di *e-mail* pervenute alla casella dedicata, alle quali si è dato puntuale riscontro.

25

Servizio controllo di gestione

RPD

25

25.4. “Amministrazione trasparente” e adempimenti relativi alla disciplina anticorruzione

Presso l’Autorità ha continuato a trovare attuazione la disciplina di trasparenza come pure le misure generali volte a prevenire fenomeni rientranti nell’ampia accezione del termine “corruzione”; un quadro sintetico degli aspetti salienti dell’attività svolta può desumersi dalla relazione annuale del Responsabile della prevenzione della corruzione e della trasparenza (RPCT) riferita al 2023, oggetto di pubblicazione nella sezione “Amministrazione trasparente” (doc. web n. 9979018).

Entro questa cornice generale di riferimento, il Garante, muovendo dalla considerazione che le autorità amministrative indipendenti non sono tenute all’adozione del Piano integrato di attività e organizzazione (PIAO) – come pure ribadito dall’ANAC nei propri “Orientamenti per la pianificazione anticorruzione e trasparenza 2022” del 2 febbraio 2022, in particolare alle pp. 3-4, e nel Piano nazionale anticorruzione 2022, p. 26 – ha adottato, con la deliberazione 23 marzo 2023, n. 78, il Piano triennale di prevenzione della corruzione e della trasparenza 2023-2025 (doc. web n. 9870327).

Grazie al contributo delle unità organizzative competenti è stata alimentata la sezione “Amministrazione trasparente” del sito web istituzionale; sulla scorta della delibera ANAC 17 maggio 2023, n. 203, è stata altresì pubblicata la griglia di rilevazione (cfr. doc. web n. 9929200) resa disponibile mediante l’applicativo web realizzato dall’ANAC, la cui redazione, in assenza di OIV o strutture equivalenti presso l’Autorità, è stata curata dal RPCT; quest’ultimo ha quindi provveduto a pubblicare anche la scheda di monitoraggio e attestazione (doc. web n. 9961572).

Anche all’esito delle attività di monitoraggio testé menzionate, al fine di assicurare il puntuale assolvimento degli obblighi di trasparenza, l’Autorità ha provveduto a innovare il processo interno di pubblicazione ricorrendo al supporto professionale fornito da una *software house* specializzata in soluzioni SaaS per la pubblica amministrazione, consistente in una soluzione applicativa ceduta con la formula del riuso *ex artt.* 68-69 del CAD. L’adozione di un *software* professionale per adempiere in modo più efficace alle disposizioni del d.lgs. n. 33/2013 (nella fattispecie PAT - Portale amministrazione trasparente di AgID) ha infatti l’obiettivo di fluidificare i flussi informativi interni, consentendo alle singole unità organizzative di gestire in autonomia le funzioni di inserimento degli atti di propria competenza attraverso una procedura rapida, intuitiva e costantemente aggiornata al quadro normativo. Tale innovazione produrrà i suoi effetti con la piena operatività del portale (che avrà luogo nel 1° trimestre 2024). Quale azione ulteriore volta al miglioramento quali-quantitativo delle pubblicazioni pregresse va menzionata la puntuale ricognizione dei dati recuperabili in formato aperto.

In chiave prospettica (anche per finalità di prevenzione della corruzione e di incremento del livello di trasparenza), particolare rilevanza è stata attribuita progettazione del sistema di gestione digitale dei processi di lavoro (*Business Process Management*) mediante la costituzione di un *team* composto da personale appartenente a diverse funzioni amministrative (tecnologica ed organizzativa) (cfr. par. 25.5).

A seguito dell’introduzione del decreto legislativo 10 marzo 2023, n. 24 (Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali), la procedura di segnalazione degli illeciti – già attiva presso l’Autorità dal 2018 – ha formato oggetto di rivisitazione attraverso le apposite istruzioni impartite dal Segretario generale con circolare 28 dicembre 2023, pubblicate nella intranet nonché nella sezione “Amministrazione trasparente” del sito web (doc. web n. 9967753).

25

Sono state intraprese le attività prodromiche all'aggiornamento del Piano triennale di prevenzione della corruzione e della trasparenza (PTPCT 2024-2026), che hanno visto il coinvolgimento del personale dirigenziale mediante la compilazione di apposite schede di rilevazione predisposte dal RPCT finalizzate a verificare l'attualità della mappatura dei processi in essere presso il Garante e dei relativi rischi; tale attività ha consentito di integrare alcuni ulteriori processi connessi, in particolare, all'introduzione del nuovo codice dei contratti pubblici (d.lgs. 31 marzo 2023, n. 36).

Infine, con riguardo alla disciplina in materia di accesso civico introdotta con decreto legislativo n. 33/2013, nel corso dell'anno è stato dato tempestivo riscontro a tutte le istanze pervenute all'Autorità nel 2023 (pari a quattordici) e a quelle di riesame (pari a due); non sono pervenute istanze di accesso civico relative a dati soggetti a pubblicazione obbligatoria (*ex art. 5, comma 1, d.lgs. n. 33/2013*).

25.5. Il settore informatico-tecnologico e la transizione digitale

Il 2023 è stato caratterizzato da significative attività di sviluppo ed evoluzione dei sistemi informativi in ottica *cloud* nelle componenti applicative-funzionali (servizi *online*) e in quelle infrastrutturali.

Per quanto attiene agli sviluppi applicativo-funzionali, sono state effettuate numerose attività di carattere evolutivo e di progettazione finalizzata alla reingegnerizzazione di alcuni processi.

Con riguardo ai servizi *online*, sono state apportate modifiche migliorative al servizio riservato alla comunicazione dei dati di contatto del RPD, con il rilascio della nuova funzionalità per l'invio dei riscontri ai precedenti RPD in occasione di variazione delle comunicazioni.

Nell'ambito del servizio riservato alle segnalazioni di telefonate indesiderate è stata attivata la possibilità di effettuare segnalazioni previa autenticazione mediante sistemi SPID, CIE ed eIDAS.

Per le segnalazioni *online* in materia di *revenge porn* sono state rese disponibili ulteriori modalità per la consultazione sicura del materiale fornito dai segnalanti.

Utilizzando la stessa piattaforma tecnologica, inoltre, sono state sviluppate e rese disponibili ai competenti Dipartimenti/Servizi le seguenti funzionalità:

- per le segnalazioni in materia di *revenge porn*, è stato realizzato un sistema che consente la gestione delle assegnazioni nonché lo stato di lavorazione;
- per la gestione delle relazioni con il pubblico, è stato realizzato un sistema che consente un più rapido ed efficiente riscontro delle richieste di informazioni relativamente alle comunicazioni dei dati di contatto del RPD;
- per le segnalazioni in materia di telefonate indesiderate, sono state implementate nuove funzioni per l'analisi delle informazioni raccolte.

Nell'ambito della reingegnerizzazione dei processi interni si è proceduto all'individuazione di una nuova piattaforma tecnologica per l'implementazione di un sistema di *Business Process Management* (e relativa procedura di approvvigionamento di beni e servizi) e alla progettazione di una prima *release* del nuovo servizio, rivolto all'utenza esterna, per la trasmissione di reclami e segnalazioni.

Infine, in relazione agli aspetti di potenziamento della resilienza in materia di *cybersecurity*, l'Autorità ha aderito a una specifica iniziativa promossa dall'Agenzia per la cybersicurezza nazionale e finanziata con fondi previsti dal PNRR (cfr. avviso pubblico n. 7/2023), che è poi sfociata nel riconoscimento di un cospicuo finanziamento per l'analisi della postura dell'Autorità sul versante della sicurezza.

Per quanto riguarda gli aspetti infrastrutturali, di particolare rilievo è stata la partecipazione al bando PNRR pubblicato dal Dipartimento per la trasformazione

25

digitale della Presidenza del Consiglio di ministri, che ha consentito di presentare una domanda di finanziamento per la migrazione della propria infrastruttura informatica nel costituendo Polo strategico nazionale.

Nell'ambito di tali attività, l'Autorità è stata ammessa a fruire di un finanziamento (con decreto del Capo del Dipartimento per la trasformazione digitale), la cui provvista finanziaria è prevista dai fondi PNRR.

A seguito del finanziamento, sono state avviate le attività per la stipulazione di un contratto di servizi con il Polo strategico nazionale S.p.A. che comprende sia i servizi relativi all'erogazione della piattaforma web a supporto del sito istituzionale, sia quelli relativi alla realizzazione di un'infrastruttura IaaS (*Infrastructure as a Service*) federata con l'attuale infrastruttura e dotata di caratteristiche di resilienza, affidabilità, prestazioni e sicurezza idonee alle sfide della trasformazione digitale. A tal fine l'Autorità ha altresì aderito alla specifica Convenzione della Presidenza del Consiglio dei ministri - Dipartimento per la trasformazione digitale del 24 agosto 2022.

Nel corso del 2023 sono state inoltre portate a compimento numerose altre attività in ambito IT, tra le quali si evidenziano la realizzazione di un nuovo collegamento al Sistema pubblico di connettività (SPC) tramite rete Fastweb, la riconfigurazione e l'ammodernamento degli apparati attivi di rete, la messa in opera di un nuovo sistema *mail exchanger* con caratteristiche avanzate di sicurezza e la predisposizione dell'infrastruttura *Virtual Desktop Infrastructure* a supporto della mobilità interna e del lavoro da remoto.

Rilevante e fondamentale, infine, il contributo di analisi tecnologica fornito alle attività di valutazione e decisione dell'Autorità in molteplici contesti, alla luce dei progressi dell'amministrazione digitale e dell'implementazione del PNRR nonché, come è ovvio, del ricorso pervasivo a nuove tecnologie o a tecnologie già note, ma impiegate con modalità innovative. Segnaliamo a tale riguardo la realizzazione del laboratorio a supporto delle attività di accertamento riferite al caso strategico individuato a livello di CEPD sulle *smart TV* (cfr. par. 12.9).



GPDP

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

I dati statistici

RELAZIONE ANNUALE

2023

PAGINA BIANCA

IV - I dati statistici 2023

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	634
Risposte ad atti di sindacato ispettivo e di controllo	1
Audizioni del Presidente del Garante o memorie scritte trasmesse al Parlamento	8
Pareri su norme di rango primario statale, delle regioni e delle autonomie ex art. 36, par. 4, RGPD	6
Pareri su atti regolamentari e amministrativi ex art. 36, par. 4, RGPD	53
Pareri ai sensi dell'art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)	6
Pareri ai sensi dell'art. 110 del Codice per la realizzazione di un progetto di ricerca medica, biomedica e epidemiologica nonché ex art. 36 del RGPD	16
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	22
Autorizzazioni di accordi amministrativi ai sensi degli artt. 46, par. 3, lett. b), 58, par. 3, lett. i) e 63, RGPD	2
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio	110
Provvedimenti collegiali a seguito di reclamo, segnalazione nonché a seguito di accertamenti d'ufficio con contestuale ordinanza-ingiunzione	153
Provvedimenti collegiali a seguito di notifica di violazione di dati	4
Provvedimenti collegiali a seguito di notifica di violazione di dati con contestuale ordinanza-ingiunzione	9
Misure correttive e sanzionatorie (art. 58, par. 2, RGPD)	394
Misure correttive e sanzionatorie (d.lgs. n. 51/2018)	0
Ricorsi giurisdizionali trattati ex art. 152, d.lgs. n. 196/2003	101
Opposizioni (trattate) a provvedimenti del Garante	75
Pagamenti derivanti dall'attività sanzionatoria	7.977.343
Comunicazioni di notizia di reato all'Autorità giudiziaria	7
Delibere dirigenziali in materia di <i>revenge porn</i> ratificate dal Collegio	299
Provvedimenti di approvazione di codici di condotta	1
Violazioni di dati personali notificate	2.037
Accertamenti e controlli effettuati <i>in loco</i> (artt. 157-158, d.lgs. n. 196/2003)	144
Riscontri a segnalazioni e reclami (art. 11, reg. Garante n. 1/2019)	9.281
Riscontri a quesiti (art. 11, reg. Garante n. 1/2019)	506
Contatti Servizio relazioni con il pubblico	15.048
Procedure IMI di cooperazione e di coerenza (Capo VII RGPD)	1.595
Riunioni del Comitato europeo per la protezione dei dati personali	15
Partecipazione a sottogruppi di lavoro del CEPD	176
Riunioni e ispezioni autorità comuni di controllo/organismi di supervisione (EUROPOL, SIS II, Dogane, EURODAC, VIS)	12
Riunioni presso il CoE e l'OCSE	17
Conferenze internazionali	6
Altre conferenze e incontri	9

Tabella 1. Sintesi delle principali attività dell'Autorità

(*) inerenti anche ad affari pervenuti anteriormente al 2023

Tabella 2. Pareri ex art. 36, par. 4, RGPD su norme di rango primario statale, delle regioni e delle autonomie

Pareri ex art. 36, par. 4, RGPD su norme di rango primario statale, delle regioni e delle autonomie	
Temi	Riscontri resi nell'anno*
Attività economiche/accertamento fiscale	2
Digitalizzazione p.a.	1
Giustizia	2
Open data	1
Totale	6

Tabella 3. Pareri ex art. 36, par. 4, RGPD su atti regolamentari e amministrativi resi al Governo

Pareri ex art. 36, par. 4, RGPD su atti regolamentari e amministrativi resi al Governo	
Temi	Riscontri resi nell'anno*
Digitalizzazione p.a.	10
Fisco	1
Funzioni di interesse pubblico	1
Giustizia	18
Imprese	4
Intercettazioni	2
Istruzione	2
Sanità	13
Trasporti	2
Totale	53

Tabella 4. Pareri ex art. 36, par. 4, RGPD su atti regolamentari e amministrativi resi ad altre istituzioni

Pareri ex art. 36, par. 4, RGPD su atti regolamentari e amministrativi resi ad altre istituzioni	
Temi	Riscontri resi nell'anno*
Digitalizzazione p.a.	3
Diritti fondamentali	2
Fisco	6
Funzioni di interesse pubblico	1
Statistica	1
Totale	13

Pareri ex art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)	
Temì	Riscontri resi nell'anno*
Digitalizzazione p.a.	2
Funzioni di interesse pubblico	3
Statistica	1
Totale	6

Tabella 5. Pareri ex art. 36, par. 1, RGPD (valutazione d'impatto sulla protezione dati)

Misure correttive e sanzionatorie (art. 58, par. 2, RGPD)	
Avvertimenti a titolare/responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare il RGPD (art. 58, par. 2, lett. a), RGPD)	8
Ammonizioni a titolare/responsabile del trattamento per violazioni RGPD (art. 58, par. 2, lett. b), RGPD)	65
Ingiunzioni a titolare/responsabile del trattamento a soddisfare le richieste degli interessati di esercitare i diritti loro derivanti dal RGPD (art. 58, par. 2, lett. c), RGPD)	25
Ingiunzioni a titolare/responsabile del trattamento di conformare i trattamenti alle disposizioni del RGPD (art. 58, par. 2, lett. d), RGPD)	46
Ingiunzioni a titolare del trattamento di comunicare all'interessato una violazione dei dati personali (art. 58, par. 2, lett. e), RGPD)	3
Imposizioni di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento (art. 58, par. 2, lett. f), RGPD)	62
Ordine di rettifica/cancellazione di dati personali o limitazione del trattamento ex artt. 16, 17 e 18 e altre misure previste dall'art. 58, par. 2, lett. g), RGPD)	21
Sanzioni amministrative pecuniarie ex art. 83, (art. 58, par. 2, lett. i), RGPD)	166
Totale	396

Tabella 6. Misure correttive e sanzionatorie (art. 58, par. 2, RGPD)

Pagamenti derivanti dall'attività sanzionatoria	
Pagamenti spontanei dei contravventori	6.432.046,65
Riscossione coattiva	1.545.296,12
Totale	7.977.342,77

Tabella 7. Pagamenti derivanti dall'attività sanzionatoria

Comunicazioni di notizia di reato all'Autorità giudiziaria	
Accesso abusivo ad un sistema informatico o telematico (art. 615-ter, c.p.)	1
Inosservanza di provvedimenti del Garante (art. 170, d.lgs. n. 196/2003)	1
Sostituzione di persona (art. 494, c.p.)	2
Trattamento illecito dei dati (art. 167, d.lgs. n. 196/2003)	1
Violazioni in materia di controlli a distanza dei lavoratori (art. 171, d.lgs. n. 196/2003)	2
Totale	7

Tabella 8. Comunicazioni di notizia di reato all'Autorità giudiziaria

*relative anche a violazioni notificate negli anni precedenti

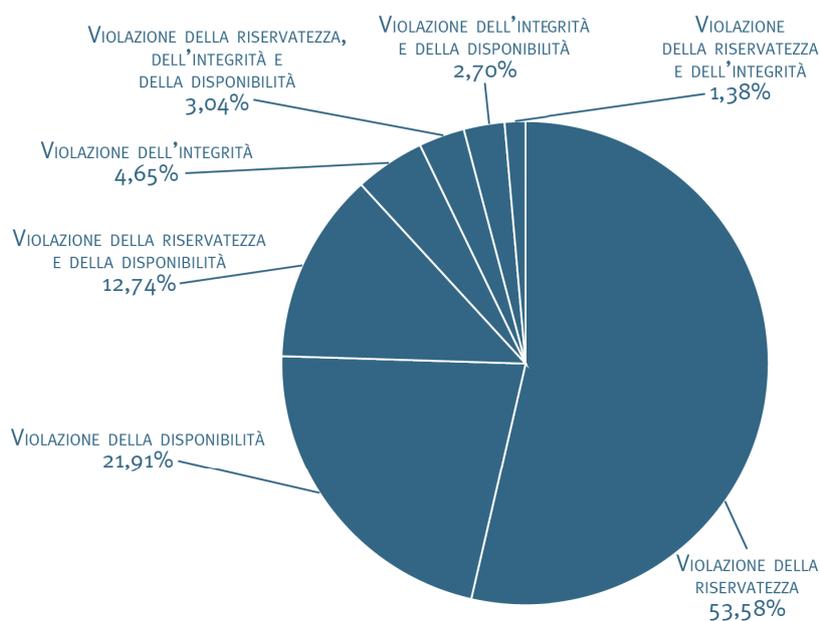
Tabella 9. Violazioni di dati personali notificate per tipologia del titolare

Violazioni di dati personali notificate per tipologia del titolare	
Soggetti pubblici	753
Soggetti privati	1.284
Totale	2.037

Tabella 10. Notifiche di violazioni di dati personali ricevute per tipologia di notifica

Notifiche di violazioni di dati personali ricevute per tipologia di notifica	
Completa	734
Preliminare	1.303
Integrativa*	1.403
Totale	3.440

Grafico 11. Notifiche di violazioni di dati ricevute per natura della violazione



(*) inerenti anche ad affari pervenuti anteriormente al 2023

Segnalazioni e reclami		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
Attività ispettive	0	20
Affari legali e giustizia	170	130
Intelligenza artificiale	1	0
Libertà di manifestazione del pensiero e cyberbullismo	1.335	999**
Realtà economiche e produttive	3.232	3.388
Realtà pubbliche	1.284	1.124
Reti telematiche e <i>marketing</i>	113.829	3.142
Sanità e ricerca	255	278
Tecnologie digitali e sicurezza informatica	44	43
Altre UU.OO.	161	157
Totale	120.311	9.281

Tabella 12. Segnalazioni e reclami

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
Affari legali e giustizia	6	9
Intelligenza artificiale	3	0
Libertà di manifestazione del pensiero e cyberbullismo	12	16
Realtà economiche e produttive	87	157
Realtà pubbliche	113	179
Reti telematiche e <i>marketing</i>	48	27
Sanità e ricerca	38	33
Tecnologie digitali e sicurezza informatica	1	0
Altre UU.OO.	73	85
Totale	381	506

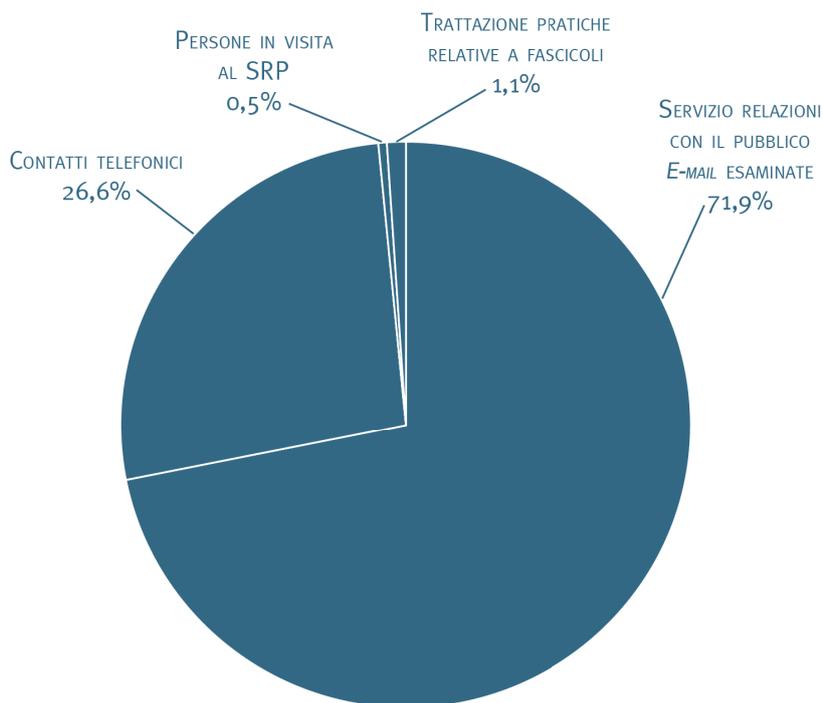
Tabella 13. Quesiti

(*) inerenti anche ad affari pervenuti anteriormente al 2023

(**) di cui 299 in materia di *revenge porn*

Tabella 14. Servizio relazioni con il pubblico

Servizio relazioni con il pubblico	
E-mail esaminate	10.815
Contatti telefonici	4.000
Persone in visita al SRP	72
Trattazione pratiche relative a fascicoli	161
Totale	15.048



Cooperazione tra autorità nazionali di protezione dei dati personali - procedure IMI (Capo VII RGPD)	
← (segue)	
4) Procedure di cooperazione informale <i>ex art. 60 del RGPD</i> alle quali l'Autorità ha partecipato in qualità di:	87
a) "autorità interessata"	87
b) "autorità capofila"	-
5) Progetti di decisione <i>ex art. 60 del RGPD</i> rispetto ai quali l'Autorità ha cooperato in qualità di:	343
a1) "autorità interessata"	321
a2) "autorità interessata" e rispetto ai quali sono state sollevate "obiezioni pertinenti e motivate" o commenti <i>ex art. 60, par. 4, del RGPD</i>	15
b) "autorità capofila"	2
c) altro	5
6) Richieste di assistenza reciproca <i>ex art. 61 del RGPD</i>	278
a) ricevute da altre autorità	247
b) inviate ad altre autorità	31
7) Operazioni congiunte <i>ex art. 62 del RGPD</i> alle quali l'Autorità ha preso parte	3

Tabella 17. Meccanismo di coerenza - procedure IMI (Capo VII RGPD)

Meccanismo di coerenza - procedure IMI (Capo VII RGPD)	
1) Procedure relative all'attività consultiva dell'EDPB <i>ex art. 64 del RGPD</i>	1
2) Procedure relative all'attività decisoria dell'EDPB per la risoluzione delle controversie <i>ex art. 65 del RGPD</i> con la partecipazione dell'Autorità	4
3) Procedure d'urgenza <i>ex art. 66 del RGPD</i>	2

Tabella 18. Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza

Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza	
Assicurazioni	9
Associazioni	1
Biometria	2
Concessionari	1
Confessioni religiose	2
Credito	78
Cyberbullismo	2
Dati in ambito pubblico	11
Dati in ambito sanitario	11
Diritto all'oblio	34
Imprese	205
<i>Deep fake</i>	1
Lavoro	15
Libertà di espressione e di informazione	14
(continua)→	

*in relazione a procedure pervenute dal 01/01/2023

Principali ambiti interessati dalle procedure di cooperazione e dal meccanismo di coerenza	
← (segue)	
Notificazioni di violazione dei dati	63
Recupero crediti	1
Reti telematiche	1.129
RGPD	6
Ricerca	1
Sicurezza informatica	2
Videosorveglianza	7
Totale	1.595

Attività di comunicazione dell'Autorità	
Comunicati stampa	62
Newsletter	17
Prodotti editoriali	10
Campagne informative	4
Video spot e teaser informativi	45
Infografiche e pagine tematiche	71

Tabella 19. Attività di comunicazione dell'Autorità

Personale in servizio (*)				
Area	ruolo (a)	fuori ruolo (b)	comandato presso altre amm.ni o in aspettativa (c)	impiegato dall'Ufficio (a+b-c)
Segretario generale	0	1	0	1
Dirigenti	17	0	2	15
Funzionari	107	5	2	110
Operativi	23	0	0	23
Esecutivi	2	0	0	2
Totale	149	6	4	151
Personale a contratto (art. 156, commi 4 e 5 del Codice)				14

Tabella 20. Personale in servizio

(*) Situazione alla data del 31/12/2023

Tabella 21. Gestione finanziaria

Gestione finanziaria				
Entrate accertate	Anno 2023	Anno 2022	Variazione	
			€	%
Entrate correnti	47.367.934	44.584.987	2.782.947	6,24
Altre entrate, trasferimenti e rimborsi	23.347	726.554	-703.207	-96,79
Totale entrate	47.391.281	45.311.541	2.079.740	4,59
Spese impegnate				
Spese di funzionamento	37.630.314	33.347.228	4.283.086	12,84
Spese in c/capitale	210.566	448.728	-238.162	-53,07
Trasferimenti ad amministrazioni	362.908	380.968	-18.060	-4,74
Totale spese	38.203.788	34.176.924	4.026.864	11,78

Tabella 22. Attività internazionale dell'Autorità

Unione europea			
Comitato europeo per la protezione dati	Sessioni plenarie		17 gennaio 14 e 28 febbraio 28 marzo 13 e 26 aprile 24 e 25 maggio 20 giugno 18 luglio 2 agosto 19 settembre 17 e 27 ottobre 14 novembre 12 e 13 dicembre
	Riunioni dei sottogruppi	Sottogruppo questioni strategiche e attività consultiva (SAESG)	7 e 23 febbraio 29 marzo 26 giugno 17 luglio 5 e 12 settembre 16, 19 e 24 ottobre 10 e 20 novembre
		Border Travel Law Enforcement (BTLE)	26 gennaio 10 febbraio 23 marzo 4 maggio 15 giugno 19 settembre 26 ottobre 30 novembre
			(continua)→

Unione europea	
← (segue)	
Comitato europeo per la protezione dati	<p>Cooperation</p> <p>18 gennaio 9 febbraio 21 marzo 18 e 24 aprile 16 maggio 15 giugno 22 e 30 agosto 5 e 26 settembre 19 ottobre 16 novembre</p>
	<p>Compliance, E-Government and Health</p> <p>24 gennaio 21 febbraio 9 e 10 marzo (<i>workshop</i>) 16 marzo 27 aprile 17 maggio 8, 19 e 26 giugno 11 luglio 21 settembre 20 ottobre 7 novembre 22-24 novembre (<i>workshop</i>) 19 dicembre</p>
	<p>Financial Matters</p> <p>19 gennaio 20 febbraio 6 e 13 marzo 4 aprile 3 maggio 6 giugno 7 e 11 luglio 1° e 21 settembre 28 novembre</p>
	<p>Cookie Banner Task Force</p> <p>11 ottobre 15 novembre</p>
	<p>Key Provisions</p> <p>25 gennaio 1° marzo 18 aprile 30 maggio 6 luglio 26 settembre 26 ottobre 21 e 22 novembre</p>
(continua)→	

Unione europea		
← (segue)		
Comitato europeo per la protezione dati	<i>International Transfers</i>	10, 11 e 31 gennaio 1° e 10 febbraio 14 marzo 11 aprile 31 maggio 1° giugno 4 luglio 5 e 6 settembre 4 e 5 ottobre 7 e 8 novembre 22-24 novembre (<i>workshop</i>) 5 e 6 dicembre
	<i>Technology</i>	18-19 gennaio 16 febbraio 22 marzo 19 aprile 10 maggio 12 e 13 giugno (<i>bootcamp</i>) 14 giugno 13 luglio 13 settembre 18 e 19 ottobre 16 novembre 4 dicembre
	<i>IT Users</i>	13 marzo 16 giugno 9 ottobre 4 dicembre
	<i>Enforcement</i>	8 e 17 febbraio 2, 16 e 22 marzo 4 e 18 aprile 7, 19 e 27 giugno 4, 10, 20 luglio 22 e 30 agosto 12 settembre 18 ottobre 5 dicembre
	<i>Fining Task Force</i>	7 febbraio 9 marzo 19 aprile 8 giugno 13 settembre 15 novembre 11 dicembre
	<i>Task Force 101 Complaints</i>	6 febbraio 6 marzo
	(continua) →	

Unione europea		
← (segue)		
Comitato europeo per la protezione dati	<i>Task Force ChatGPT</i>	18 aprile 3 maggio 12 luglio 6 settembre 20 ottobre 8 novembre 1° dicembre
	<i>Task Force Competition and Consumer Law</i>	28 aprile 21 giugno 6 settembre 15 e 23 novembre 15 dicembre
	<i>Task Force International Engagements</i>	22 maggio 10 luglio 18 settembre 27 novembre
	<i>Social Media Working Group</i>	23 gennaio 23 febbraio 23 maggio 29 giugno 7 settembre 10 ottobre 7 dicembre
	<i>Coordinated Enforcement Framework</i>	9 e 26 gennaio 16 febbraio 4 marzo 12 ottobre 7 e 17 novembre 4 e 8 dicembre
	<i>EDPB DPO Network</i>	25 settembre
	<i>EDPB Communications Network</i>	11 gennaio 9 febbraio 22 marzo 20 aprile 17 maggio 15 giugno 12 luglio 13 settembre 11 ottobre 9 novembre 6 dicembre
	<i>Coordinators</i>	30 gennaio 7 febbraio 27 marzo

Unione europea

Gruppo di coordinamento della supervisione VIS	13 giugno, 28 novembre
Gruppo di supervisione del sistema EURODAC	13 giugno, 28 novembre
Gruppo di coordinamento della supervisione del sistema di informazione doganale: SID	13 giugno
Comitato di controllo coordinato (CSC)	22 marzo, 14 giugno, 29 novembre
EUROPOL <i>Data Protection Experts Network</i> (EDEN)	18 e 19 settembre
<i>High-level Group for the Digital Markets Act</i>	29 novembre
CPC-DPA (Tavolo di lavoro relativo alla cooperazione fra autorità di protezione dati e autorità di tutela dei consumatori)	10 maggio 10 novembre

Riunioni presso OCSE e CoE

Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	Comitato DGP (<i>Data Governance and Privacy in the Digital Economy</i>)	17-18 aprile 9-10 novembre
	DGP <i>Bureau</i>	10 gennaio 21 marzo 12 aprile 6 giugno
Consiglio d'Europa	Comitato consultivo Convenzione 108/1981 (T-PD)	14-16 giugno 15-17 novembre
	T-PD <i>Bureau</i>	22-24 marzo 27-29 settembre
	<i>Committee on Artificial Intelligence</i> (CAI)	11-13 gennaio 1-3 febbraio 19-21 aprile 21 maggio-2 giugno 24-26 ottobre 5-8 dicembre

Conferenze internazionali

GPA (Conferenza internazionale delle autorità di protezione dati)	15-20 ottobre
<i>Spring Conference</i> (Conferenza di primavera delle autorità di protezione dati)	10-12 maggio
<i>Privacy Symposium 2022</i>	17-21 aprile
G7 dei Garanti per la protezione dei dati	20 e 21 giugno
IWGDPT (Gruppo di Berlino)	5-7 giugno 6-8 dicembre

Altre conferenze e *meeting*

ENISA <i>Working group on data protection engineering</i>	30-31 maggio
EDPS <i>Future of Data Protection. Effective enforcement in the digital world</i>	16-17 giugno
<i>Privacy Hub - From Data Access to Data Transformations: How to Govern Data in the Age of Analytics and AI?</i>	23 giugno
<i>Regarding AI & Data Privacy Conference</i>	23 giugno
<i>PETs Network - Future of Privacy Forum</i>	26-27 giugno
CEN JTC 13 WG 5	5 luglio
ENISA <i>Working group on data spaces</i>	2 ottobre
<i>European Case Handling workshop</i>	8-9 novembre
<i>Synthetic Data Summit</i>	30 novembre

PAGINA BIANCA



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Redazione

Garante per la protezione dei dati personali

Piazza Venezia, 11

00187 Roma

Tel. 06 696771

e-mail: protocollo@gdp.it

www.gdp.it



PAGINA BIANCA



191360102820